18. Tätigkeitsbericht 2010/2011

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tätigkeitsbericht 2010/2011 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte hat der Bundesversammlung periodisch einen Bericht über seine Tätigkeit vorzulegen (Art. 30 DSG). Der vorliegende Bericht deckt den Zeitraum zwischen 1. April 2010 und 31. März 2011 ab.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Vertrieb:

BBL, Verkauf Bundespublikationen, CH-3003 Bern

www.bbl.admin.ch/bundespublikationen

Art.-Nr. 410.018.d/f

Inhaltsverzeichnis

Vorwort

Ein Aufruf zum digitalen Spiessertum?

«Wer die ohne Zweifel attraktiven Internetangebote verschiedener Unternehmen nutzen will, soll nicht das Recht auf Privatheit wie den Mantel an der Garderobe abgeben müssen. Wenn digitales Spiessertum bedeutet, auf diesem liberalen Grundrecht zu beharren, sind wir gerne kleinkariert», meinte die NZZ in einem Kommentar kurz vor der Gerichtsverhandlung zu Google Street View Ende Februar 2011. So gesehen, können wir gut mit diesem Prädikat leben.

Andere sprachen von einem Steinzeitdatenschutz und einem Kreuzzug gegen die Moderne, weil wir von Google die Einhaltung unserer Gesetze einfordern und nicht hinnehmen, dass ein global tätiges Unternehmen selber definieren will, welche Massnahmen zum Schutz der Privatsphäre ihm zugemutet werden dürfen. Das Verfahren in Sachen Google Street View und die dadurch lancierte Debatte haben in der Schweiz und im Ausland hohe Wellen geworfen, unterschiedliche Reaktionen ausgelöst (gemäss Umfragen sind die Meinungen ziemlich genau geteilt) und die Auseinandersetzung um den Persönlichkeitsschutz im digitalen Zeitalter zugespitzt. Das Bundesverwaltungsgericht ist unseren Überlegungen weitgehend gefolgt. Das Urteil war bei Redaktionsschluss dieses Tätigkeitsberichts noch nicht rechtskräftig. Dank seiner überzeugenden Begründung leistet es aber auf jeden Fall einen wichtigen Beitrag zur Klärung der Frage, wo die Grenzlinien bei der Abwägung der wirtschaftlichen Interessen von Anbietern neuartiger Medienformate und den Persönlichkeitsrechten der betroffenen Personen verlaufen.

Unabhängig davon steht die Frage im Zentrum, ob eine Firma, deren Datenbearbeitung nicht nur in der Schweiz stattfindet, gemäss den hier geltenden Gesetzen zur Verantwortung gezogen werden kann, wenn Bewohnerinnen und Bewohner dieses Landes in ihren Rechten verletzt werden. Google hat die Zuständigkeit der Schweiz stets verneint. Würde sich diese Rechtsauffassung durchsetzen, hätte das dramatische Folgen für den Persönlichkeitsschutz. Es wäre eine Einladung für global tätige Unternehmen, ihre Datenbearbeitung dorthin auszulagern, wo das Datenschutzniveau am Tiefsten ist. Diese Problematik hat inzwischen auch die EU auf den Plan gerufen: Viviane Reding, EU-Justiz-Kommissarin, ist klar der Meinung, dass jede Firma, die im EU-Markt operiert, oder jedes Online-Produkt, das sich an EU-Konsumenten richtet, die EU-Regeln erfüllen muss. Genau so sollte es auch für die Schweiz sein!

Neben dieser formellen Frage geht es auch darum, ob der Schutz der Privatsphäre lediglich einer vollautomatischen Software überlassen werden darf, auch wenn diese nachweislich nicht immer funktioniert. Oder darf ein zusätzlicher Aufwand für die manuelle Überprüfung verlangt werden, wenn damit die Gefahr ernst zu nehmender

Persönlichkeitsverletzungen gebannt werden kann? Hängt das im Datenschutz realisierbare Mass künftig davon ab, was eine Software zu einem gegebenen Zeitpunkt leisten kann?

Egal, wie diese Punkte höchstrichterlich beantwortet werden: Das Verfahren hat auch Schwachpunkte im Gesetz und bei der internationalen Koordination offen gelegt. Es stellt sich die Frage, ob und wie diese Schwachstellen beseitigt werden können. Auf nationaler Ebene böte die kürzlich vom Bundesrat in Auftrag gegebene Evaluation der Wirksamkeit des Datenschutzgesetzes einen Anknüpfungspunkt. Gestützt auf diese Evaluation wird der Bundesrat gegen Ende des Jahres dem Parlament Bericht erstatten, ob und in welche Richtung beim Datenschutz Handlungsbedarf besteht. Das Parlament hat inzwischen selber bereits zahlreiche Vorstösse zur Verbesserung des Gesetzes eingebracht.

Aus unserer Sicht müsste auf gesetzgeberischer Ebene in erster Linie die Frage beantwortet werden, ob Produkte und Dienstleistungen mit einer grossen Einwirkung auf die Privatsphäre vor ihrer Lancierung nicht einer datenschutzrechtlichen Überprüfung zu unterziehen wären und der Anbieter damit den Nachweis erbringen müsste, dass er alles Zumutbare zum Schutz der Persönlichkeitsrechte unternommen hat. Die heutige Rechtslage führt dazu, dass solche Produkte erst gestoppt werden können, wenn die Rechtsverletzung festgestellt worden ist. Das ist weder für ein innovatives Unternehmen, das viel und möglicherweise falsch in die Entwicklung eines Produkts investierte, noch für die Betroffenen sinnvoll und zumutbar.

Die Frage der nationalen Zuständigkeit bleibt unabhängig vom Urteil der Gerichte zu Street View eine Knacknuss für die Datenschutzbeauftragten. Wie verhält es sich beispielsweise, wenn Anbieter von sozialen Netzwerken ihren Userinnen und Usern Dienstleistungen anbieten, welche die Privatsphäre von Dritten tangieren, die weder informiert wurden noch ihre Zustimmung gaben – wer ist verantwortlich? Der Nutzer, der von den Angeboten Gebrauch macht und dem Netzwerk ungefragt Informationen über Dritte weiter gibt, oder der Anbieter selbst? Und wo ist allenfalls zu klagen? Offene Fragen, die auch im internationalen Kontext noch nicht wirklich geklärt worden sind.

Ferner stellt sich in diesem Zusammenhang auch die Frage, wie die internationale Zusammenarbeit und Koordination zu verbessern wäre. Google hat unter anderem damit argumentiert, dass die Schweiz das einzige Land sei, in dem Google wegen Verletzung des Datenschutzes eingeklagt worden sei, während die Einführung von Street View in über zwei Dutzend anderen Ländern ohne Widerstände vonstatten ging. Auch wenn diese Aussage nicht zutrifft, bleibt dennoch das Faktum, dass die an Street View gestellten Anforderungen je nach Land variierten. Das ermöglicht einem agilen Unternehmen natürlich, seine Produkte zuerst in jenen Ländern einzuführen, in denen mit

keinem oder wenig Widerstand zu rechnen ist. Anschliessend kann es die nachfolgenden Länder mit «vollendeten Tatsachen» unter Druck setzen.

Die Enthüllungen und Aktivitäten von Wikileaks stellten uns vor brisante Fragen. Darf ein uneingeschränktes Transparenzgebot Whistleblower auch dann schützen, wenn sie Personen zu Unrecht angreifen? Wann ist Whistleblowing überhaupt zulässig, wenn Amts- und Geschäftsgeheimnisse auf dem Spiel stehen? Die intensiv geführte Debatte in der Öffentlichkeit hat einiges geklärt. Die öffentliche Verwaltung und die Wirtschaft müssen Voraussetzungen schaffen, damit effektiv festgestellte Missstände aufgedeckt werden können und der Überbringer der schlechten Nachricht nicht «geköpft» wird. Der Bund ist damit vorangegangen und hat klare Regeln aufgestellt. Die kantonalen Verwaltungen haben Nachholbedarf, zum Teil auch die Wirtschaft. Eine anonyme Anschwärzung von Unschuldigen darf nicht akzeptiert werden. Ein Whistleblower muss sämtliche zumutbaren Schritte unternommen, insbesondere die parlamentarischen Aufsichtsgremien informiert haben, bevor er an die Öffentlichkeit gelangt.

Dass ein Öffentlichkeitsbeauftragter, der zugleich Datenschutzbeauftragter ist, zwischen dem Interesse der Öffentlichkeit an grösstmöglicher Transparenz und dem Schutz der Privatsphäre eines Betroffenen die richtige Gewichtung vornehmen kann, hat der Fall Eberle gezeigt. Ein Journalist wollte die Abgangsvereinbarung des ehemaligen Generalsekretärs von alt Bundesrat Blocher einsehen, was das EJPD und das Bundesverwaltungsgericht in einer ersten Runde entgegen unserer Empfehlung ablehnten. Nachdem das Bundesgericht moniert hatte, dass die Vorinstanz keine Güterabwägung der verschiedenen Interessen vorgenommen hatte, hat das Bundesverwaltungsgericht dies nun nachgeholt und ist unserer Einschätzung gefolgt: Im konkreten Fall überwiegen die Interessen der Öffentlichkeit an der Offenlegung der Abgangsentschädigung.

Kurz vor dem Ziel stehen wir – so scheint es – in Bezug auf die Eliminierung des indirekten Auskunftsrechts in Belangen des Staatschutzes. Seit meinem Amtsantritt vor zehn Jahren wiederhole ich regelmässig die Forderung, auch im Staatschutz sollte grundsätzlich das direkte Auskunftsrecht gelten. Das heisst, der Gesuchsteller soll im Regelfall selber Einsicht in die Akten nehmen können, wenn keine Staatschutzinteressen dagegen sprechen. Nachdem das Parlament noch 2010 einen entsprechenden Vorstoss abgelehnt hat, insistiert nun der Bundesrat im Rahmen der «BWIS-Revision reduziert» auf der Einführung eines direkten Einsichtsrechts nach den Regeln von Art. 8 und 9 DSG. Wir sind zuversichtlich, dass nun der Gesetzgeber nach dem Bericht «Datenbearbeitung im Staatsschutzinformationssystem ISIS» seiner Aufsichtskommission – der GPDel – die Rechte der Betroffenen verbessern will. Dieser Bericht hatte nämlich einige ernst zu nehmende Mängel beim Staatschutz offen gelegt und brachte uns eine nie da gewesene Flut von Einsichtsgesuchen. Um der spürbaren Verunsicherung vieler Bürgerinnen und Bürger Rechnung zu tragen, haben wir alles Mögliche unternommen, um

diese Gesuche prioritär zu behandeln. Mit einer massiven Bündelung unserer Kräfte konnten wir sie bis Ende letztes Jahr erledigen. Dabei haben wir auf Grund der speziellen Situation in zahlreichen Fällen von der Ausnahmebestimmung gemäss Art. 18 BWIS Gebrauch gemacht und den Gesuchstellern mitgeteilt, dass sie nicht eingetragen sind.

Die Sensibilisierung von Kindern und Jugendlichen war auch in diesem Jahr ein Schwerpunkt. Dabei ging es uns vor allem auch darum, private Initiativen zu unterstützen. Es kann nicht nur die Aufgabe der öffentlichen Hand sein, die heranwachsende Generation fit für den Umgang mit den neuen Medien zu machen. Wir haben deshalb sehr gerne die multimediale Kampagne «NetLa – meine Daten gehören mir!» als beispielhafte Initiative begleitet und unterstützt. NetLa wurde vom Rat für Persönlichkeitsschutz lanciert und massgeblich von der Privatwirtschaft finanziert. Gemeinsam mit dem Rat haben wir die Kampagne anlässlich des 5. Europäischen Datenschutztages der Öffentlichkeit vorgestellt. Wichtig für uns war, dass sie nicht nur als einmalige Aktion konzipiert ist, sondern das Thema über einen längeren Zeitraum mit verschiedenen Angeboten altersgerecht behandelt und am Ende auch eine Erfolgskontrolle stattfindet.

Abkürzungsverzeichnis

AFAPDP	Association francophone des autorités de protection des données personnelles
AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung
ASTRA	Bundesamt für Strassen
AsylG	Asylgesetz
AUG	Bundesgesetz über die Ausländerinnen und Ausländer, Ausländergesetz
BAFU	Bundesamt für Umwelt
BAG	Bundesamt für Gesundheit
BAV	Bundesamt für Verkehr
BAZL	Bundesamt für Zivilluftfahrt
BEtmG	Bundesgesetz über die Betäubungsmittel und die psychotropen Stoffe
BFM	Bundesamt für Migration
BFS	Bundesamt für Statistik
BGer	Bundesgericht
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung
BIT	Bundesamt für Informatik und Telekommunikation
BJ	Bundesamt für Justiz
BK	Bundeskanzlei
BLW	Bundesamt für Landwirtschaft
BPG	Bundespersonalgesetz
BSV	Bundesamt für Sozialversicherungen
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
BVGer	Bundesverwaltungsgericht
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit

DBA	Doppelbesteuerungsabkommen
DSG	Bundesgesetz über den Datenschutz
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDI	Eidgenössisches Departement des Innern
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFD	Eidgenössisches Finanzdepartement
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EKIF	Eidgenössische Impfkommission
EPA	Eidgenössisches Personalamt
EpG	Epidemiengesetz
ESTV	Eidgenössische Steuerverwaltung
EVD	Eidgenössisches Volkswirtschaftsdepartement
FABER	Fahrberechtigungsregister
fedpol	Bundesamt für Polizei
GAV	Gesamtarbeitsverträge
GEWA	Datenverarbeitungssystem zur Bekämpfung der Geldwäscherei
GK	Gemeinsame Kontrollinstanz Schengen
GPDel	Geschäftsprüfungsdelegation
GPEN	Global Privacy Enforcement Network
ISAS	Informationssystem Äussere Sicherheit
ISIS	Informationssystem Innere Sicherheit
ISP	Information Service Provider, Telekommunikationsdienstleister
JANUS	Gemeinsames Informationssystem der kriminalpolizeilichen Zentralstellen des Bundes
MOFIS	Automatisierte Fahrzeug- und Fahrzeughalterregister

ND-Aufsicht	Nachrichtendienstliche Aufsicht VBS
NDB	Nachrichtendienst des Bundes
N-SIS	Nationaler Teil des Schengener Informationssystems
OECD	Organisation for Economic Co-operation and Development (Oganisation für wirtschaftliche Zusammenarbeit und Entwicklung)
OR	Obligationenrecht
OZD	Oberzolldirektion
PISA	Personalinformationssystem der Armee
PNR	Passenger Name Records, Fluggastdatensätze
RFID	Radio Frequency Identification
RVOG	Regierungs- und Verwaltungsorganisationsgesetz
SAS	Schweizerische Akkreditierungstelle
SBF	Staatssekretariat für Bildung und Forschung
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs
SiaG	Bundesgesetz über den Informationsaustausch zwischen den Strafverfolgungsbehörden des Bundes und denjenigen der anderen Schengen-Staaten
SIS	Schengener Information System
StGB	Schweizerisches Strafgesetzbuch
StPO	Schweizerische Strafprozessordnung
SVG	Strassenverkehrsgesetz
UID	Unternehmens-Identifikationsnummer
UIDG	Bundesgesetz über die Unternehmensidentifikationsnummer
URG	Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz)
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation

VBS	Departement für Verteidigung, Bevölkerungsschutz und Sport
VDSZ	Verordnung über die Datenschutzzertifizierungen
VeöB	Verordnung über die elektronische öffentliche Beurkundung
VüV-ÖV	Verordnung über die Videoüberwachung im öffentlichen Verkehr (Videoüberwachungsverordnung ÖV)
WG	Bundesgesetz über Waffen, Waffenzubehör und Munition
ZEMIS	Zentrales Migrationsinformationssystem
ZGB	Zivilgesetzbuch
ZNDG	Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes

1. Datenschutz

1.1 Grundrechte

1.1.1 Outsourcing im Rahmen der Volkszählung

Im Rahmen der Volkszählung kontrollierten wir ein privates Institut, das im Auftrag des Bundesamts für Statistik (BFS) Personendaten bearbeitet. Grundsätzlich stellten wir fest, dass sich die beteiligten Parteien dafür einsetzen, die datenschutzrechtlichen Vorschriften zu realisieren. Die Kontrolle ist noch nicht abgeschlossen.

Das BFS überträgt die Datenbeschaffung im Rahmen von Erhebungen meist an externe Dienstleistungsunternehmen. Diese Übertragung der Datenbearbeitung an Dritte erzeugt spezielle Risiken aus Sicht des Datenschutzes. Deshalb haben wir im Rahmen der Volkszählung eine Kontrolle der Datenbearbeitungen durchgeführt, die ein privates Marktforschungsinstitut im Auftrag des BFS bei der Abwicklung des Omnibus 2010 vornahm. Die Omnibusstatistiken sind Teil der Volkszählung und liefern zusätzliche Informationen zu aktuellen Fragestellungen. Im vorliegenden Fall wurde die Schweizer Bevölkerung zu Informations- und Kommunikationstechnologien und dem Internetnutzungsverhalten befragt. Das betreffende Institut führt regelmässig Erhebungen für das BFS durch. Wir beabsichtigten mit unserer Kontrolle, eventuell vorhandenes Optimierungspotential aufzuzeigen.

Anhand der von den Parteien eingereichten Dokumentation überprüften wir die verschiedenen Datenbearbeitungsschritte von der Erhebung bis zur Löschung. Einen speziellen Fokus richteten wir einerseits auf die Einhaltung der Vorgaben der Datensicherheit und der Trennung der verschiedenen Erhebungen, anderseits auf die Qualitätssicherungsmassnahmen. Wir besuchten das Institut auch vor Ort und liessen uns gewisse Datenbearbeitungen vorführen.

Wir stellten fest, dass die beteiligten Parteien für datenschutzrechtliche Belange sensibilisiert sind und sich dafür einsetzen, die entsprechenden rechtlichen Vorschriften einzuhalten. Einige unserer Vorschläge zur Optimierung der Datenbearbeitungen wurden von den Parteien angenommen und umgesetzt, so bspw. zur Trennung der Erhebungen und zur symmetrischen Verschlüsselung der Back-ups.

Zu zwei Punkten, die wir kritisiert hatten, konnte noch keine Einigung gefunden werden. Einerseits stellten wir fest, dass die vorgängige Information des BFS an die betroffenen Personen noch verbessert werden kann. Bisher wurden die befragten Personen nicht ausdrücklich über das Bestehen einer Auskunftspflicht informiert. Ein entsprechender Test des BFS, in welchem die Befragten direkt über die Freiwilligkeit informiert

wurden, hatte eine schlechte Rücklaufquote zur Folge. Das BFS wird bei der Durchführung des Omnibus 2011 verschiedene Arten der Information testen. Unsere Kontrolle kann deshalb erst nach Auswertung dieser Tests, voraussichtlich im Spätsommer 2011, abgeschlossen werden.

Anderseits kritisierten wir die Qualitätskontrolle, die durch das private Institut vorgenommen wird. Es beschäftigt für die Durchführung der Erhebung zum grössten Teil nicht fest angestellte Personen in Teilzeitbeschäftigung. Diese müssen jeweils besonders geschult werden, da die Fragestellungen der Interviews, die sie im Rahmen der Erhebungen durchführen, anspruchsvoll sind. Zur Qualitätssicherung überwacht das Institut die Mitarbeitenden, die bei ihrer Einstellung darüber informiert werden und ihre Einwilligung dazu geben. Während der Durchführung der Interviews kann die mit der Überwachung beauftragte Person jederzeit unbemerkt das Telefongespräch mithören und sieht auch die Bildschirmmaske und die Eingaben des Mitarbeitenden. Die Befragten wie auch die Mitarbeiter werden jeweils zu Gesprächsbeginn daran erinnert, dass Dritte das Gespräch mithören könnten, indem zunächst der Disclaimer mit einem entsprechenden Hinweis vorgelesen werden muss. Mitarbeitende, die kontrolliert wurden, erhalten nach Beendigung der Arbeit eine Auswertung der Kontrolle und müssen dazu Stellung nehmen, bevor sie den Arbeitsplatz überhaupt verlassen dürfen.

Uns erscheint eine solcherart ausgeführte Qualitätskontrolle als unverhältnismässig, denn sie erzeugt bei den Mitarbeitenden den Eindruck, ständig überwacht zu werden, selbst wenn tatsächlich vielleicht nur ein kleiner Teil der Gespräche kontrolliert wird. Da diese Art der Kontrolle einen einschneidenden Eingriff in ihre Privatsphäre darstellt, sind wir der Meinung, dass die Angestellten jeweils eindeutig über die bevorstehende Kontrolle resp. das Mithören des Gesprächs informiert werden müssen. Auch müssen die Folgen, die die Auswertungen haben, systematisch und für die Mitarbeitenden klar ersichtlich festgelegt werden.

1.1.2 Volkszählung 2010: Mikrozensus Mobilität und Verkehr

Wir hatten einige Meldungen von Bürgerinnen und Bürgern, welche sich über den Umfang der Mikrozensus-Befragung ärgerten und die Fragen als unverhältnismässigen Eingriff in ihre Privatsphäre empfanden.

Für den Mikrozensus Mobilität und Verkehr wurden etwa 60'000 Haushalte befragt. Der Mikrozensus ist Teil der Volkszählung. Die betroffenen Personen werden computergestützt per Telefon befragt. Wir hatten verschiedene Beschwerden aus der Bevölkerung, die vor allem die Auskunftspflicht, aber auch den Umfang der Fragen betrafen. Im Rahmen unserer Beratungstätigkeit haben wir auf die rechtlichen Rahmenbedingungen der Erhebung hingewiesen, d.h. vor allem auch auf die Tatsache, dass die Teilnahme daran freiwillig ist.

1.1.3 Projekt zur Modernisierung der Ausbildungsstatistik

Die neue AHV-Nummer ist das Kernstück des Projekts zur Modernisierung der Ausbildungsstatistik des Bundesamtes für Statistik (BFS). Die Verwendung dieser Nummer erfordert eine klare Gesetzesgrundlage.

Das BFS hat eine ganze Reihe von Modernisierungsprojekten, unter anderem bei der Ausbildungsstatistik, in Angriff genommen. Bei letzterem geht es namentlich um die Verbesserung der Vergleichbarkeit und der Aktualität der Daten, die Steigerung der Datenqualität sowie die Vereinfachung und Beschleunigung der Abläufe bei der Erfassung und Bearbeitung. Um dieses Ziel zu erreichen, verwendet das BFS konsequent die Verwaltungsdaten der bestehenden Register des Bundes, der Kantone und der Schulen. Die neue 13-stellige AHV-Versichertennummer (AHVN13), ein wesentlicher Bestandteil der Modernisierung, wurde als der allen Registern gemeinsame Personenidentifikator eingeführt. Im Verlauf des vergangenen Jahres haben wir mehrere Anfragen von Bildungseinrichtungen und Schulen erhalten, die sich angesichts dieser Praxis erstaunt und besorgt zeigten. Wir haben daher eine erste summarische Prüfung durchgeführt.

Damit eine generelle Verwendung der AHVN13 als Personenidentifikator möglich ist, muss sie auf einer formellen Gesetzesgrundlage beruhen. Da der rechtliche Rahmen, auf den sich das BFS stützt, wegen der Wechselwirkung zwischen den verschiedenen Gesetzgebungen über die Alters- und Hinterlassenenversicherung, über die Harmonisierung der Register und über die Statistik nicht sehr klar ist, haben wir uns entschlossen, diese Frage nicht nur in Bezug auf die Ausbildungsstatistiken, sondern auch im Rahmen der verschiedenen sonstigen statistischen Erhebungen und Untersuchungen eingehender zu prüfen.

1.1.4 Datenzyklus bei der Unternehmensidentifikationsnummer

Wer «Löschen» sagt, meint nicht immer auch endgültiges Entfernen. Diese altbekannte Tatsache mussten wir im Rahmen der Ämterkonsultation zur Verordnung über die Unternehmensidentifikationsnummer (UID) von Neuem zur Kenntnis nehmen. In unseren beiden Stellungnahmen rieten wir dazu, die Löschung im UID-Register rechtlich klar zu regeln.

Bereits mehrfach haben wir uns kritisch zur Einführung der UID vor allem auch im Bereich Business to Business geäussert. Wir verweisen an dieser Stelle auf die entsprechenden Aussagen in früheren Tätigkeitsberichten.

In der zweiten Ämterkonsultation haben wir das Bundesamt für Statistik (BFS) darauf aufmerksam gemacht, dass in der Verordnung nicht alle Bearbeitungsschritte geregelt sind. Zwar regelt das Bundesgesetz über die Unternehmensidentifikationsnummer (UIDG) die Löschung der UID-Daten auf Gesetzesebene. Dabei ist jedoch die Verwendung des Begriffs «Löschung» irreführend, die Daten werden nämlich nicht gelöscht (d.h. vernichtet), sondern es wird ein Löschungsvermerk angeführt. Die Daten werden anschliessend noch während zehn Jahren im Internet publiziert. In der Botschaft zum Gesetz wird dazu weiter ausgeführt, UID-Stellen hätten auch nach Ablauf der zehnjährigen Frist Zugriff auf die Daten.

Der Grundsatz der Verhältnismässigkeit verlangt, dass nicht mehr benötigte Daten vernichtet, d.h. unwiderruflich gelöscht werden. Die genannten rechtlichen Grundlagen regeln diesen letzten Abschnitt einer Datenbearbeitung nur unzureichend. Es gibt aber auch sachliche Gründe, die gegen die Verwendung des Begriffs Löschung in diesem Bereich sprechen. Mittelfristig soll die Unternehmensidentifikationsnummer nämlich alle anderen administrativen Nummern ablösen. Die Handelsregisternummer als solches Beispiel wird auch nie wirklich gelöscht, die Einträge über die Unternehmen bestehen im Handelsregister zeitlich unbeschränkt weiter.

Wir beantragten demzufolge, die Löschung im UID-Register in den rechtlichen Grundlagen klar und transparent zu regeln. Das BFS hat diesem Anliegen zu einem späteren Zeitpunkt entsprochen.

1.1.5 Entwicklung der Zertifizierung von Produkten und Dienstleistungen

Infolge der im Bereich der Zertifizierung von Produkten und Dienstleistungen aufgetretenen Schwierigkeiten haben wir beschlossen, unsere diesbezüglichen Tätigkeiten vorübergehend einzustellen. Wir haben das Bundesamt für Justiz um eine Klärung gewisser Fragen zur Gesetzgebung ersucht.

Vertreter eidgenössischer und kantonaler Stellen sowie verschiedener in den Bereichen Informatik, Finanzen und Gesundheit, Zertifizierung und Akkreditierung tätiger Privatunternehmen kamen im Frühjahr 2010 zu einer Bestandesaufnahme zur Zertifizierung von Produkten und Dienstleistungen zusammen. Die Arbeitsgruppe gelangte zum Schluss, dass eine Zertifizierung von Informatikprodukten (Hard- und Software), gestützt beispielsweise auf den Anforderungskatalog «European Privacy Seal» (EuroPriSe) – unter finanziellen Gesichtspunkten – in einem kleinen Markt wie dem unseren kaum in Frage käme, und dass ihr ausserdem verschiedene technische und rechtliche Hindernisse im Wege ständen. Überdies äusserten mehrere Teilnehmer das Bedürfnis nach der Einführung einer Zertifizierung von Dienstleistungen, die eine Bearbeitung von Personendaten mit sich bringen. Technisch gesehen wäre eine solche Zertifizierung ohne weiteres realisierbar, zum Beispiel durch eine Ausweitung der Norm ISO/IEC 20000 für Service-Managementsysteme auf den Datenschutz, wie das bei der Zertifizierung von Organisationen geschehen ist, die auf der Grundlage von ISO/IEC 27001 erfolgreich durchgeführt wurde. Vom juristischen Standpunkt aus stellt indessen die Zertifizierung von Dienstleistungen den Auftraggeber oder Leistungsbezüger, der grundsätzlich der Inhaber der Datensammlung ist, dem Auftragnehmer oder Leistungserbringer, also einem Dritten im Sinne von Artikel 10a Absatz 2 des Datenschutzgesetzes (DSG) gegenüber. Gemäss dieser Bestimmung muss sich der Auftraggeber insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet, was als Aufforderung zur Zertifizierung des Dritten in Sachen Informationssicherheit (ISO/IEC 27001) verstanden werden kann. Da jedoch der Auftraggeber für die Einhaltung der Grundsätze des Datenschutzes verantwortlich ist (gegebenenfalls über eine Organisationszertifizierung), ist eine Zertifizierung im Bereich des Datenschutzes für den Leistungserbringer schwerlich denkbar.

Es muss auch festgestellt werden, dass die geltende Gesetzgebung Lücken oder Ungenauigkeiten aufweist: Artikel 11 Absatz 1 DSG sieht nur die Zertifizierung von Systemen, nicht aber von Dienstleistungen vor; Artikel 5 der Verordnung über die Datenschutzzertifizierungen (VDSZ), der die Zertifizierung von Produkten regelt, könnte durch eine neue Bestimmung betreffend die Zertifizierung von Dienstleistungen ersetzt oder

ergänzt werden. In Artikel 11 Absatz 2 DSG wiederum heisst es, der Bundesrat erlasse Vorschriften über die Einführung eines Datenschutz-Qualitätszeichens; in der Verordnung wurde jedoch keine solche Bestimmung vorgesehen.

Angesichts dieser Probleme und unter Berücksichtigung der Tatsache, dass unsere Nachbarländer wie Deutschland und Frankreich ebenfalls Schwierigkeiten haben, eine Zertifizierung von Produkten und/oder Dienstleistungen einzuführen, haben wir im Sommer 2010 beschlossen, unsere Arbeiten in diesem Bereich vorläufig einzustellen. Wir haben das Bundesamt für Justiz um eine Klärung der Gesetzesfragen, gegebenenfalls im Rahmen der Revision des DSG, gebeten.

1.2 Datenschutzfragen allgemein

1.2.1 Via sicura

Das Handlungsprogramm des Bundes für mehr Sicherheit im Strassenverkehr weist aus Sicht des Datenschutzes verschiedene Schwachpunkte auf. Wir regten Verbesserungen insbesondere in den Bereichen Anonymisierung, Bekanntgabe der Daten und Blackbox-Aufzeichnungen an.

Wir hatten Gelegenheit, zum Handlungsprogramm des Bundes für mehr Sicherheit im Strassenverkehr und zur vorgesehenen Revision des Strassenverkehrsgesetzes (SVG), kurz Via sicura, Stellung zu nehmen. Aus datenschutzrechtlicher Sicht gibt es verschiedene heikle Punkte.

Zunächst soll nun mit der Revision die formell-gesetzliche Grundlage für das Strassenverkehrsunfallregister geschaffen werden. Teil dieses Registers bildet das Auswertungsregister, mit dem Statistiken erstellt werden sollen (vgl. Ziff. 1.2.5 unseres 17. Tätigkeitsberichts 2009/2010). Der Entwurf des revidierten SVG regelt abgesehen von der Strassenverkehrsunfall-Statistik neu auch noch die Strassenverkehrskontroll-Statistik. In beiden Fällen werden die Daten in pseudonymisierter Form (mittels PIN) in den Auswertungsregistern erfasst. Dank des PIN und der Verknüpfung mit anderen Informationssystemen des Bundesamtes für Strassen (ASTRA) kann jederzeit auf die effektiven Personendaten zurückgegriffen werden. Wir sind daher der Auffassung, dass die Daten nicht in pseudonymisierter, sondern von Anfang an in anonymisierter Form in den Auswertungsregistern erfasst werden müssten. Zumindest wäre es wichtig, die pseudonymisierten Daten möglichst rasch wieder zu löschen resp. zu anonymisieren.

Der Entwurf gibt dem Bundesrat sodann die Möglichkeit, auf Verordnungsstufe vorzusehen, dass den Motorfahrzeug-Haftpflichtversicherungen Auskunft betreffend Administrativmassnahmen gegen einzelne Versicherte erteilt werden kann. Die Botschaft hält aber ausdrücklich fest, dies sei für die Verkehrssicherheit nicht zwingend erforderlich und nur in Einzelfällen rechtens. Zudem möchte der Bundesrat «im Gegenzug» die Unfalldaten der Versicherungen erhalten, um genauere Statistiken erstellen zu können. Wir wiesen darauf hin, dass solche Gegengeschäfte nicht zulässig sind – entweder sind die (datenschutzrechtlichen) Voraussetzungen für die Bekanntgabe von Daten an die Versicherer gegeben, oder sie sind es nicht. Dann ist aber eine Datenbekanntgabe nicht rechtens.

Weiter soll mit der Revision die formale Konsolidierung der bestehenden Informationssysteme erfolgen. Die vier bestehenden Register MOFIS, FABER, ADMAS und TARGA werden mit anderen Worten in einer einzigen Datenbank für die

Verkehrszulassung zusammengeführt. Diese Änderung wurde in letzter Minute eingefügt. Wir bedauerten, dass dafür nur eine Ämterkonsultation mit verkürzter Frist und keine externe Vernehmlassung durchgeführt wurde. Unseres Erachtens wäre es wichtig gewesen, diese Vorlage noch einmal sorgfältig zu prüfen, um sicherzustellen, dass bei der Zusammenführung der gesetzlichen Grundlagen Zweck, Zugriffe, bearbeitete Datenkategorien, Abrufverfahren und andere datenschutzrechtlich relevante Aspekte für die einzelnen Informationssysteme tatsächlich gleich bleiben. Für uns war auch die technische Umsetzung nicht klar; ob beispielsweise die heute bestehenden Register als (Sub-)Systeme wirklich technisch tel quel bestehen bleiben sollen. Unseres Erachtens hätte diese Konsolidierung auch in den Erläuterungen respektive in der Botschaft näher ausgeführt werden müssen. Wir begrüssen allerdings, dass die Datensammlung der Verkehrszulassung im Entwurf als nicht-öffentlich bezeichnet wird und die Halter- und Versicherungsdaten nur unter bestimmten Voraussetzungen an Dritte bekannt gegeben werden dürfen.

In der Botschaft wurde zudem korrekterweise darauf hingewiesen, dass der Einsatz von Datenaufzeichnungsgeräten (Blackboxen) tief in die Privatsphäre eingreift. Daher begrüssten wir die ausdrückliche gesetzliche Bestimmung, dass die Aufzeichnungen der Blackbox ausschliesslich der Kontrolle der Geschwindigkeit dienen dürfen. Für uns stellte sich noch die Frage, ob dafür auch der jeweilige Standort aufgenommen werden müsse, wodurch ein Bewegungsprofil entstehen könnte. Auf jeden Fall sollte in der Bundesratsverordnung unter anderem sorgfältig geprüft werden, welche Daten für den verfolgten Zweck überhaupt nötig und geeignet sind und wie lange diese aufbewahrt werden dürfen.

Hinsichtlich der Fahreignungsprüfung vertraten wir die Auffassung, dass kantonale IV-Stellen resp. Ärztinnen und Ärzte eine allfällige Fahruntüchtigkeit nicht direkt an das Strassenverkehrsamt, sondern zuerst an eine ärztliche Stelle melden müssten.

Via sicura kommt nun ins Parlament.

1.2.2 Personendatenbearbeitung bei der Abschnittsgeschwindigkeitskontrolle

Das Bundesamt für Strassen (ASTRA) führte Tests mit der so genannten Abschnittsgeschwindigkeitskontrolle durch und unterbreitete uns das Projekt im Vorfeld. Aus datenschutzrechtlicher Sicht hatten wir nichts gegen diese Art der Kontrolle, wie sie uns vorgestellt wurde, einzuwenden.

Das ASTRA hat uns die Unterlagen für die geplanten Abschnittsgeschwindigkeitskontrollen (AGK) auf Nationalstrassen im Vorfeld der Tests zur Stellungnahme unterbreitet. Als Standorte wurden der Arisdorftunnel auf der A2 sowie eine Strecke im Kanton Waadt auf der A9 gewählt. AGK überwachen nicht wie herkömmliche Radaranlagen die Einhaltung der Geschwindigkeit an einem einzigen Punkt, sondern über einen längeren Abschnitt. In einer ersten Phase wurden Tests zur Funktionsfähigkeit der neuen Messgeräte durchgeführt, wobei allfällige Übertretungen noch nicht gebüsst wurden.

Aus datenschutzrechtlicher Sicht hatten wir nichts gegen diese AGK einzuwenden. So werden zwar am Anfang und am Ende des überwachten Abschnitts sämtliche Fahrzeuge fotografiert, jedoch nur von hinten. Zudem werden die Daten sämtlicher Fahrzeuge, die korrekt fahren, wieder gelöscht, ohne an Dritte weitergegeben oder mit anderen Informationssystemen abgeglichen zu werden. Fahrzeuge, welche die Geschwindigkeit übertreten, werden hingegen automatisch auch von vorne fotografiert. Nur diese Daten werden dann der zuständigen Kantonspolizei weitergeleitet.

1.2.3 Videoüberwachung gemäss Eisenbahn- und Personenbeförderungsgesetz

Das revidierte Eisenbahngesetz sowie das revidierte Personenbeförderungsgesetz enthalten seit dem 1. Januar 2010 je eine ausdrückliche formellgesetzliche Grundlage für die Videoüberwachung. Konzessionierte Tätigkeiten fallen neu unter das DSG.

Auf den 1. Januar 2010 traten das revidierte Eisenbahngesetz sowie das revidierte Bundesgesetz über die Personenbeförderung in Kraft. Beide Gesetze gelten für Unternehmen mit einer Bundeskonzession und halten ausdrücklich fest, dass für die konzessionierten Tätigkeiten das DSG anwendbar ist. Daraus folgt, dass die kantonalen Datenschutzgesetze für diese Bereiche nicht gelten. Weiter besteht nun mit diesen beiden Gesetzen auch eine ausdrückliche formellgesetzliche Grundlage für die Videoüberwachung. Einzelheiten werden in der Verordnung über die Videoüberwachung im öffentlichen Verkehr geregelt. Sie besagt, dass für die Videoüberwachung bei der

regelmässigen und gewerbsmässigen Personenbeförderung auf Schienen, auf der Strasse und auf dem Wasser das DSG anwendbar ist und nicht die kantonalen Datenschutzgesetze gelten. Damit sind neu wir und nicht mehr die kantonalen Datenschutzbehörden für die Videoüberwachung im öffentlichen Verkehr zuständig.

Ein weiterer Bericht zum Thema Videoüberwachung im öffentlichen Verkehr befindet sich in Ziff. 1.6.2.

1.2.4 Biometrische Zugangssysteme beim Sportzentrum KSS: Abschluss des Verfahrens

Das Sportzentrum KSS musste die zentralisierte Speicherung biometrischer Daten im Rahmen seiner Zutrittskontrolle aufgrund eines Urteils des Bundesverwaltungsgerichts anpassen. Wie wir anlässlich einer Nachkontrolle vor Ort feststellen konnten, setzt KSS das Urteil datenschutzkonform um.

Nachdem das Bundesverwaltungsgericht in seinem Urteil vom 4. August 2009 die zentralisierte Speicherung biometrischer Daten im Rahmen der Zutrittskontrolle zu einem Sport- und Freizeitzentrum als eine unverhältnismässige Persönlichkeitsverletzung der Betroffenen erachtet hat (vgl. unseren 17. Tätigkeitsbericht 2009/2010, Ziff. 1.2.2), ist das Sportzentrum KSS daran, sein Zutrittssystem anzupassen. Künftig werden die biometrischen Daten zwar noch immer zentralisiert gespeichert. Der Bezug zu weiteren vom Sportzentrum erhobenen Personendaten ist jedoch unterbrochen und kann nur mit Hilfe der Abonnementskarte hergestellt werden. Diese befindet sich im Besitz des Kunden. Die zentral gespeicherten Templates (codiert gespeicherte biometrische Rohdaten) werden dynamisch verschlüsselt. Ihre Entschlüsselung ist nur mit Hilfe der Abonnementskarte möglich, da ein Teil des Schlüssels auf dieser Karte gespeichert ist.

Auf der Karte ist ein Code gespeichert, der die Zuordnung der biometrischen Daten zu weiteren Personendaten (Personalien und weitere Nutzerdaten) überhaupt erst ermöglicht. Nur wenn der Kunde seine Karte in das Lesegerät einlegt, kann anhand des auf der Karte gespeicherten Zuordnungscodes das zum Kunden gehörende Fingerabdruck-Template geladen, entschlüsselt und mit dem am Lesegerät eingelesenen Fingerabdruck verglichen werden. Zudem ist nur in diesem Moment eine Zuordnung zu den Kunden- und Abonnementsdaten möglich. Sobald die Karte aus dem Lesegerät entfernt wird, ist die Verbindung zwischen den einzelnen Datensätzen wieder unterbrochen; sie kann vom Sportzentrum KSS nicht anderweitig (z.B. via Zeitstempel) wieder hergestellt werden.

Damit kann das Template zwar theoretisch noch immer einer Person zugeordnet werden, da es selbst ein Personendatum ist. Diese Zuordnung ist jedoch ohne

Abonnementskarte nach heutigem Stand der Technik faktisch nicht möglich. Mit dem oben geschilderten Prozedere wird erreicht, dass die Kunden jede Verwendung ihrer biometrischen Daten explizit und bewusst freigeben müssen und damit weitestgehende Kontrolle darüber haben. Das Sportzentrum KSS hat keinen Zugriff auf die biometrischen Daten bestimmter Personen, ein mit einer dezentralen Datenspeicherung vergleichbarer Effekt.

Wir haben dieses neue System einer Kontrolle unterzogen und dabei festgestellt, dass die Fingerabdruck-Templates nun wie oben beschrieben von den übrigen Personendaten getrennt sind. Ausserdem besteht für alle Kunden die Möglichkeit, eine Dauerkarte ohne Verwendung zentral gespeicherter biometrischer Daten zu erwerben. Bei diesen Dauerkarten wird eine Gesichtsfotografie auf die Karte gedruckt, die es dem Kassenpersonal erlaubt, den Inhaber durch eine einfache Sichtkontrolle zu identifizieren. Die Fotos werden dabei nirgends zentral gespeichert. Mit dieser Alternative hat jeder Badegast die Wahl, der zentralisierten Speicherung seiner biometrischen Daten zuzustimmen oder auf die (weniger komfortable) Fotokarte auszuweichen.

Das geänderte System setzt damit die zwei zentralen Punkte des Urteils des Bundesverwaltungsgerichts um: Zum Einen basiert die Verwendung der biometrischen Daten auf einer rechtsgültigen Einwilligung, da diese nun freiwillig erfolgt. Zum Anderen wurde der durch diese Datenbearbeitung verursachte Eingriff in die Persönlichkeit der Betroffenen auf ein Minimum reduziert. Wir sind daher zum Schluss gelangt, dass das biometrische Zutrittssystem des Sportzentrums KSS nach der vollständigen Umsetzung dieser Änderungen datenschutzkonform ausgestaltet ist.

Damit ein reibungsloser Badebetrieb aufrechterhalten werden kann, wird das Sportzentrum das neue System nun laufend umsetzen. Noch gültige Abonnementskarten werden beibehalten. Alle neuen oder verlängerten Abonnemente laufen aber ab sofort auf dem neuen System, so dass bis in zwei Jahren alle Abonnemente umgestellt sein sollten.

1.2.5 Zentrale Speicherung von Kundenfotos bei Skistationen

Da die in vielen Skistationen praktizierten Zugangskontrollen mittels Fotoabonnementskarten bei einigen Kunden auf Widerstand gestossen sind, prüfen wir zurzeit die Datenschutzkonformität solcher Systeme.

Die meisten Schweizer Skistationen verwenden Zugangskontrollsysteme, bei denen eine Gesichtsfotografie des Kunden zentral gespeichert und bei jedem Passieren eines Drehkreuzes auf dem Bildschirm des Kontrollpersonals angezeigt wird. Bei diesen Systemen findet kein automatisierter Vergleich zwischen dem Foto und der anwesenden Person statt, weshalb sie keine biometrischen Erkennungssysteme darstellen.

Dennoch sind Gesichtsfotografien biometrische Rohdaten und zählen zu den besonders schützenswerten Personendaten, die nun in den Skistationen zentral gespeichert werden. Es sind daher besondere Anforderungen an die Datenbearbeitung zu stellen, insbesondere im Bereich der Datensicherheit.

Um auf die diesbezüglichen Bedenken betroffener Abonnementsinhaber einzugehen, haben wir beschlossen, diese Zugangskontrollsysteme einer Prüfung zu unterziehen und uns eine Anlage vorführen zu lassen. Wir sind derzeit dabei, die gesammelten Daten zu analysieren.

1.2.6 Biometrisches Erkennungssystem für die Reservation von Sportplätzen

Ein Tennisclub hat ein neues Reservationssystem mit biometrischer Personenerkennung eingeführt. Neu muss jedes Mitglied seine Tennisplatzreservation mittels Fingerabdruck bestätigen, damit der Platz bespielt werden darf. Aufgrund von Anfragen besorgter Clubmitglieder haben wir das System einer Kontrolle unterzogen und dabei festgestellt, dass es den datenschutzrechtlichen Anforderungen nicht entspricht und angepasst werden muss. Wir haben eine entsprechende Empfehlung erlassen und prüfen zurzeit zusammen mit dem Club, wie diese umgesetzt werden kann.

Ein Tennisclub hatte in der Vergangenheit das Problem, dass immer wieder Unbefugte die Tennisplätze benutzten. Die Clubanlage ist unübersichtlich, nur schlecht gegen fremde Zutritte gesichert und verfügt über keine ständig besetzte Reception, so dass schwer kontrollierbar ist, wer auf den Plätzen spielt. Ein zur Verhinderung unbefugter Zutritte eingeführtes Reservationssystem mit Verifizierung mittels PIN nützte nur unzureichend, da diese unrechtmässig an Nichtmitglieder weitergegeben wurden. Aus diesem Grund hat der Club ein System eingeführt, das die Zutrittsberechtigung der Spieler mittels Fingerabdruck verifiziert. Die Fingerabdruck-Templates werden hierbei zentral auf einem Computer gespeichert, so dass kein Mitgliederausweis mitgeführt werden muss.

Auf Hinweis einzelner Mitglieder haben wir die Anlage einer Kontrolle unterzogen und sind zu folgendem Ergebnis gekommen: Die Verwendung biometrischer Daten zur Verifizierung der zahlenden Clubmitglieder ist zwar durch ein überwiegendes privates Interesse gerechtfertigt. Es handelt sich aber um ein Verifizierungssystem bei einer Freizeitanlage, bei dem eine zentrale Speicherung biometrischer Daten nicht notwendig und daher grundsätzlich unverhältnismässig ist (vgl. unsere Ausführungen zum Fall KSS im 17. Tätigkeitsbericht 2009/2010, Ziff. 1.2.2). Die vom Tennisclub angeführten Gründe für

die Zentralisierung (Wirtschaftlichkeit und Komfort) sind als Rechtfertigung für eine unverhältnismässige Datenbearbeitung ungenügend. Wir sind daher zum Schluss gelangt, dass der Tennisclub sein Reservationssystem anpassen muss.

Gemäss der von uns in diesem Fall erlassenen Empfehlung an den Club sehen wir folgende Möglichkeiten, die Datenspeicherung bei einem Verifizierungssystem in einer Freizeitanlage datenschutzkonform auszugestalten: Die beste Lösung besteht darin, die biometrischen Daten vollkommen dezentral auf einem Datenträger zu speichern, welcher der Kontrolle der betroffenen Personen unterliegt (z.B. auf der Mitgliederkarte). Eine weitere Möglichkeit besteht darin, die biometrischen Daten zwar zentral zu speichern, hierbei aber nur Templates und keine Rohdaten (z.B. Fingerabdruckbilder oder Fotografien) zu verwenden und die Daten vor der Speicherung zu verschlüsseln. Die Daten müssen zudem getrennt von weiteren, die fraglichen Personen betreffenden Angaben (z.B. den Personalien) gespeichert werden. Der Bezug zu einer bestimmten Person soll einzig durch deren bewusste und explizite Freigabe mit Hilfe einer persönlichen Karte hergestellt werden können (vgl. die Ausführungen zum Abschluss des Verfahrens KSS in Ziff. 1.2.4 des vorliegenden Tätigkeitsberichts). Wird eine Lösung ohne Karte angestrebt, ist eine zentrale Datenspeicherung unumgänglich. Dies ist aber nur dann zulässig, wenn keine Rohdaten gespeichert und nur biometrische Charakteristika verwendet werden, die keine physischen oder digitalen Spuren hinterlassen (also z.B. Fingervenen oder Handumriss, nicht aber z.B. Fingerabdrücke). Die Daten sind auch hier verschlüsselt und ohne Bezug zu weiteren Personendaten zu speichern.

Daneben war beim Tennisclub zu beanstanden, dass die Massnahmen zur Datensicherheit der Sensibilität biometrischer Daten keineswegs angemessen waren. So befindet sich der Server in einem von aussen her zugänglichen und nur rudimentär gegen Einbruch gesicherten Raum. Die Datenübertragung erfolgt zudem drahtlos via ein Funknetzwerk, das allen Mitgliedern für den Zugang zum Internet auf dem Clubgelände zu Verfügung steht. Damit wären sowohl ein physischer als auch ein digitaler Zugang zu den fraglichen Daten für Unberechtigte zu leicht möglich. Biometrische Daten müssen jedoch besonders geschützt werden. Wir haben daher die Empfehlung erlassen, die Datensicherheit beim Tennisclub müsse durch geeignete technische Massnahmen erhöht werden. Aus demselben Grund sind auch die Zugangs- und Zutrittsberechtigungen der Mitarbeitenden und der Mitglieder genau und restriktiv zu regeln.

Wir prüfen zurzeit zusammen mit dem Tennisclub, welche Variante der Datenspeicherung umgesetzt werden kann und welche konkreten technischen und organisatorischen Massnahmen nötig sind, damit die Datensicherheit gewährleistet ist.

1.2.7 Nacht- und Jugendclubs: Schwarze Listen und Biometrie

Diverse Nacht- und Jugendlokale suchen nach Möglichkeiten, Personen mit Hausverbot bereits am Eingang zu erkennen und abzuweisen. Wir haben daher in diesem Jahr verschiedene Projekte begutachtet, die sich mit der Verwendung biometrischer Erkennungssysteme zur Identifizierung der in Blacklists erfassten Delinquenten beschäftigen. Insbesondere der in diesem Zusammenhang geplante Datenaustausch zwischen den Lokalbetreibern ist aus datenschutzrechtlicher Sicht problematisch.

Nacht- und Jugendlokale haben immer wieder Probleme mit Personen, die bspw. durch übermässigen Alkoholkonsum, Gewalttätigkeit oder Diebstähle auffallen. Gegen solche Lokalbesucher ausgesprochene Hausverbote sind nur schlecht durchsetzbar, da die fraglichen Personen am Eingang teilweise nicht erkannt werden. Ausserdem weichen auffällige Gäste nach Erhalt eines Hausverbots auf andere Lokale aus, wo sie erneut Probleme verursachen. Lokalbetreiber suchen daher nach Lösungen, die eine Erkennung der fehlbaren Personen bereits am Eingang ermöglichen.

Die bei uns zur Prüfung eingereichten Projekte weisen folgendes Grundmuster auf: Wer ein Hausverbot erhält, wird mit Personalien, Gesichtsfotografie sowie Grund und Länge des Hausverbotes in einer zentralen Datenbank (der eigentlichen Blacklist) gespeichert. Als Variante werden sämtliche Clubgäste in die Datenbank aufgenommen (System Memberclubs) und solche mit Hausverbot speziell gekennzeichnet. Am Eingang werden alle Personen entweder durch einfache Sichtkontrolle mit Hilfe einer Memberkarte oder durch eine Videokamera mit automatisierter Gesichtserkennung überprüft. Personen mit Hausverbot können so bereits am Eingang erkannt und abgewiesen werden. Diese Systeme sollen im Verbund betrieben werden. Alle an das System angeschlossenen Lokale könnten damit auf sämtliche in der zentralen Datenbank gespeicherten Daten zugreifen. Auf diese Weise könnten auch Personen erkannt werden, die in anderen Lokalen auffällig geworden sind. Memberclubs können die Daten gemäss Konzept zudem zu Werbzwecken oder für Kundenbindungsprogramme verwenden und austauschen.

Unsere datenschutzrechtliche Beurteilung hat Folgendes ergeben: Bei diesen Systemen werden (besonders schützenswerte) Personendaten bearbeitet und ausgetauscht. Dafür muss ein überwiegendes privates Interesse gegeben sein und müssen die Bearbeitungsgrundsätze, insbesondere die Verhältnismässigkeit, eingehalten werden. Die Bearbeitung von Personendaten zur Durchsetzung des Hausrechts und im Interesse der Sicherheit ist vor diesem Hintergrund unbedenklich, sofern genau definiert ist, wann eine Person erfasst wird, und die erfassten Daten nur für diese Zwecke verwendet werden.

Anders stellt sich die Situation beim Austausch der fraglichen Daten zwischen den angeschlossenen Clubbetreibern dar. Auch hier muss ein überwiegendes privates Interesse gegeben sein. Das wäre etwa dann der Fall, wenn von einer Person mit einiger Sicherheit angenommen werden muss, dass sie sich auch an anderen Orten unkorrekt verhalten wird. Bei einem automatisierten Abfrageverfahren und damit einem automatischen Datenaustausch zwischen den Clubbetreibern kann aber nicht geprüft werden, ob ein solches Interesse im konkreten Einzelfall besteht. Es dürfen daher nur diejenigen Personen in die Datenbank aufgenommen werden, gegen die objektiv ein derartiger Verdacht besteht, damit ein Interesse am Datenaustausch in jedem einzelnen Fall von vornherein gegeben und die Weitergabe verhältnismässig wäre. Besucher, die aufgrund eines persönlichen Konflikts mit dem Barpersonal oder dem Lokalbetreiber ein Hausverbot erhalten, dürfen beispielsweise nicht in die Datenbank aufgenommen werden. Dadurch würde die Datenbank für die einzelnen Clubs aber unvollständig, was ihren Zweck stark untergraben würde. Wir empfehlen daher, auf den automatischen Datenaustausch zu verzichten und Daten nur in begründeten Einzelfällen weiterzugeben.

Werden die Daten sämtlicher Clubgäste registriert und zu Werbezwecken oder für Kundenbindungsprogramme verwendet, so dient dies weder der Sicherheit noch der Wahrung des Hausrechts. Vielmehr stehen rein wirtschaftliche Interessen im Vordergrund, die weniger schwer wiegen als der Persönlichkeitsschutz. Daher muss die Teilnahme an Werbeaktionen und Kundenbindungsprogrammen freiwillig sein. Die Einwilligung der Betroffenen müsste sich hier auch explizit auf einen allfällig vorgesehenen Datenaustausch zwischen den Lokalen beziehen.

Wir haben den Beteiligten unsere Standpunkte in einer Stellungnahme zukommen lassen und werden die Projekte einer genaueren Überprüfung unterziehen, sobald die Detailplanung vorliegt.

1.2.8 Datenschutzkonformität des Frequenzmeters

Das Frequenzmeter ist eine technische Lösung, die videobildgestützt ermittelt, mit welcher Häufigkeit Fussgänger oder Fahrzeuge eine bestimmte Stelle passieren. Da hierbei auch Personen oder Objekte, die einer bestimmten Person zugeordnet werden können, erfasst werden, handelt es sich um eine Bearbeitung von Personendaten. Daher haben wir das Frequenzmeter auf seine Datenschutzkonformität hin geprüft und sind zum Schluss gelangt, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden.

Das Frequenzmeter besteht aus einem Mini-PC, einem USB-Speicherstick und einer Videokamera, die miteinander verbunden sind. Die Ermittlung der Frequenzdaten erfolgt über die Kamera, ohne dass jedoch Bilddaten über längere Zeit gespeichert werden. Mittels Software wird in einem beliebigen Bereich des Aufnahmefeldes der Kamera eine virtuelle Lichtschranke errichtet. Zwei aufeinander folgende Videobilder werden fortlaufend in einem flüchtigen Speicher miteinander verglichen. Findet im Bereich der virtuellen Lichtschranke eine Bildveränderung statt, wird das als ein die fragliche Stelle passierendes Objekt gewertet. In einer Datenbank wird dies daraufhin entsprechend eingetragen. Danach werden die Videobilder durch zwei neue überschrieben. Eine Objekterkennung findet nicht statt. Die in der Datenbank gespeicherten Daten sind damit ohne Personenbezug.

Dieser Vorgang findet 25 Mal pro Sekunde statt. Dadurch, dass die Videobilder fortlaufend überschrieben und die letzten beiden Bilder bei Programmende sofort gelöscht werden, wird das einzelne Bild nur gerade für einen Sekundenbruchteil gespeichert. Diese extrem kurze Speicherdauer potentiell personenbezogener Daten ermöglicht keine weitergehende Bearbeitung.

Wenngleich auf dem durch die Kamera erzeugten Bild Personen erkennbar und teilweise sogar identifizierbar sind, schätzen wir die Intensität dieser Datenbearbeitung aufgrund der extrem kurzen Speicherdauer und der fehlenden Möglichkeiten einer weitergehenden Bearbeitung als gering ein. Wir gehen daher davon aus, dass durch das Frequenzmeter keine widerrechtliche Persönlichkeitsverletzung stattfindet.

1.2.9 Bekanntgabe von AHV-Daten an Verwertungsgesellschaften

Mit der Teilrevision des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG) soll die Urheberrechtsverwertungsgesellschaft ProLitteris Auszüge aus dem AHV-Register erhalten, um die Gebühren effizienter erheben zu können.

Im Jahr 2007 gelangte das Institut für geistiges Eigentum mit dem Begehren der ProLitteris an uns, Daten aus dem AHV-Register beziehen zu können. Wir wiesen darauf hin, dass es für eine Datenbekanntgabe aus dem Register an die Verwertungsgesellschaft eine gesetzliche Grundlage braucht. In der Folge wurde mit der Motion Stadler unter dem Titel «Copyright-Vergütungen für Urheber statt Prozesse» die Anpassung des AHVG vorgeschlagen.

Im Rahmen der Ämterkonsultation zur Revision der entsprechenden Bestimmung, des Artikels 50a AHVG, haben wir unsere Vorbehalte zur Ausgestaltung der neu vorgesehenen gesetzlichen Grundlage geäussert. Wir bemängelten vor allem die erweiterte Zweckbestimmung der durch die Ausgleichskassen erhobenen Daten, zusammen mit der Abkehr von der im Urheberrecht verankerten Pflicht zur Selbstdeklaration durch die Werknutzer. Wir sind der Meinung, dass der Systemwechsel von dieser Selbstdeklaration zur automatischen Datenbekanntgabe (Name, Adresse, Branchenzugehörigkeit und Mitarbeiteranzahl der Firma) durch die Ausgleichskassen an Verwertungsgesellschaften auch im Urheberrechtsgesetz (URG) angepasst werden müsste. Bleibt anzumerken, dass es auf der Basis der übermittelten AHV-Daten nur dann möglich ist, die Urheberrechtsgebühren korrekt zu berechnen, wenn die Stellenprozente bekannt sind. Die Ausgleichskassen verfügen jedoch nur über Informationen zur Anzahl der Mitarbeiter.

Der Abschluss der Vernehmlassung zur Teilrevision ist für Juni 2011 geplant.

1.2.10 Teilrevision des Immobiliarsachenrechts

Im Rahmen der Teilrevision des Immobiliarsachenrechts wurden wir zu einer Ämterkonsultation über die neuen Entwürfe der Ausführungsverordnungen eingeladen. Unsere Eingaben zielten u. a. darauf ab, die Risiken des elektronischen Grundstückindexes zu minimieren und zu Datensparsamkeit aufzurufen.

Die Teilrevision des Immobiliarsachenrechts hat Auswirkungen auf Verordnungsstufe, namentlich im Hinblick auf die Einführung des Register-Schuldbriefs, die Ausdehnung der Beurkundungspflicht für Dienstbarkeiten und Pfandrechte, sowie die neue Regelung über die Anmerkung öffentlich-rechtlicher Eigentumsbeschränkungen. Im

Rahmen dieser Teilrevision konnten wir zu den Entwürfen der neuen Grundbuchverordnung und der Verordnung über die elektronische öffentliche Beurkundung (VeöB) Stellung nehmen. Es ist vorgesehen, dass die Verordnungen auf den 1. Januar 2012 in Kraft treten.

Die neue Grundbuchverordnung ist inhaltlich auf die Grundbuchführung mittels Informatik ausgerichtet. Der Entwurf sieht bereits die nötigen Fundamente für die Einführung des elektronischen Geschäftsverkehrs mit den Grundbuchämtern vor. Die entsprechenden Belege können auch in elektronischer Form nach VeöB eingereicht werden. Gemäss dieser neuen Verordnung kann jede Person vom Grundbuchamt ohne das Glaubhaftmachen eines Interesses Auskunft unter anderem über sämtliche Anmerkungen verlangen. Wir haben hier angeregt, dass die bisherigen Ausnahmen, um des Persönlichkeitsschutzes von betroffenen Grundeigentümern Willen, auch in der neuen Grundbuchverordnung aufgeführt werden. Es geht hier insbesondere um Grundbuchsperren, deren Anlässe eng mit der Person des Grundeigentümers verknüpft sind.

Der Entwurf für die neue Grundbuchverordnung sieht vor, dass ein gesamtschweizerischer Grundstücksindex eingerichtet wird, der den Zugang zu den ohne Interessensnachweis einsehbaren Geodaten mittels öffentlicher Datennetze ermöglicht. Wir haben eine Einschränkung angeregt; mit den heutigen elektronischen Möglichkeiten (z. B. Verknüpfung mit Geoinformationssystemen) und der weltweiten, einfachen und schnellen Verfügbarkeit von Daten ist das Missbrauchspotential für frei einsehbare Grundbuchdaten, und damit auch das Risiko für Persönlichkeitsverletzungen, gestiegen. Die Daten lassen sich leicht kopieren und können von Dritten in missbräuchlicher Weise für andere (z. B. kommerzielle) Zwecke verwendet werden. Deshalb ist die Internetabfrage aus Gründen des Persönlichkeitsschutzes und der Verhältnismässigkeit auf die Bezeichnung des Grundstücks sowie die Grundstücksbeschreibung zu beschränken.

Für alle übrigen Angaben, welche ebenfalls ohne Interessensnachweis zugänglich sind, kann eine interessierte Person eine telefonische oder schriftliche Anfrage machen oder persönlich beim Grundbuchamt vorbeigehen. Mit dieser Lösung und diesen Angaben wird unseres Erachtens der positiven Publizitätswirkung von Grundbuchdaten ausreichend Genüge getan. Weiter sollten die Verantwortlichkeiten beim gesamtschweizerischen Grundstücksindex klar und detailliert in einer Verordnung des EJPD geregelt werden. Insbesondere sind hier Fragen des Zugriffs auf die Daten, der Kontrolle und der Aufsicht zu klären.

Ergänzt wird die Grundbuchverordnung wie erwähnt durch die VeöB, welche die Ausführungsbestimmungen des ZGB betreffend elektronische Ausfertigung und Beglaubigung enthält. Dabei geht es im Wesentlichen um Folgendes:

Vorgesehen sind elektronische Ausfertigungen öffentlicher Urkunden, die den Inhalt der Urschrift wortgetreu wiedergeben und diese im Rechtsverkehr vertreten. Wie von Art. 55a SchlT ZGB vorgegeben, muss die Urschrift, d.h. das Original der öffentlichen Urkunde, weiterhin als Papierdokument erstellt werden.

Mit elektronischen Beglaubigungen bestätigt die Urkundsperson, dass eine Kopie das Originaldokument wiedergibt, oder dass eine Unterschrift von einer bestimmten Person stammt. Die Urkundsperson verfügt über eine qualifizierte elektronische Signatur, die sie nicht nur als Person, sondern auch als Träger ihrer beruflichen Funktion ausweist. Erbracht wird der Nachweis der Berechtigung zur Beurkundung durch ein im Zertifikat enthaltenes, geprüftes und zum Zeitpunkt der Signatur gültiges Berufsattribut, oder durch ein separates, für die jeweilige Beurkundung aus einem Register der Urkundspersonen abgerufenes Zulassungszertifikat, welches bestätigt, dass der Inhaber die Berechtigung zur Beurkundung besitzt. Die Kantone bestimmen, nach welchem Verfahren dieser Nachweis erbracht wird.

Das Bundesamt für Justiz überträgt einer Organisation ausserhalb der zentralen Bundesverwaltung die Bereitstellung und den Betrieb eines Systems zur Führung eines schweizerischen Registers der Urkundspersonen, das sich durch kostendeckende Gebühren selber finanziert. Der Schweizerische Notarenverband, die Fondation Notariat Suisse und private Investoren haben mit dem Ziel des Aufbaus und der Bereitstellung eines solchen Registers eine Aktiengesellschaft gegründet. Unseres Erachtens müssen insbesondere die Verantwortlichkeiten zwischen Bundesbehörden und den Kantonen klar geregelt werden. Weiter machten wir darauf aufmerksam, dass die Angabe von Geburts- bzw. Heimatort und Nationalität unserer Ansicht nach zur Identifikation der Urkundsperson in diesem Register nicht notwendig ist.

1.2.11 Arbeitsgruppe «Fachanforderungen an GEVER als System»

Es ist wichtig, dass die Erfordernisse des Datenschutzes und des Öffentlichkeitsprinzips in der Verwaltung in das Projekt «GEVER Bund» ebenso integriert werden wie die Anforderungen betreffend Informatiksicherheit und Informationsschutz. Überdies haben wir bei der Programmverantwortlichen Vorbehalte hinsichtlich des Zeitplans für die GEVER-Migration geäussert: Nur ein Aufschub der Frist bis Ende 2013 würde eine Integration der Anforderungen in die Standardprodukte ermöglichen.

Im Rahmen des Projekts GEVER Bund konnten die datenschutzspezifischen Anforderungen an die für den Informationsschutz geltenden Anforderungen angeglichen

werden, wobei die funktionelle Unabhängigkeit der Klassifizierungen beibehalten wurde. So gilt das erste Schutzniveau nun sowohl für als «intern» klassifizierte Dokumente als auch für solche, die Personendaten enthalten. Das zweite Niveau umfasst die als «vertraulich» eingestuften Schriftstücke ebenso wie Dokumente mit besonders schützenswerten Personendaten oder Persönlichkeitsprofilen. Das dritte Niveau schliesslich ist den Dokumenten vorbehalten, die als «geheim» klassifiziert sind oder Personendaten enthalten, deren Missbrauch unter Umständen das Leben der betroffenen Person gefährden könnten. Die Dokumente dieses Niveaus müssen derzeit ausserhalb des GEVER-Systems bearbeitet werden, während die Bearbeitung von Dokumenten des zweiten Niveaus nur in verschlüsselter Form erfolgen kann, um den Zugriff darauf durch Administratoren und Leistungserbringer zu verhindern.

Um den Anforderungen des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) Rechnung zu tragen, muss die Zugangsberechtigung zu jedem GEVER-Dokument zunächst vom Ersteller selbst als Hinweis und bei einem konkreten Zugangsgesuch von der Behörde bestimmt werden. So kann der Zugang «aufgeschoben», «gewährt», «teilweise gewährt» oder «verweigert» werden; wenn die Behörde zum Schluss kommt, das Gesuch falle nicht unter das BGÖ, kann es den Status «nicht anwendbar» wählen. Der einmal definierte Zugangsstatus kann nach einem allfälligen Schlichtungsverfahren (gegebenenfalls zusammen mit einer Empfehlung des Beauftragten) oder nach Entscheiden des Bundesverwaltungsgerichts oder in letzter Instanz des Bundesgerichts durch die zuständige Behörde abgeändert werden. Das Öffentlichkeitsgesetz verlangt, dass jede Behörde jährlich die Anzahl der eingegangen Zugangsgesuche und deren Bewertung sowie den Gesamtbetrag der erhobenen Gebühren erfasst. Das GEVER muss deshalb das Führen entsprechender Statistiken ermöglichen.

Bezüglich des Zeitplans der Migration haben wir bei der Verantwortlichen des Programms GEVER Bund Vorbehalte geäussert. Bei einer von der Konferenz der Generalsekretäre für den Sommer 2011 geplanten Annahme des Katalogs der Fachanforderungen wird nämlich aller Wahrscheinlichkeit nach keines der beiden derzeit standardisierten Produkte in der Lage sein, die erwarteten Funktionalitäten bis Ende 2011 zu integrieren. Demzufolge werden nicht alle Dokumente des zweiten Schutzniveaus (vertraulich oder besonders schützenswert) in GEVER angemessen geschützt werden können. Wir sind daher der Ansicht, dass die durch Beschluss des Bundesrates vom 23. Januar 2008 (GEVER-Programm Bund) ursprünglich auf Ende 2011 angesetzte Frist für die Einführung der GEVER-Systeme in den Ämtern auf Ende 2013 verschoben werden sollte. Ein solcher Aufschub würde mit den am 16. Dezember 2009 beschlossenen und vom Bundesrat am 4. Juni 2010 bestätigten ergänzenden Massnahmen für die Umsetzung der Anforderungen betreffend Informations- und Datenschutz zusammenfallen.

1.3 Internet und Telekommunikation

1.3.1 Anonym surfen im Internet?

Ist es heutzutage möglich, beim Surfen im Internet anonym zu bleiben? Cookies beispielsweise werden immer leistungsfähiger, wenn es darum geht, Web-Browser zu personalisieren. Doch auch ganz abgesehen von dieser Technologie ist zu bemerken, dass der benutzte Browser selbst einen Abdruck hinterlässt, der uns eindeutig identifiziert. Diese Feststellung konnten wir nach der Prüfung und Testanwendung des Algorithmus Panopticlick bestätigen.

Seit den Anfängen des Internet können wir mit Hilfe der Cookies bequemer surfen. Diese kleinen Dateien werden beim Besuch auf einer Website in unseren Computern abgelegt, speichern die Präferenzen des Nutzers (wie zum Beispiel die Sprache, in der eine Website angezeigt werden soll) und ermöglichen es so der Website, den Nutzer bei einem künftigen Besuch wieder zu «erkennen».

Über die Cookies-Technologie hinaus haben Forscher Folgendes festgestellt: Jeder Internet-Browser hinterlässt einen Abdruck, der einzigartig oder beinahe einzigartig ist. Somit braucht es keine Cookies mehr, um zu erkennen, welcher Computer sich mit einer Website verbunden hat; es genügt, die Spur des benutzten Browsers zu beobachten.

Wir haben den von Electronic Frontiers Foundation angebotenen Algorithmus Panopticlick geprüft und getestet (Panopticon ist ein Modellgefängnis, in dem die Wärter die Gefangenen unbemerkt beobachten können). Dieser Algorithmus betrachtet eine gewisse Anzahl Parameter bei der Eingabe und liefert ein Entropiemass, mit dem die Einzigartigkeit des getesteten Browsers bestimmt werden kann. Die Parameter sind zum Beispiel der «user agent», der Informationen über den Typ und die Version des Browsers, aber auch des verwendeten Betriebssystems liefert, die Liste der eingerichteten Plug-ins – wobei ein Plug-in eine kleine Software ist, die den Browser mit neuen Funktionalitäten wie etwa das Abspielen von Videos, die eingerichteten Schriftarten oder Informationen über den benutzten Bildschirm ergänzt. Tatsächlich werden sämtliche Informationen gesammelt, auf die man über den Browser zugreifen kann. Diese Informationen gelten aneinander gereiht als Identifikator (Abdruck) des Browsers. So bestimmt die mögliche Einzigartigkeit dieser Kennung die Eindeutigkeit des Browsers.

In der ersten Verbreitungsphase des Algorithmus wurden rund 400'000 solcher Identifikatoren gesammelt und anonymisiert. Jeder neue Abdruck wird mit dieser Sammlung abgeglichen, um festzustellen, ob er einem der bereits bekannten Abdrücke ähnlich ist. Ist dies der Fall, wird ermittelt, wie viele Abdrücke in einer Untergruppe enthalten sein müssen, um darin mit Sicherheit einen identischen Identifikator finden zu können.

Wir haben diesen Algorithmus mit den neuesten Versionen der bekanntesten Browser (Internet Explorer, Firefox, Chrome, Safari, Opera) unter verschiedenen Bedingungen getestet: unmittelbar nach der Einrichtung des Browsers, nach einer gewissen Surf-Dauer, in anonymem Modus und nach Zufügung gewisser Erweiterungen.

Abschliessend stellen wir Folgendes fest: Es muss tatsächlich eingeräumt werden, dass der Abdruck jedes Browsers einzigartig oder leicht identifizierbar ist. Es gibt indes Möglichkeiten, die Gefahren einer eindeutigen Identifikation etwas zu vermindern. So ist der anonyme Surf-Modus, der heute von sämtlichen Browsern angeboten wird (zumindest in ihrer neuesten Version) ein nützliches Tool. Gekoppelt mit gewissen Erweiterungen wie NoScript, die insbesondere vom Browser Firefox angeboten werden, ist er das beste Mittel zur Wahrung der Anonymität beim Surfen im Internet.

1.3.2 Neuentwicklung bei den Cookies

Im Rahmen unserer Beobachtungen im Bereich der Technologie haben wir die Entwicklungen bei der Verwendung von Cookies untersucht. Cookies sind ein bei den Web-Browsern wohlbekannter Mechanismus, der es ermöglicht, die beim Surfen hinterlassene Spur des Nutzers zu speichern. Sie sind gewissermassen das Gedächtnis der Browser. Mit der technologischen Entwicklung sind diese Cookies, ursprünglich bloss kleine Textdateien, immer leistungsfähiger und damit eine eigentliche Bedrohung für die Privatsphäre geworden.

Ein Cookie ist die von einer Webseite beim ersten Besuch an den Browser gesandte kleine Datei, die bei jedem erneuten Besuch an die Seite zurück geschickt wird. So erkennt die Webseite den Browser und demzufolge den Computer und den Benutzer. Gewisse Präferenzen des Nutzers können gespeichert und durch die Webseite bei jedem weiteren Besuch reaktiviert werden.

Eine erste Weiterentwicklung waren die so genannten Drittanbieter-Cookies. Diese werden nicht von der besuchten Webseite abgelegt, sondern von der Webseite einer Drittpartei, deren Objekte – beispielsweise Werbeeinblendungen – auf der besuchten Seite erscheinen. Hier handelt es sich um einen einschneidenden Eingriff in die Privatsphäre, da der Nutzer nicht damit rechnen kann, solche Cookies zu erhalten. Wenn eine Werbung auf mehreren anderen Websites erscheint, kann der Nutzer anhand der Spur, welche die Drittanbieter-Cookies hinterlassen, beim Surfen verfolgt werden.

Flash Cookies (local shared objects) verfügen über viel mehr Speicherplatz als die herkömmlichen Cookies. Die Information, die sie enthalten können, ist damit auch viel gewichtiger. Überdies haben diese Cookies die Eigenschaft, dass sie für verschiedene Browser sichtbar sind und nicht nur für denjenigen, der zum Zeitpunkt der Ablage des Cookie auf dem Computer benutzt wurde.

Die letzte Entwicklung schliesslich, die wir bei den Cookies festgestellt haben, ist das Auftreten von Evercookies. Sie haben die Fähigkeit, sich zu vervielfachen und Kopien in verschiedenen Bereichen des PCs anzulegen. Um ein solches Cookie zu deaktivieren, muss man nicht nur das «Original», sondern auch seine sämtlichen Kopien löschen – es können bis zu deren 13 sein. Es braucht nur eine einzige Kopie vergessen zu gehen, damit sich das Cookie automatisch erneut repliziert. Die Cookies auf die übliche Art zu löschen, genügt also nicht, um als Nutzer gegenüber den besuchten Websites wieder eine gewisse Anonymität zu erlangen.

Aufgrund verschiedener Tests konnten wir feststellen, dass diese Evercookies äusserst schwer zu beseitigen sind. Verschiedene Löschmethoden müssen miteinander kombiniert werden, und es bleiben immer Kopien übrig, die sich nicht auf einfache Weise vernichten lassen. Als Reaktion auf diese neue Technologie sind verschiedene Projekte in Entwicklung, die sich aber bei unseren Tests nicht als zuverlässig erwiesen.

Wie die Entwicklung bei den Cookies zeigt, wird es immer schwieriger, beim Surfen im Internet anonym zu bleiben. Diese in die Computer eingespeisten und schwer löschbaren Informationen geben den Webseiten Aufschluss über die Surfgewohnheiten jedes Nutzers und damit über seine Vorlieben, seine Interessensgebiete und vieles mehr.

1.3.3 Strassenansichten im Internet

Nachdem Google unsere Empfehlungen zur datenschutzkonformen Ausgestaltung von Street View nicht befolgen wollte, haben wir die Angelegenheit dem Bundesverwaltungsgericht zur Entscheidung vorgelegt. Dieses hat unsere Forderungen in allen wesentlichen Punkten gutgeheissen. Auch weitere Anbieter von Strassenansichten im Internet wurden von uns unter die Lupe genommen. Diese unterscheiden sich von Google Street View in mancher Hinsicht.

Wie im 17. Tätigkeitsbericht 2009/2010, Ziff. 1.3.2 berichtet, hatte Google es abgelehnt, Street View gemäss unseren Empfehlungen so anzupassen, dass dem Datenschutz angemessen Rechnung getragen wird. Das von uns in der Folge angerufene Bundesverwaltungsgericht hat nun mit Urteil vom 30. März 2011 bestätigt, dass die datenschutzrechtliche Zulässigkeit von Street View nach Schweizer Recht zu beurteilen ist und der EDÖB zum Erlass der Empfehlung zuständig war. Google hatte beides bestritten.

Das Gericht hat Google nun verpflichtet, sämtliche aufgenommenen Gesichter und Kontrollschilder vor der Veröffentlichung unkenntlich zu machen. Solange dies durch eine Softwarelösung nicht zuverlässig möglich ist, müssen die Bilder manuell bearbeitet werden. Aufnahmen aus dem Bereich von sensiblen Einrichtungen wie etwa Gefängnissen, Spitälern oder Frauenhäusern muss Google zudem soweit anonymisieren, dass auch weitere individualisierende Merkmale wie Hautfarbe, Kleidung, Hilfsmittel von körperlich behinderten Personen etc. nicht mehr feststellbar sind. Bilder, die umfriedete Gärten, Höfe oder andere Privatbereiche zeigen, die dem Anblick eines gewöhnlichen Passanten verschlossen bleiben, dürfen nicht aufgenommen bzw. müssen aus Street View entfernt werden, wenn keine Einwilligung vorliegt. Jeweils eine Woche im Voraus muss Google im Internet und in lokalen Presseerzeugnissen über die Aufnahme und die Publikation neuer Bilder orientieren.

Das Urteil des Bundesverwaltungsgerichts war bei Redaktionsschluss dieses Tätigkeitsberichts noch nicht rechtskräftig. Dank seiner überzeugenden Begründung leistet es aber auf jeden Fall einen wichtigen Beitrag zur Klärung der Frage, wo die Grenzlinien bei der Abwägung der wirtschaftlichen Interessen von Anbietern neuartiger Medienformate und den Persönlichkeitsrechten der betroffenen Personen verlaufen. Das Urteil (A-7040/2009) ist auf unserer Website www.derbeauftragte.ch unter Themen – Datenschutz – Internet – Google Street View und auf derjenigen des Bundesverwaltungsgerichts abrufbar.

Wir haben zu vier weiteren Anbietern von virtuellen Stadtrundgängen im Internet nähere Sachverhaltsabklärungen getätigt und konnten feststellen, dass alle Anbieter Anstrengungen zum Persönlichkeitsschutz unternehmen. Die Angebote weisen aber jeweils spezifische Eigenheiten auf, namentlich mit Bezug auf die konkreten Modalitäten der Aufnahme und der Wiedergabe der Bilder. Die verwendeten technischen Hilfsmittel, Verfahren und Vorgehensweisen unterscheiden sich massgeblich von denjenigen bei Google Street View. Entsprechend differenziert hat die Interessenabwägung zu erfolgen und müssen die jeweils angemessenen Massnahmen zum Persönlichkeitsschutz ausgestaltet werden.

Bei den von uns untersuchten Angeboten werden die Bilder (im Gegensatz zu Google Street View) nicht flächendeckend und automatisch vom Dach eines fahrenden Autos aus, sondern an einigen ausgewählten, im Gemeinbereich gelegenen Standorten manuell mittels einer auf einem Stativ auf Augenhöhe montierten Digitalkamera mit «Fisheye»-Objektiv aufgenommen. An jedem Standort werden dabei Aufnahmen in alle Himmelsrichtungen gemacht, was längere Zeit dauert. Zufällige Passanten haben damit Gelegenheit zu erkennen, dass sie fotografiert werden, und können sich abwenden oder den fotografierten Bereich verlassen. Zudem kann auch der Fotograf durch die Wahl des Aufnahmezeitpunkts vermeiden, dass Personen, die das offensichtlich

nicht wünschen, auf dem Bild zu sehen sind. Da der Fotograf zu Fuss unterwegs ist und sich nicht in einem fahrenden Auto befindet, kann er von den Anwesenden auch direkt angesprochen werden. Sie können sich so über den Zweck der Fotoaufnahmen und die geplante weitere Verwendung des Bildmaterials erkundigen oder einer Publikation widersprechen.

Die aufgenommenen Einzelbilder werden zudem manuell (und nicht wie bislang bei Google Street View mit einer fehleranfälligen vollautomatischen Software) nachbearbeitet. Dabei werden durch Verwischung oder durch Überlagerung von mehreren kurz nacheinander aufgenommenen Bildern die abgebildeten Personen weiter unkenntlich gemacht.

Die von uns untersuchten Beispiele zeigen nicht nur, wie dem Datenschutz durch eine andere technische Vorgehensweise besser Rechnung getragen werden kann, sondern beweisen auch, dass kreative Lösungen gefunden wurden, wie «belebt» wirkende Strassenansichten unter Wahrung der Persönlichkeitsrechte der darauf abgebildeten Passanten veröffentlicht werden können.

1.3.4 Erfassung von WLAN-Netzwerken

Im Frühjahr 2010 wurde bekannt, dass Google auf seinen Kamerafahrten für Street View auch in der Schweiz Daten aus WLAN-Funknetzen gespeichert hatte. Unsere Abklärungen haben ergeben, dass die Erfassung dieser Daten nicht datenschutzkonform war.

Im April 2010 haben wir betreffend Erfassung von WLAN-Netzen durch Google Abklärungen eingeleitet und die Firma zur Stellungnahme aufgefordert. Anfangs Mai 2010 teilte uns Google schriftlich mit, dass tatsächlich Daten zu WLAN-Netzen in der Schweiz erhoben und bearbeitet werden, jedoch keine Kommunikationsinhalte (Payload). Der Zweck der Datenerhebung sei der Aufbau einer von GPS unabhängigen Lokalisierungsfunktion anhand der WLAN-Router- und Funkantennenstandorte. Bereits Mitte Mai 2010 berichtete uns Google dann aber, dass im Rahmen der Street-View-Aufnahmefahrten doch auch unbeabsichtigt Kommunikationsinhalte aus offenen Netzwerken aufgezeichnet worden seien. In der Folge stellte Google die Aufnahmefahrten solange ein, bis die WLAN-Ausrüstungen aus den Fahrzeugen demontiert waren.

Unmittelbar nach dem Bekanntwerden der WLAN-Datenaufzeichnung hat Google die Daten aus dem Firmennetzwerk separiert, für weitere Verwendungen gesperrt und verschlüsselt. Bei der Analyse dieser Daten haben wir Fragmente aus den WLAN-Übertragungen entdeckt, die jeweils in dem Moment stattfanden, als das Street-View-Fahrzeug den Sendebereich des WLAN-Routers passierte. Es handelt sich unter anderem um vollständige E-Mail-Nachrichten, Webseitenaufrufe, Benutzernamen, Passwörter,

Telefonnummern, E-Mail-Adressen und Geschäftsadressen. Damit decken sich unsere Erkenntnisse mit den Ergebnissen von anderen Datenschutzbehörden.

Mit dem Verzicht auf die WLAN-Ausrüstung in den Aufnahmefahrzeugen werden künftig bei den Fahrten von Google keine Payloaddaten mehr erfasst. Ausserdem empfahlen wir der Firma, die in der Schweiz widerrechtlich erhobenen Payloaddaten komplett zu löschen und technische und organisatorische Massnahmen zur Verhinderung ähnlicher Vorfälle zu treffen. Das beinhaltet unter anderem die Berücksichtigung von Privacy by Design bereits in der Entwicklungsphase, aber auch Audits vor Einführung von neuen Dienstleistungen oder Produkten.

Im Rahmen dieser Abklärungen haben wir überdies festgestellt, dass noch immer eine Vielzahl von WLAN-Netzwerken unverschlüsselt betrieben werden. Insbesondere überrascht, dass nicht nur private, sondern auch geschäftliche Informationen (z.B. E-Mails zum Datawarehouse-Projekt einer Bank) offen über die WLAN-Netzwerke übertragen werden. Wir empfehlen dringend, WLAN-Netzwerke nur verschlüsselt zu betreiben (WPA2-AES), um zum einen die Datenübertragung vor dem Zugriff durch Drittpersonen zu schützen, zum andern aber auch, um Unbefugte daran zu hindern, als Trittbrettfahrer die Bandbreite des WLANs für den Internetzugang zu schmälern oder ihn gar für illegale Handlungen zu missbrauchen. Zusätzlich regen wir an, vertrauliche Informationen selbst dann zu chiffrieren, wenn diese über gesicherte Verbindungen (SSL, VPN) übermittelt werden.

1.3.5 Internet-Tauschbörsen: Entscheid des Bundesgerichts

Das Bundesgericht hat die Logistep AG angewiesen, jede Datenbearbeitung im Bereich des Urheberrechts einzustellen, und es ihr untersagt, die bereits beschafften Daten den betroffenen Urheberrechtsinhabern weiterzuleiten. Es setzte damit ein Zeichen gegen die auch in anderen Bereichen erkennbare Tendenz von Privaten, Aufgaben an sich zu ziehen, die klar dem Rechtsstaat obliegen.

Im Auftrag von Urheberrechtsinhabern sammelte die Logistep AG in Peer-to-Peer-Netzwerken IP-Adressen von Nutzern, die angeblich illegal urheberrechtsgeschützte Inhalte (Musik- oder Videodateien) zum Tausch anboten. Mit diesen IP-Adressen stiessen die Rechteinhaber Strafverfahren an, um mittels der dann gewährten Akteneinsicht die Identität der Betroffenen zu erfahren und von ihnen Schadenersatz zu verlangen. Nach unserer Einschätzung war diese Datenbearbeitung für die Betroffenen nicht erkennbar und verstiess gegen das Zweckbindungsprinzip, ohne dass dafür

ein Rechtfertigungsgrund vorlag. Anfang 2008 empfahlen wir der Logistep AG daher, ihre Nachforschungen in Peer-to-Peer-Netzwerken einzustellen, solange der Gesetzgeber keine rechtliche Basis dafür geschaffen hat (vgl. unseren 15. Tätigkeitsbericht 2007/2008, Ziff. 1.3.1).

Logistep lehnte die Empfehlung ab, worauf wir ans Bundesverwaltungsgericht gelangten. Dieses wies die Klage mit Urteil vom 27. Mai 2009 ab. Es gewichtete die Interessen der Urheberrechtsinhaber höher als die Interessen der P2P-Nutzer (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.3.1). Diesen Entscheid haben wir durch das Bundesgericht überprüfen lassen. Es hat das erstinstanzliche Urteil umgestossen und ist damit im Ergebnis unserer Ansicht gefolgt: Es hat die Logistep AG angewiesen, jede Datenbearbeitung im Bereich des Urheberrechts einzustellen, und es ihr untersagt, die bereits beschafften Daten den betroffenen Urheberrechtsinhabern weiterzuleiten. Der Link auf das Urteil 1C_285/2009 vom 8. September 2010 befindet sich auf unserer Webseite www.derbeauftragte.ch unter Dokumentation – Datenschutz – Weiterzüge).

Dem Urteil des höchsten Schweizer Gerichts kommt über den konkreten Fall hinaus Bedeutung zu. Die folgenden wesentlichen Aussagen in der Urteilsbegründung sind besonders bemerkenswert:

- Im Falle der Weitergabe von Daten ist es für deren Qualifikation als Personendaten ausreichend, wenn erst der Empfänger die betroffenen Personen zu identifizieren vermag. Trifft dies zu, ist das DSG auf die ganze Datenbearbeitung anwendbar.
- Eine abstrakte Feststellung, ob es sich bei (insbesondere dynamischen) IP-Adressen um Personendaten handelt oder nicht, ist nicht möglich; jeder Einzelfall ist konkret zu betrachten. IP-Adressen sind jedenfalls dann Personendaten, wenn nach der allgemeinen Lebenserfahrung damit zu rechnen ist, dass der Aufwand für die Bestimmung der betroffenen Person auf sich genommen werden könnte. Im Fall Logistep war die Frage zu bejahen, da ja das ganze Geschäftsmodell von Logistep auf der Identifizierung der Betroffenen beruhte.
- Die Logistep AG verletzte mit ihrer Datenbearbeitung das Zweckbindungs- und das Erkennbarkeitsprinzip. Zu prüfen war, ob dafür ein Rechtfertigungsgrund vorlag. Eine strikt systematische Auslegung, wonach lediglich bei lit. b und c, nicht aber bei lit. a von Art. 12 Abs. 2 DSG das Geltendmachen eines Rechtfertigungsgrunds zulässig sein soll, erwiese sich nämlich als verfehlt, zumal in der aktuellen Fassung von lit. a die Rechtfertigungsgründe zwar nicht mehr erwähnt, jedoch auch nicht ausdrücklich ausgeschlossen werden. Die

Bestimmung ist daher so auszulegen, dass eine Rechtfertigung der Bearbeitung von Personendaten entgegen der Grundsätze von Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG zwar nicht generell ausgeschlossen ist, dass Rechtfertigungsgründe im konkreten Fall aber nur mit grosser Zurückhaltung bejaht werden können.

- Eine Empfehlung des EDÖB bezweckt die Verteidigung einer Vielzahl von Personen und liegt damit letztlich im öffentlichen Interesse. Diese Bedeutung der Empfehlung des EDÖB ist bei der Interessenabwägung nach Art. 13 Abs. 1 DSG zu berücksichtigen, zumal eine (gegebenenfalls richterlich bestätigte) Empfehlung auch eine indirekte Wirkung für all jene Personen zeitigt, die nach einer ähnlichen Methode vorgehen.
- Die Logistep AG verfolgte wirtschaftliche Interessen, indem sie mit einer dafür entwickelten Software in P2P-Netzwerken nach urheberrechtlich geschützten Werken suchte und von deren Anbietern Daten speicherte. Eine solche Methode führt allgemein – über den konkreten Fall hinaus – wegen fehlender gesetzlicher Reglementierung zu einer Unsicherheit in Bezug auf Art und Umfang der im Internet gesammelten Daten und ihrer Bearbeitung. Insbesondere sind die Speicherung und die mögliche Verwendung der Daten ausserhalb eines ordentlichen Gerichtsverfahrens nicht klar bestimmt. Auch das Interesse an der wirksamen Bekämpfung von Urheberrechtsverletzungen vermag die Tragweite der Persönlichkeitsverletzungen und der mit der umstrittenen Vorgehensweise einhergehenden Unsicherheiten über die Datenbearbeitung im Internet nicht aufzuwiegen.
- Dem Bundesgericht ging es erklärtermassen nicht darum, dem Datenschutz generell den Vorrang gegenüber dem Schutz des Urheberrechts einzuräumen. Es sei aber Sache des Gesetzgebers und nicht des Richters, die allenfalls notwendigen Massnahmen zu treffen, um einen den neuen Technologien entsprechenden Urheberrechtsschutz zu gewährleisten.
- Ausdrücklich offen gelassen hat das Bundesgericht, ob die Strafverfolgungsbehörden die von Logistep erlangten Daten verwenden dürfen.

1.3.6 Online Marketing: Neue e-Privacy-Richtlinie der EU

Das EU-Parlament hat Ende 2009 eine Revision der e-Privacy-Richtlinie 2002/58/EG beschlossen. Das Ziel war, mehr Transparenz und Sicherheit für die Verbraucher zu schaffen. Die praktische Umsetzung der neuen Richtlinie in den Mitgliedstaaten dürfte sich ab 2011 konkretisieren, was auch Konsequenzen für die Schweiz haben wird.

Die e-Privacy-Richtlinie wurde entworfen, um den Anforderungen der neuen digitalen Technologien gerecht zu werden. Die Richtlinie ergänzt die EU-Datenschutzrichtlinie und umfasst alle Themen im Bereich der Privatsphäre im Sektor der elektronischen Kommunikation. Die Direktive behandelt den Schutz persönlicher Daten sowie der Privatsphäre in elektronischen Kommunikationsnetzwerken.

Mit der neuen Richtlinie 2009/136/EG werden Dienstanbieter erstmals zur aktiven Information ihrer Nutzer über Datenpannen bzw. spezifische Risiken wie Viren oder Malware-Attacken verpflichtet.

Eine weitere Neuerung: Cookies oder Spyware sollen künftig nicht mehr ohne Zustimmung des Internetnutzers auf dessen PC installiert werden dürfen. Cookies können Logins, Passwörter und Präferenzen abspeichern, was für den Nutzer praktisch ist. Doch Cookies können auch dazu verwendet werden, das Surfverhalten im Netz zu verfolgen. So ist es für einzelne Werbetreibende möglich, anhand der Cookies, die sie über unterschiedliche Webseiten verteilen, Nutzerprofile anzulegen. Dieses Verfahren ist auch unter dem Namen «Online Tracking» bekannt.

Die alte Richtlinie verlangte von den Webseitenbetreibern, den Nutzern die Wahl des «Opt-out» zu geben. Dies passierte normalerweise, indem sie die entsprechende Einstellung im Browser vornahmen. Hier setzt die neue EU-Richtlinie an und schreibt vor, dass die Nutzer ihre ausdrückliche Einwilligung für die Speicherung von Informationen oder für den Zugriff auf solche Informationen geben müssen («Opt-in»-Verfahren). Deshalb müssen die Nutzer vorgängig klare und umfassende Informationen über die Zwecke der Speicherung oder des Zugangs erhalten.

Die Mitgliedstaaten der EU müssen die Richtlinie bis zum 25. Mai 2011 in nationales Recht umsetzen. Wie dies in den einzelnen Ländern passieren wird, entscheidet sich in einem intensiven Diskurs zwischen Internetunternehmen, Werbefirmen, Gesetzgeber und Datenschützern, welcher noch im Gange ist.

Da die Schweiz nicht Mitglied der EU ist, gilt das Gemeinschaftsrecht für sie grundsätzlich nur dann, wenn sie dies explizit beschliesst. So oder so werden die Regelungen auch für die in der Schweiz ansässigen Anbieter und Nutzer Konsequenzen haben. Wir verfolgen deshalb die Diskussionen intensiv. Des Weiteren haben wir zu verschiedenen

nationalen und internationalen Branchenverbänden Kontakte geknüpft und führen laufend Gespräche, um die Konsequenzen für Schweizer Unternehmen abzuschätzen und Lösungen zu suchen.

Grundsätzlich sind die vorgesehenen Änderungen zugunsten einer datenschutzfreundlicheren Ausgestaltung des Online-Marketings mittels Cookies und dergleichen Instrumente begrüssenswert. Die Ausgestaltung soll aber gleichzeitig benutzerfreundlich und einfach handhabbar sein.

1.3.7 Soziale Netzwerke und Datenschutz

Social Networking Services im Internet bleiben weiterhin ein Thema. Da es hierbei regelmässig um internationale Sachverhalte geht, ist die Rechtslage kompliziert. Die Internet-Nutzer sind gut beraten, ihre Eigenverantwortung wahrzunehmen und persönliche Daten nur mit Bedacht zu veröffentlichen.

Soziale Netzwerke im Internet geben immer wieder Anlass zu Anfragen bei uns. Gerade was den räumlichen Anwendungsbereich der nationalen Datenschutzgesetzgebungen bei Internetanbietern mit Sitz im Ausland betrifft, sind viele Fragen aber noch ungeklärt. Auf dem Rechtsweg gegen solche Anbieter vorzugehen, ist schwierig und aufwendig. Wir beobachten die Entwicklung bei den Sozialen Netzwerken genau und prüfen – in Zusammenarbeit mit ausländischen Datenschutzstellen – Vorgehensmöglichkeiten, um dem Grundrecht auf informationelle Selbstbestimmung auch in einem weltumspannenden Medium wie dem Internet Geltung zu verschaffen.

Die «Freundefinder»-Funktion von Facebook führte zu besonders vielen Meldungen von Betroffenen. Facebook geht davon aus, dass jemand mit anderen Personen in Verbindung steht, wenn diese dessen E-Mail-Adresse an Facebook weitergeben, z.B. indem sie über die «Freundefinder»-Funktion ihre elektronischen Adressbücher auf die Plattform laden. Gestützt auf diese Annahme verschickt Facebook dann personalisierte Werbe-E-Mails mit Hinweisen auf mögliche «Freunde», um neue Nutzer zu gewinnen.

Wir empfehlen betroffenen Personen, ihre Bekannten darauf aufmerksam zu machen, dass sie eine Weitergabe ihrer persönlichen Daten an Facebook nicht wünschen. Facebook stellt zudem eine (nicht einfach auffindbare) Möglichkeit zur Verfügung, die weitere Werbe-E-Mails in Zukunft unterbinden sollte. Unter www.facebook.com/help/contact.php?show_form=database_removal findet man ein Formular für die Mitteilung, man wolle aus der Datenbank entfernt werden und keine E-Mails von Facebook mehr erhalten.

In unserem 16. Tätigkeitsbericht 2008/2009, Ziff. 1.3.6, haben wir bereits auf unsere Erläuterungen zu Risiken und Gefahren von Sozialen Netzwerken hingewiesen und konkrete Empfehlungen für einen verantwortungsvollen Umgang damit formuliert. Die Erläuterungen sind auch auf unserer Homepage aufgeschaltet (Themen – Datenschutz – Internet – Soziale Netzwerke).

1.3.8 Bearbeitung von Kundendaten bei Telekomunternehmen

Die Telekombranche agiert in einem innovativen und sich schnell wandelnden Markt. Aus datenschutzrechtlicher Sicht muss die korrekte Verwaltung und Berichtigung der Kundenadressen eines Unternehmens mit den Entwicklungen Schritt halten können und jederzeit sichergestellt sein.

In den Jahren 2007 und 2009 kontaktierten uns wiederholt Kundinnen und Kunden eines Telekomunternehmens im Zusammenhang mit fehlerhafter Bearbeitung von Umzugsmeldungen oder sonstigen Adressänderungen (z.B. Namensänderungen). Angesichts dessen haben wir im letzten Jahr eine Sachverhaltsabklärung bei diesem Unternehmen durchgeführt. Dabei konzentrierten wir uns auf die Berichtigung von Kundendaten sowie deren weitere Pflege, mit besonderem Augenmerk auf den Umgang mit den Umzugsmeldungen und die technischen und organisatorischen Massnahmen zu ihrer Erfassung.

Das Telekomunternehmen bestätigte grundsätzlich die uns bis Herbst 2009 gemeldeten Probleme. Entsprechend waren bereits Massnahmen in der Organisation und Struktur der «Office Operations» ergriffen worden. Gemäss dem Unternehmen müsse weiter berücksichtigt werden, dass die Vorlaufzeit für die Abwicklung einer Adressänderung ab Meldungseingang etwa einen Monat betrage. Einige Kunden seien sich nicht bewusst, dass eine Umzugsmeldung oder Adressänderung nicht von einem Tag auf den anderen abgewickelt sei. Dies zeige sich vor allem, wenn Fakturierung und Umzugsbearbeitung parallel zueinander laufen und die Rechung aufgrund der Vorlaufzeit an die alte Adresse verschickt wurde. Manche Kunden dürften insbesondere bei der selbständigen Änderung ihrer Adresse im Internet erwartet haben, dass diese sofort wirksam werde. Seit einiger Zeit mache nun das Unternehmen aktiv auf der Homepage oder direkt im Kundenkontakt auf die einmonatige Vorlaufzeit aufmerksam und habe den Kundendienst generell verbessert.

Im Bereich Marketing und Werbung hat uns das Telekomunternehmen bestätigt, dass es seine Kundenadressen weder an Dritte verkaufe noch vermiete. Zudem würden bis auf die zur Verrechnung der Dienstleistungen notwendigen Angaben keinerlei Daten über das Nutzungsverhalten der Kunden erhoben, und es finde keine Auswertung oder

Profilierung statt. Auch im Bereich Digital-TV finde keine Auswertung des Konsumverhaltens (auch keine anonymisierte) statt.

Gesamthaft kommen wir anhand der erhaltenen Informationen und Dokumentationen zum Schluss, dass zum Zeitpunkt der Sachverhaltsabklärung beim fraglichen Telekomunternehmen im Bereich der Kundenadressverwaltung keine Probleme mehr vorhanden waren. Das Unternehmen hat auf die in der Vergangenheit aufgetretenen Schwierigkeiten reagiert und die Abläufe korrigiert. Entsprechend lässt sich ein klarer Rückgang der seit November 2009 eingegangenen Beschwerden beobachten. Wir haben feststellen können, dass sich die Firma der Sorgfaltspflicht betreffend ihrer Kundenadressen bewusst ist. Diese Sorgfalt lässt sich auch in der IT-Infrastruktur und deren Management erkennen. Schliesslich haben wir dem Unternehmen vorgeschlagen, allfällige datenschutzrechtliche Fragen regelmässig mit uns zu bereinigen.

1.3.9 Bearbeitung von Personendaten bei departementsübergreifenden GEVER-Systemen

Die gesetzliche Grundlage zur Bearbeitung von Personendaten in einem GEVER-System auf Bundesorganebene befindet sich in Artikel 57h des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG). Diese Bestimmung genügt jedoch nicht als rechtliche Grundlage für ein überdepartementales GEVER-System in einem automatisierten Verfahren.

Der Begriff GEVER steht in der Bundesverwaltung als Synonym für elektronische Geschäftsverwaltung. Das System soll grundsätzlich sowohl die rechtskonforme und effiziente Aktenführung durch die systematische Verwaltung als auch die rasche Verfügbarkeit von Informationen ermöglichen. Es bildet auch die Voraussetzung für durchgängige und automatisierte Prozesse im Bereich eGovernment. Im Rahmen des Programms «GEVER Bund» sollen daher die Bundesrats- und Parlamentsgeschäfte im Sinne von so genannt überdepartementalen Prozessen (ÜDP) bis Ende 2011 auf eine durchgängige elektronische (d.h. medienbruchfreie) Basis umgestellt werden.

Für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen benötigen Bundesorgane eine gesetzliche Grundlage im formellen Sinn. Diese rechtliche Grundlage ist der Artikel 57h RVOG, der es jedem Bundesorgan erlaubt, ein Informations- und Dokumentationssystem zu führen. Dieses kann besonders schützenswerte Daten und Persönlichkeitsprofile enthalten, soweit sie sich aus dem Schriftverkehr oder aus der Art des Geschäfts ergeben. Diese Regelung gilt indessen nur für die Geschäftsverwaltung innerhalb eines Bundesorgans, also eines Amts oder Departements. Der Gesetzgeber wollte nicht, dass sich der automatisierte Zugriff, das so genannte Abrufverfahren, auf solche Systeme über mehrere Bundesorgane erstreckt,

und hielt deshalb im 2. Absatz des RVOG-Artikels fest, dass «zu den Personendaten ausschliesslich Mitarbeiterinnen und Mitarbeiter des betreffenden Bundesorgans Zugang haben, und dies nur soweit sie sie zur Erfüllung ihrer Aufgabe brauchen.»

Damit stellt sich die Frage nach der für eine departements- respektive ämterübergreifende Geschäftsverwaltung notwendigen gesetzlichen Grundlage; eine Frage, die wir mehrfach in Sitzungen mit den GEVER-Bund-Vertretern diskutierten. Unserer Meinung nach reicht Artikel 57h RVOG für GEVER ÜDP im Abrufverfahren nicht aus, falls darin besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden. Allenfalls muss die Bestimmung angepasst und ihr Geltungsbereich erweitert werden.

1.3.10 Elektronische Erledigung der Zollformalitäten

Das eCustoms-Projekt in der Europäischen Union hat zum Ziel, alle papiergestützten Zollverfahren durch elektronische Verfahren zu ersetzen. Damit soll ein moderneres und effizienteres Zollumfeld geschaffen werden. In der Schweiz hat eine Arbeitsgruppe, welche wir begleitet haben, eine Machbarkeitsstudie über eine mögliche Zusammenarbeit ausgearbeitet.

Ziel des eCustoms-Projekts ist es, alle Zollvorgänge (Import, Export, Transit) in einfacher und effizienter Weise auf einem einzigen Internetportal abzuwickeln. Der Datenaustausch zwischen den Herstellern, Zollämtern des In- und Auslandes und den Kunden soll von A bis Z elektronisch ablaufen. Auf nationaler Ebene beinhaltet dies die Umsetzung der eGovernment-Prinzipien in den Zollverfahren. Auf internationaler Ebene bedeutet es insbesondere, dass die elektronischen Verzollungssysteme der Schweiz und der EU miteinander verbunden würden.

Aus Vertretern des EVD, EFD, EDA und EJPD wurde eine Arbeitsgruppe gebildet, die eine Machbarkeitsstudie über eine Zusammenarbeit der Schweiz mit der EU im eCustoms-Projekt ausgearbeitet hat. Die Studie dient dem Bundesrat als Entscheidungsgrundlage für mögliche Verhandlungen mit der EU und deckt verschiedene Bereiche ab.

Koordiniert mit dem Bundesamt für Justiz haben wir das Projekt aus der Sicht des Datenschutzes begleitet. Wir stellten u. a. fest, dass das Zollgesetz und die Datenbearbeitungsverordnung für die Eidgenössische Zollverwaltung angepasst werden müssen. Zum Zeitpunkt der Machbarkeitsstudie war es jedoch zu früh zu beurteilen, welche Regelungen konkret angepasst werden müssen, da viele Fragen bezüglich der Realisierung des eCustoms-Projekts noch nicht geklärt waren. Welche tatsächlichen Anpassungen notwendig sind und worauf aus datenschutzrechtlicher Sicht besonders zu achten ist, werden wir bei der Konkretisierung des Projektes beurteilen können.

1.4 Justiz/Polizei/Sicherheit

1.4.1 Umsetzung Schengen: Kontrolle beim Generalkonsulat in Istanbul

Im Rahmen der Schengen-Zusammenarbeit haben wir beim Generalkonsulat in Istanbul eine Kontrolle durchgeführt. Teil der Überprüfung waren unter anderem die Terminvergabe durch ein türkisches Unternehmen sowie die Logfiles.

Bereits zum dritten Mal haben wir aufgrund der Schengen-Zusammenarbeit eine Kontrolle bei einer Auslandsvertretung der Schweiz durchgeführt. Bei diesen Überprüfungen geht es insbesondere darum, die Erteilung von so genannten Schengenvisa und die damit verbundene Datenbearbeitung im Schengener Informationssystem (SIS) zu beleuchten. Dieses Jahr inspizierten wir das Generalkonsulat in Istanbul, wo die Terminvergabe für die Visumsantragsteller an ein privates türkisches Unternehmen ausgelagert worden war. Eine solche Auslagerung ist durch das Schengenrecht zugelassen, muss aber strengen Anforderungen genügen. Unsere Überprüfung umfasste die ganze Datenbearbeitung im Zusammenhang mit der Erteilung von Schengenvisa inklusive der Auslagerung der Terminvergabe. Dabei haben wir auch die Zugriffe des Generalkonsulats Istanbul auf das SIS und das Informationssystem ZEMIS des Bundesamtes für Migration (BFM) sowie die entsprechenden Logfiles überprüft. Dies geschah, indem wir zunächst vor Ort verschiedene Abfragen im SIS und im ZEMIS notierten und später in Bern, bei fedpol für das SIS und beim BFM für das ZEMIS, kontrollierten, ob diese Zugriffe in den Logfiles protokolliert worden waren.

Wir konnten feststellen, dass die von uns überprüften Datenbearbeitungen datenschutzkonform verlaufen waren. Aus unserer Kontrolle resultierten daher einzig zwei Verbesserungsvorschläge, die beide akzeptiert wurden. Der erste Vorschlag war an das Generalkonsulat resp. das Departement für auswärtige Angelegenheiten gerichtet und hielt fest, dass bis Ende 2011 die Datenschutzausbildung des betreffenden Personals nachgeholt werden müsse. Der zweite Vorschlag ging an das BFM. Bei der Überprüfung der Benutzerliste für ZEMIS waren wir auf einen Account gestossen, der nicht auf den Namen eines bestimmten Sachbearbeiters lautete, sondern mit «Datenbereinigung» betitelt war. Wir schlugen dem BFM daher vor, diesen für den Support benutzten Account auf den Namen des zuständigen Sachbearbeiters umzuschreiben und, falls mehrere Personen für den Support zuständig seien, weitere personalisierte Accounts zu eröffnen.

1.4.2 Umsetzung Schengen: Kontrolle beim Grenzwachtkorps

Unsere Kontrolle beim Grenzwachtkorps hat ergeben, dass die Mitarbeiterinnen und Mitarbeiter das Schengener Informationssystem (SIS) in Einklang mit den einschlägigen Gesetzesvorschriften konsultiert haben. Im Bereich der Schulung der Nutzer sind indessen Abklärungen erforderlich.

Im Rahmen unserer Aufsichtsbefugnisse über die Bearbeitung von Personendaten durch Bundesorgane, welche den nationalen Teil des Schengener Informationssystems (N-SIS) nutzen, haben wir den Zugriff auf das System durch die Mitarbeiterinnen und Mitarbeiter einer Region des Grenzwachtkorps kontrolliert. Wir führten unsere Analyse ausgehend von den Logfiles des N-SIS durch und überprüften die Zugriffe der Hälfte der im gewählten Zeitraum (ein Samstag und ein Sonntag) Dienst habenden Mitarbeitenden (rund 50 Personen). Insgesamt suchten diese Mitarbeiter in der fraglichen Zeit nach etwa zwanzig Personen im N-SIS.

Eine Dienst habende Person stellte Nachforschungen mit ihrem eigenen Familiennamen an. Eine weitere Analyse der Logfiles betreffend diese Person über einen Zeitraum von sieben Monaten ergab, dass sie vier Mal mit ihrem eigenen Familiennamen im N-SIS nachgeforscht hatte. Die kantonalen Datenschutzbehörden stellten im Rahmen ihrer eigenen Kontrollen ebenfalls fest, dass mehrere kantonale Nutzer mit ihrem eigenen Familiennamen Nachforschungen im N-SIS angestellt hatten. Die Nutzer gaben den kantonalen Datenschutzbehörden an, die Nachforschungen hätten Schulungszwecken gedient. Wir sind der Ansicht, dass der bei unserer Kontrolle beim Grenzwachtkorps festgestellte Fall ebenfalls in diese Kategorie gehört. Aus diesem Grunde verzichteten wir darauf, mit der betreffenden Person Kontakt aufzunehmen.

Die Koordinationsgruppe Schengen der Schweizerischen Datenschutzbehörden hat ein Schreiben vorbereitet, das die Nutzer für die Notwendigkeit sensibilisieren soll, den Gesetzesrahmen einzuhalten und insbesondere im N-SIS nicht nach Ausschreibungen von Personen aus ihrer Familie, ihrem Umfeld oder bekannten Persönlichkeiten zu suchen. Dieses Schreiben weist weiter darauf hin, dass die Einhaltung der gesetzlichen Normen auch bei Schulungskursen gewährleistet sein muss, indem beispielsweise die dafür vorgesehene Plattform benutzt wird. Jedes Mitglied der Koordinationsgruppe kann dieses Schreiben im Rahmen seiner Sensibilisierungs- bzw. Kontrolltätigkeiten in seinem Zuständigkeitsbereich auf Bundes- oder Kantonsebene verwenden. Im Rahmen unserer Kontrolle haben wir es dem Grenzwachtkorps zukommen lassen.

1.4.3 Umsetzung Schengen: Rahmenbeschluss 2008/977/JI

Aufgrund des Rahmenbeschlusses über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen bearbeitet werden, obliegen uns Verpflichtungen, welche die Revision mehrerer Bundesgesetze erforderlich machten. Die neuen einschlägigen Bestimmungen des Datenschutzgesetzes (DSG) verstärken namentlich die Unabhängigkeit unserer Behörde.

Der Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen bearbeitet werden, ist eine Weiterentwicklung des Schengen-Besitzstandes. Wie die übrigen Mitgliedstaaten mussten wir die notwendigen Massnahmen treffen, um den Bestimmungen des Rahmenbeschlusses nachzukommen, und dies bis Ende November 2010.

Der Rahmenbeschluss ruft die allgemeinen Grundsätze der Rechtmässigkeit, der Verhältnismässigkeit, der Zweckbindung und der Richtigkeit der Daten sowie die Rechte der betroffenen Person in Erinnerung und führt gewisse spezifische Vorschriften ein. Er definiert insbesondere die Zwecke, zu denen die von einem Schengen-Staat übermittelten Daten bearbeitet werden können, und bestimmt, welche Bedingungen gelten, wenn die Behörde eines Schengen-Staates die Übermittlung der von einem anderen Schengen-Staat bereitgestellten Daten an einen Drittstaat, an eine internationale Einrichtung oder an eine Privatperson erwägt.

Obwohl die Bestimmungen des Rahmenbeschlusses direkt anwendbar sind, mussten mehrere Gesetzestexte überarbeitet werden: das Datenschutzgesetz, das Schengen-Informationsaustausch-Gesetz (SIaG), das Ausländergesetz (AuG), das Asylgesetz (AsylG), das Waffengesetz (WG), das Betäubungsmittelgesetz (BEtmG) und das Strafgesetzbuch (StGB).

Die wichtigsten Gesetzesänderungen im Bereich des Datenschutzes sind jedoch im DSG enthalten. Dessen Revision, in Kraft getreten am 1. Dezember 2010, bewirkt eine Stärkung der Unabhängigkeit unserer Behörde. Der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte wird künftig vom Bundesrat mit Zustimmung des Parlaments für eine Amtszeit von vier Jahren ernannt. Überdies richten wir unsere jährlichen Tätigkeitsberichte neu an die Bundesversammlung und übermitteln sie gleichzeitig an den Bundesrat. Damit werden nicht nur die Anforderungen des Rahmenbeschlusses, sondern auch die im Jahre 2008 anlässlich der Evaluation der Umsetzung des Schengen-Besitzstandes in der Schweiz ausgesprochenen Empfehlungen der EU verwirklicht.

1.4.4 Methodik der koordinierten Kontrollen im Rahmen von Schengen

Die Schengen-Abkommen sehen die Einführung von Kontrollen bei den Endnutzern des Schengener Informationssystems (SIS) vor. Wegen der förderalen Strukturen der Schweiz ist die Zuständigkeit für die Kontrollen zwischen dem Bund und den Kantonen aufgeteilt. Daher ist eine gemeinsame Kontrollmethode erforderlich.

Auf schweizerischer Ebene beaufsichtigen wir in Zusammenarbeit mit den kantonalen Datenschutzbehörden die im Rahmen der Nutzung des SIS durchgeführten Datenbearbeitungen. Wir koordinieren die Aufsichtstätigkeiten mit den kantonalen Behörden, arbeiten eng mit der Gemeinsamen Kontrollinstanz Schengen (GK) zusammen und sind auch deren nationaler Ansprechpartner.

Die GK beschliesst bisweilen die Einleitung von Kontrollen, für die sie um Massnahmen auf nationaler Ebene ersucht. Die betreffenden schweizerischen Behörden sind dann aufgefordert, eine koordinierte Untersuchung durchzuführen. Diese neue Aufgabe stellt zwei Probleme. Das eine betrifft die Methodik: Um die Kontrollen der verschiedenen Datenschutzbehörden koordinieren und vergleichen zu können, ist eine gewisse Einheitlichkeit bei der Methode erforderlich. Das zweite Problem liegt in der mangelnden Erfahrung: Manche kantonale Behörden verfügen nämlich nur über geringe Mittel zur Durchführung von Kontrollen.

Zur Lösung dieser Probleme und auf Wunsch der Kantone beschloss die Koordinationsgruppe der schweizerischen Datenschutzbehörden am 12. November 2009 die Einsetzung einer Arbeitsgruppe, bestehend aus Vertretern des EDÖB und mehrerer kantonaler Behörden, die die Koordination und Methodik der Kontrollen schriftlich festhalten soll.

Aus diesen Arbeiten resultierte ein Dokument, das die verschiedenen Rollen sowie die Etappen und Abläufe der koordinierten Kontrollen beschreibt. Es ist an der Sitzung der Koordinationsgruppe vom 16. September 2010 vorgelegt und verabschiedet worden (siehe auch Ziff. 1.4.5 des vorliegenden Tätigkeitsberichts).

1.4.5 Koordinationsgruppe der schweizerischen Datenschutzbehörden

Über die «Koordinationsgruppe der Schweizerischen Datenschutzbehörden im Rahmen der Umsetzung des Schengen-Assoziierungsabkommens» koordinieren wir unsere Tätigkeiten zur Beaufsichtigung der in der Schweiz in Anwendung der Schengen-Zusammenarbeit im Bereich Migration, Polizei und Justiz vorgenommenen Datenbearbeitungen mit den kantonalen Datenschutzbehörden.

Die Koordinationsgruppe der schweizerischen Datenschutzbehörden tagte am 16. September 2010. Bei diesem Treffen haben wir die kantonalen Datenschutzbehörden über die wichtigsten bei den Sitzungen der Gemeinsamen Kontrollinstanz Schengen (GK) behandelten Punkte und über ihre Tätigkeit informiert. Zudem haben wir unsere kantonalen Kollegen auch über die Ergebnisse unserer Kontrollen beim Schweizerischen Grenzwachtkorps sowie beim Schweizerischen Konsulat in Istanbul in Kenntnis gesetzt. Die Kantone ihrerseits stellten die Ergebnisse ihrer Kontrolltätigkeiten bei den kantonalen Nutzern des SIS vor (namentlich Bern, Basel-Stadt, Freiburg und Zug). Aufgrund der Resultate der verschiedenen Kontrollen und der Diskussionen der Koordinationsgruppe haben wir einige Fälle einer missbräuchlichen Nutzung des SIS zu privaten oder Ausbildungszwecken festgestellt. Um hier Abhilfe zu schaffen, hat die Koordinationsgruppe beschlossen, ein Schreiben herauszugeben, das die Nutzer des SIS auf Bundes- wie auf Kantonsebene für das Problem sensibilisieren soll. Schliesslich hat die Koordinationsgruppe ein Dokument für eine gemeinsame Methodik bei den zwischen unseren jeweiligen Behörden koordinierten Inspektionen geprüft und verabschiedet (siehe auch Ziff. 1.4.4 des vorliegenden Tätigkeitsberichts).

1.4.6 Entwurf zur Revision des BWIS an das Parlament überwiesen

Der Bundesrat hat einen Entwurf zur Revision des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) an das Parlament überwiesen. Dieser Entwurf sieht vor, das so genannte indirekte Auskunftsrecht durch das direkte zu ersetzen, und zwar entsprechend den in Artikel 8 und 9 des Datenschutzgesetzes (DSG) erwähnten Modalitäten.

Der Bundesrat hat im Oktober 2010 einen Entwurf zur Revision des BWIS an das Parlament überwiesen. Bezüglich des Auskunftsrechts hatte der in die Ämterkonsultation gegebene ursprüngliche Entwurf noch ein direktes Auskunftsrecht auf der Grundlage der Gesetzgebung über den Zugriff zu den Informationssystemen JANUS und GEWA

vorgesehen. Der Bundesrat ging nun einen Schritt weiter, indem er das direkte Auskunftsrecht in Anwendung von Artikel 8 und 9 DSG einführte. Dieser Vorschlag stellt einen ganz erheblichen Fortschritt für die Rechte der betroffenen Personen dar. Sie erhalten nämlich die Möglichkeit, Auskunft über die sie betreffenden Daten zu erhalten und gegebenenfalls ihren Anspruch auf Berichtigung geltend zu machen.

Bei den übrigen Punkten des Entwurfs bezweifeln wir immer noch die Notwendigkeit einer Revision des BWIS. Wir sind nämlich der Ansicht, dass die vorhandenen Instrumente des BWIS, des Strafgesetzbuchs und der Strafprozessordnung genügen, um die angestrebten Sicherheitsziele zu erreichen. Im Rahmen der Ämterkonsultation haben wir namentlich darum ersucht, darauf zu verzichten, die Bestimmungen auf Gesetzesebene zu verankern, welche die Ausdehnung der Auskunftspflichten und des Melderechts von Behörden, Amtsstellen und Organisationen zur Gewährleistung der inneren und äusseren Sicherheit betreffen. Diese Bestimmungen waren bisher in der Verordnung enthalten. Eine solche Ausdehnung stellt einen erheblichen Eingriff in die Grundrechte dar und muss somit den Grundsätzen der Notwendigkeit und der Verhältnismässigkeit genügen. Wir weisen einerseits darauf hin, dass die geltende Gesetzgebung bereits für zahlreiche Behörden die Pflicht zur Erteilung beziehungsweise das Recht zur Bekanntgabe von Auskünften vorsieht. Andererseits konnte der Bericht, in dem die konkreten Ergebnisse der erwähnten Verordnung ausgewertet werden sollten, eine Rechtfertigung der Ausdehnung von Auskunftspflichten und Melderecht, die über eine rein theoretische und psychologische Wirkung hinaus gegangen wäre, nicht nachweisen. Da die in der Gesetzesrevision vorgeschlagenen (und bereits in der Verordnung enthaltenen) Massnahmen die angestrebten Ziele nicht erreicht haben, müssen wir festhalten, dass entsprechende Bearbeitungen von Personendaten dem Grundsatz der Verhältnismässigkeit zuwider laufen. Wir begrüssen dagegen die Tatsache, dass die Massnahmen, die am stärksten in die Privatsphäre eingreifen, vorerst in dem an das Parlament überwiesenen Entwurf zur Revision des BWIS nicht mehr aufgeführt sind.

1.4.7 Auskunftsgesuche zum Informationssystem ISIS

Im Jahr 2010 war die Zahl der Auskunftsgesuche zum Informatisierten Staatsschutz-Informations-System (ISIS) ausserordentlich hoch. Die Flut von Gesuchen ist auf den im Sommer 2010 veröffentlichten Bericht der Delegation der Geschäftsprüfungskommissionen der eidgenössischen Räte (GPDel) über die Datenbearbeitung in ISIS zurück zu führen.

Im Jahr 2010 wurden bei unserem Sekretariat 407 so genannte indirekte Auskunftsgesuche zu ISIS eingereicht. Seit 1998 ist dies das zweite Jahr, in dem die Zahl der Gesuche weit über dem Durchschnitt (15 bis 20 Gesuche jährlich) liegt. Im Jahr 2008 gingen

im Anschluss an Fälle betreffend gewisse Mitglieder des Grossen Rates des Kantons Basel-Stadt (vgl. unseren 16. Tätigkeitsbericht 2008/2009, Ziff. 1.4.4) 148 Gesuche ein.

Der Bericht der GPDel vom 21. Juni 2010 über die Datenbearbeitung in ISIS äussert Zweifel bezüglich der Richtigkeit und der Erheblichkeit der bearbeiteten Personendaten und deckt gravierende Verzögerungen bei der Qualitätskontrolle, ja sogar deren Fehlen auf. Die Veröffentlichung des Berichts und die Reaktionen in den Medien führten zu einer massiven Zunahme der Anzahl indirekter Auskunftsgesuche zu ISIS.

Das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) sieht vor, dass wir dem Gesuchsteller grundsätzlich in einer stets gleich lautenden Antwort mitteilen, dass die Prüfung durchgeführt wurde, nicht aber, ob er in ISIS registriert ist. Nur ausnahmsweise können wir in angemessener Weise Auskunft erteilen, nämlich wenn damit keine Gefährdung der inneren oder äusseren Sicherheit verbunden ist und wenn dieser Person sonst ein erheblicher, nicht wieder gut zu machender Schaden erwächst. Die im Bericht beschriebene Situation sowie die Reaktionen und Kommentare in den Medien haben bei mehreren Personen eine gewisse Unsicherheit hervorgerufen. Wir haben für jedes Auskunftsgesuch geprüft, ob die Voraussetzungen für eine solche Ausnahmeantwort erfüllt seien, und konnten diese Regelung in sehr vielen Fällen anwenden. In diesem Rahmen standen wir in Verbindung mit dem Nachrichtendienst des Bundes. Die grosse Mehrheit der Personen, die ein Auskunftsgesuch eingereicht hatte, hat von uns im Dezember 2010 oder im Januar 2011 eine Antwort erhalten. Personen, die mit unserer Antwort nicht zufrieden sind, können verlangen, dass die Präsidentin der Abteilung I des Bundesverwaltungsgerichts unsere Mitteilung oder die Ausführung der von uns gegebenenfalls ausgesprochenen Empfehlung überprüft.

1.4.8 Pilotversuch: Informationssystem ISAS

Wir haben den Nachrichtendienst des Bundes (NDB) gebeten, uns die Datenbanken zu nennen, die vom Pilotversuch ISAS betroffen sind, und die Zahl der daran beteiligten Mitarbeitenden zu begrenzen. Nachdem uns der NDB diese Angaben vorgelegt hatte, konnten wir eine positive Stellungnahme zu diesem Pilotversuch abgeben.

Bei Pilotversuchen muss uns die dafür verantwortliche Instanz beim Bund mitteilen, wie gemäss ihrer Planung sichergestellt werden soll, dass die datenschutzrechtlichen Anforderungen erfüllt werden. Dazu muss sie unsere Stellungnahme einholen. Dies hat vor der Ämterkonsultation zu geschehen. Im Falle des Pilotversuchs ISAS hat uns der NDB nicht vor der Ämterkonsultation, sondern erst in deren Rahmen informiert. Die Bestimmungen über die Modalitäten der Bearbeitung von Personendaten im Rahmen dieses Pilotversuchs sind in der Verordnung über die Informationssysteme des NDB

enthalten, die auch das System ISIS regelt. Die Regelung einer Datensammlung, die bereits vollumfänglich im Einsatz ist (ISIS), und einer anderen in der Versuchsphase (ISAS) in ein und derselben Verordnung ist unseres Erachtens keine optimale Lösung. Es wäre sinnvoller gewesen, eine Verordnung eigens für den Pilotversuch auszuarbeiten. Dennoch haben wir geprüft, ob die gesetzlichen Anforderungen für einen Pilotbetrieb erfüllt sind, und kamen zu folgenden Resultaten:

Erstens müssen Aufgaben, die eine automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen erfordern, in einem Gesetz im formellen Sinn geregelt sein. Das Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) sieht vor, dass der NDB namentlich die Aufgabe hat, sicherheitspolitisch bedeutsame Informationen über das Ausland zu beschaffen und sie zuhanden der Departemente und des Bundes auszuwerten. Diese Aufgaben erfordern die automatisierte Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen. Die Bearbeitung der Gesamtheit der beschafften Daten ist in der Tat nur unter Anwendung eines automatisierten Verfahrens denkbar. Es ist auch klar, dass im Rahmen der Beschaffung dieser Informationen besonders schützenswerte Daten oder Persönlichkeitsprofile bearbeitet werden. Das ZNDG sieht für die erwähnten Aufgaben sogar ausdrücklich die Bearbeitung von Personendaten vor, einschliesslich besonders schützenswerter Personendaten und Persönlichkeitsprofile. Somit konnten wir feststellen, dass die erste Voraussetzung erfüllt ist.

Zweitens müssen geeignete Massnahmen getroffen werden, um Persönlichkeitsverletzungen zu verhindern. Die Verordnung über die Informationssysteme des NDB schreibt vor, dass die organisatorischen und technischen Massnahmen und die automatische Protokollierung der Datenbearbeitung in Bearbeitungsreglementen festgehalten werden. Da sich das Auskunftsrecht betreffend das Informationssystem ISAS nach den Artikeln 8 und 9 des Datenschutzgesetzes richtet, können die betroffenen Personen ihre Rechte, namentlich den Anspruch auf Berichtigung oder Löschung, ohne besondere Einschränkungen geltend machen. Der NDB hat uns wissen lassen, dass ein Datenschutz- und Informationskonzept ausgearbeitet werden soll. Wir begrüssen dies als für den Persönlichkeitsschutz der betroffenen Personen nützliche Massnahme. Um jedoch Persönlichkeitsverletzungen zu begrenzen, darf nur ein Teil der Personendaten und der vorgesehenen Nutzer in den Pilotversuch einbezogen werden. Im Falle des Pilotversuchs ISAS reicht es aus, wenn einige Datenbanken des Systems eingerichtet werden und nur die für die betreffenden Bereiche verantwortlichen Mitarbeiter die Daten bearbeiten können. Auf unseren Vorstoss hin musste uns der NDB im Nachhinein bekannt geben, welche Datenbanken bzw. welche Bereiche vom Pilotversuch betroffen sind, und die Zahl der zur Bearbeitung von Personendaten befugten Mitarbeiter beschränken. Gerade der zweiten Voraussetzung war zunächst nur teilweise entsprochen

worden. Als dann der NDB angab, dass nur zwei von sechs Bereichen (Terrorismus und Nichtverbreitung) hauptsächlich vom Pilotversuch betroffen und nur 20 % der Mitarbeiter des NDB beteiligt seien, konnte die Bedingung als erfüllt betrachtet werden.

Drittens ist ein Pilotversuch nur dann zulässig, wenn eine Versuchsphase vor Inkrafttreten eines Gesetzes im formellen Sinne es zwingend erfordert. Laut Angaben des NDB können zahlreiche technische und organisatorische Fragen im Zusammenhang mit seinen künftigen Arbeiten nur im Rahmen des Pilotversuchs ISAS geregelt werden. So wird auch die Frage eines etwaigen eingeschränkten Zugriffs der kantonalen Behörden auf ISAS analysiert werden. Es ist nicht ausgeschlossen, dass die mit dem Staatsschutz betrauten kantonalen Behörden für die Erfüllung ihrer gesetzlichen Aufgaben Zugang zu einer begrenzten Anzahl Daten in der ISAS-Datensammlung haben müssen. Die Leistungsfähigkeit eines neu eingerichteten Instruments für die Analyse (insbesondere das Sortieren zwischen ISAS und ISIS) und für die Auswertung der eingehenden Informationen muss zwangsläufig nachgeprüft werden. Wie wir also feststellen konnten, war auch diese dritte Voraussetzung erfüllt.

Abschliessend haben wir, die Einhaltung unserer Forderungen (Begrenzung der Bereiche wie auch der Anzahl Mitarbeiter) vorausgesetzt, eine positive Stellungnahme zum Pilotversuch ISAS abgegeben. Der NDB muss spätestens zwei Jahre nach der Durchführung der Versuchsphase dem Bundesrat einen Evaluationsbericht vorlegen. Wir haben den NDB gebeten, uns einen Zwischenbericht zu übermitteln.

1.4.9 Revision des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs

Das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) soll an die technische Entwicklung angepasst werden und ausdrücklich auch das Internet, also den E-Mail-Verkehr und die Internettelefonie, erfassen. Im Rahmen der Ämterkonsultation zur Revision des BÜPF haben wir zu diversen Punkten unsere Vorschläge eingebracht.

Wir haben bereits beim ersten uns vorgelegten Entwurf des BÜPF den sehr offen gefassten Geltungsbereich des Gesetzes bemängelt. Zwar wurde er bis zum Vernehmlassungsentwurf angepasst, jedoch sind die Ausführungen im erläuternden Bericht aus unserer Sicht noch immer zu offen formuliert.

Weiter halten wir den in der Strafprozessordnung (StPO) vorgesehenen Katalog von Straftatbeständen für den Einsatz von Trojanern auf Computern und anderen Kleingeräten (z.B. Smartphones) für zu umfassend, weil damit massiv in den Privat- und Intimbereich der Betroffenen eingegriffen wird. Nach der Installation des

Überwachungsprogramms kann nämlich nicht nur die Telekommunikation, sondern der gesamte Computer überwacht werden. Das beinhaltet den Zugriff auf alle gespeicherten – darunter auch zur Privat- oder Intimsphäre gehörende – Daten sowie auf die am Gerät vorhandenen Aufnahmegeräte (Mikrofone, Kameras). Wir haben in unserer Stellungnahme einen auf besonders wichtige Strafbestände reduzierten Katalog gefordert. Leider wurde dieses Begehren im Vernehmlassungsentwurf nicht berücksichtigt.

Der Gesetzesentwurf sieht weiter vor, dass ein Einsichts- und Auskunftsrecht für Personen besteht, die überwacht worden sind. Ihre nicht in ein Strafverfahren involvierten Kommunikationspartner werden jedoch nicht darüber informiert, dass über sie Daten im Rahmen solcher Überwachungsmassnahmen gespeichert wurden. Wir sind der Meinung, dass das Einsichts- und Auskunftsrecht auch für am Strafverfahren unbeteiligte Personen auf einfache Weise gewährt werden muss.

Vor dem Hintergrund des vom deutschen Bundesverfassungsgericht gefällten Urteils, das die Vorratsdatenspeicherung nur noch unter engen Voraussetzungen erlaubt, sollte die im Entwurf des BÜPF geplante Ausdehnung der Aufbewahrungsfrist für Randdaten von sechs auf zwölf Monate aus der Sicht der Verhältnismässigkeit erneut beurteilt werden.

Weiter begrüssen wir die datenschutzrechtlichen Bestimmungen, welche für das durch den Überwachungsdienst betriebene Informationssystem eingeführt werden sollen.

1.4.10 Internationale Rechtshilfeabkommen in Strafsachen mit Argentinien und mit Kolumbien

Anlässlich der Vernehmlassung zu den internationalen Rechtshilfeabkommen in Strafsachen mit Argentinien und Kolumbien erinnerten wir zum Einen an den Rahmenbeschluss über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Zum Anderen wiesen wir auf die von der EU angenommenen Datenschutz-Modellklauseln für bilaterale Verträge im Bereich der Strafverfolgung hin, welche für die Schweiz Gültigkeit haben. Wir empfahlen die Einfügung einer Musterklausel, in der die Datenschutzgrundsätze in den von der Schweiz mit Drittstaaten ausserhalb der EU abgeschlossenen bilateralen Verträgen im Bereich Strafverfolgung aufgeführt sind.

Bei der Vernehmlassung zu den internationalen Rechtshilfeabkommen in Strafsachen der Schweiz mit Argentinien und mit Kolumbien haben wir festgestellt, dass diese Abkommen keine Klausel betreffend den Schutz personenbezogener Daten enthalten. Wir erinnerten insbesondere an die Umsetzung des Rahmenbeschlusses 2008/977/JI

über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen bearbeitet werden, sowie an die Umsetzung der von der EU angenommenen Datenschutz-Modellklauseln für bilaterale Verträge im Bereich der Strafverfolgung. Diese Vorschriften wurden im Raum der Freiheit, der Sicherheit und des Rechts der EU entwickelt, an dem die Schweiz beteiligt ist. Sie dienen auch als Richtlinien beim Abschluss von internationalen Rechtshilfeabkommen in Strafsachen zwischen der Schweiz und Drittstaaten ausserhalb der EU.

Wir betonten, dass es unbedingt erforderlich sei, ein angemessenes Datenschutzniveau für personenbezogene Daten zu gewährleisten, die im Rahmen der Rechtshilfe in Strafsachen bearbeitet werden. So würde eine Datenschutz-Modellklausel in den bilateralen Verträgen im Bereich der Strafverfolgung einen generellen Verweis auf die nationale Gesetzgebung der beteiligten Staaten in Sachen Datenschutz ermöglichen. Gegebenenfalls könnte die Klausel die Anwendung der Grundsätze des Datenschutzes sicherstellen, wie sie vorgesehen sind im Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Bearbeitung personenbezogener Daten (STE 108) und in der Empfehlung 87/15 des Europarates zur Regelung der Verwendung von personenbezogenen Daten im Polizeibereich sowie in der Gesetzgebung der EU betreffend die in diesem Rahmen bearbeiteten personenbezogenen Daten. Es geht insbesondere darum, die Rechtmässigkeit der Bearbeitung von personenbezogenen Daten, die Abgrenzung ihrer Zweckbindung und ihre Verhältnismässigkeit, die Aktualität der ausgetauschten Daten sowie die Sicherheit und Vertraulichkeit bei der Übermittlung dieser Daten zu gewährleisten.

1.5 Gesundheit

1.5.1 Totalrevision des Epidemiengesetzes

Dank mehrfachem Hinweis von unserer Seite und entsprechender Stellungnahme in der Ämterkonsultation wurde im Rahmen der Totalrevision des Epidemiengesetzes (EpG) eine ausreichende gesetzliche Grundlage für den Datenschutz geschaffen. Dabei wurde erstmals auch der grenzüberschreitende Datenschutz für sensible Patientendaten geregelt.

Angesichts verschiedener Epidemien in den letzten Jahren (Sars, Vogelgrippe, Schweinegrippe) gelangten Leistungserbringer (Spitäler, Pflegeheime, Ärztinnen und Ärzte) sowie Luftfahrt- und Reisebranche immer wieder mit der Frage an uns, wie die anfallenden sensiblen Patientendaten im dringenden Fall einer Krankheit, die Epidemieform anzunehmen droht, datenschutzkonform bearbeitet werden dürfen. Uns wurde dabei klar, dass der Datenschutz bei solch überraschend und meist global auftretenden Krankheitsausbrüchen nicht ausreichend gesetzlich verankert ist. Wir haben deshalb beim Bundesamt für Gesundheit (BAG) mehrfach angeregt, im Dienste der öffentlichen Gesundheit die Gelegenheit zu nutzen, im Rahmen der Revision des EpG für eine ausreichende gesetzliche Grundlage zu sorgen. Im Rahmen der Ämterkonsultation konnten wir unsere Änderungswünsche anbringen.

Wie wir nun der Botschaft und dem Entwurf zum revidierten Bundesgesetz über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiengesetz, EpG) entnehmen durften, wurde die Regelung bezüglich des Datenschutzes den heutigen Erfordernissen angepasst: «Das Gesetz regelt den Zweck der Datenbearbeitung, die Aufbewahrungsdauer der Daten und den Datenaustausch zwischen den Vollzugsbehörden sowie den mit der Behandlung übertragbarer Krankheiten betrauten Ärztinnen und Ärzten und anderen Institutionen. Die Möglichkeiten und Grenzen der Datenbekanntgabe an ausländische Behörden sind ebenfalls entsprechend den Grundsätzen des Datenschutzes in das Gesetz aufgenommen worden.» Der Datenschutz verfügt mit dem totalrevidierten EpG und dessen zweiten Abschnitt über die Datenbearbeitung in diesem heiklen Gesundheitsbereich nun erstmals über eine ausreichende gesetzliche Grundlage.

1.5.2 eHealth: Wichtige Detaillierungskonzepte

Auch im Berichtsjahr gab es einige datenschutzrechtliche Herausforderungen im Grossprojekt eHealth Schweiz. Sowohl auf dem Gebiet der Informatik als auch des Rechts gab es wichtige Aktivitäten. Hervorzuheben sind hier das Rollenkonzept und die Empfehlung zur rechtlichen Regelung für die Umsetzung der Strategie eHealth.

Die Aktivitäten im Gesundheitswesen erzeugen eine Unmenge an Informationen über die Patientinnen und Patienten. Da es sich dabei mehrheitlich um Informationen über deren physischen und psychischen Zustand handelt, müssen strenge Vorschriften zum Schutz der Persönlichkeitsrechte der Betroffenen umgesetzt werden. Etablierte Schwächen in den Abläufen, und seien sie auch noch so beliebt, dürfen nicht ohne Korrektur in eHealth übernommen werden. Deshalb forderten wir von den Akteuren klare Aussagen darüber, welche Informationen sie für welche Aufgaben benötigen, und welche Rollen die jetzigen und die zukünftigen Prozesse am besten abdecken können. Das Ergebnis war ein bunter Katalog mit mehr oder weniger berechtigten Wünschen.

Die Fragestellung, wer was wofür von wem und wann benötige, ermöglichte es, die Forderungen der Akteure in eHealth zu ordnen. Aus den Antworten ergaben sich folgende Grundsätze für die Planung von und das Arbeiten in bzw. mit eHealth:

- Patienten und Behandelnde müssen zur Teilnahme an eHealth eindeutig authentifiziert sein.
- Relevant sind nur diejenigen Informationen, die das Wissen schaffen oder bestätigen, das für die Behandlung der Patienten notwendig ist.
- Jede Funktion in eHealth ist einer Rolle zugeordnet, die den Anspruch auf eine bestimmte Informationsmenge definiert.
- Informationen in eHealth dürfen nur solange in Registern publiziert werden, wie sie für Rollenträger relevant sind.

Die Empfehlungen zum Rollenkonzept und auch zu den Metadaten (Standards und Architektur Empfehlungen II) spiegeln diese Grundsätze wider.

Eine Expertengruppe hat dem Eidgenössischen Departement des Innern am 30. September 2010 ihren Bericht «Umsetzung Strategie eHealth Schweiz: Empfehlungen zur rechtlichen Regelung» übergeben. In unserer Stellungnahme dazu wiesen wir darauf hin, dass wir bezüglich der vorgeschlagenen mittelfristigen Massnahmen grosse Zweifel hegen, dass Artikel 117 der Bundesverfassung dem Bund die Kompetenz erteilt, auch für die öffentlich-rechtlichen Einrichtungen der Kantone verbindliche Vorgaben für das ePatientendossier zu erlassen. Dem Bund werde lediglich die Kompetenz zur

Regelung der Kranken- und Unfallversicherung erteilt. Das ePatientendossier stellt aber primär ein Werkzeug zur Gewährleistung des Informationsflusses entlang der Behandlungskette zum Patienten und nicht im eigentlichen Sinn ein Werkzeug zur Umsetzung der Krankenversicherung dar. Wenn überhaupt, so kann sich die Regelungskompetenz von Artikel 117 BV nur auf den Bereich der obligatorischen Krankenpflegeversicherung beziehen.

Ebenfalls kritisierten wir das System der Doppelten Freiwilligkeit. Es sieht vor, dass die Nutzung des ePatientendossier sowohl für Patienten als auch für Behandelnde freiwillig sein soll. Wir sind überzeugt, dass Vision und Ziel der Strategie eHealth eindeutig die informationelle Selbstbestimmung vorsehen. Sie zieht sich als roter Faden durch alle Ideen zur Umsetzung der eHealth-Strategie. Der Patient soll bestimmen, wer welche Daten über ihn in eHealth bearbeiten darf. Der Behandelnde kann also vorschlagen, eine behandlungsrelevante Information im ePatientendossier bereitzustellen; und er darf einen gleich lautenden Vorschlag des Patienten nicht ablehnen. Das Recht zur informationellen Selbstbestimmung des Patienten darf also auch durch den Behandelnden nicht eingeschränkt werden, es sei denn, ein formelles Gesetz sieht dies vor.

1.5.3 Versichertenkarte verunsichert weiterhin

Mit der Herausgabe der Versichertenkarte durch die Krankenkassen steigt die Verunsicherung in der Bevölkerung. Vermehrt gelangten Patientinnen und Patienten mit Fragen an uns.

Viele Krankenversicherungsgesellschaften haben in der Berichtsperiode mit dem Versand der Versichertenkarte begonnen. Dazu erhielten die Versicherten von ihrer Kasse eine «Gebrauchsanweisung» und die Nutzungsbedingungen. Sowohl die Karte als auch die Informationsbeilagen schafften allerdings nicht unbedingt Klarheit. Obwohl auch die verantwortlichen Organe, wie bspw. das Bundesamt für Gesundheit, regelmässig über die Versichertenkarte informiert haben, sind die Patientinnen und Patienten verunsichert, was zu mehreren Anfragen besorgter Bürger bei uns geführt hat. Ihre Hauptsorge ist, dass die «Gesundheitskarte» den Krankenkassen den Zugriff auf die Gesundheitsdaten der Versicherten ermögliche. Das ist durch das Gesetz natürlich nicht vorgesehen. Da aber jeder Krankenversicherer Herausgeber und Eigentümer seiner Versichertenkarten ist, besteht kaum eine abschliessende Garantie über Inhalt und Funktion der Karte.

Ebenfalls zu Fragen Anlass gab das Einwilligungsverfahren für die Übermittlung von Informationen über eine allfällige Zusatzversicherung an den Behandelnden während der Onlineabfrage. Die Verordnung zur Versichertenkarte sieht vor, dass die Abfrage nur mit dem Einverständnis der betroffenen Person erfolgen darf. Die Versicherer haben aus

Gründen der Einfachheit das Opt-out-Verfahren gewählt. Der Versicherte muss der Kasse schriftlich mitteilen, wenn während der Onlineabfrage kein Hinweis auf eine Zusatzversicherung erfolgen soll. Das ist aus unserer Sicht eher kein datenschutzfreundliches Verfahren. Allerdings, so die nachvollziehbare Argumentation der Kassen, ist die Zahl der Betroffenen, welche den Zugriff auf die Informationen zur Zusatzversicherung dem Behandelnden nicht gewähren wollen, so gering, dass sich der Mehraufwand für ein Opt-in nicht rechtfertigen würde.

Alles in Allem ist die Versichertenkarte aus datenschutzrechtlicher Perspektive weiterhin kritisch zu betrachten. Zu hoffen bleibt, dass mit der Entwicklung in eHealth aus der Versichertenkarte ein sinnvolles und auch für den Versicherten verständliches Instrument im Gesundheitswesen wird.

1.5.4 Referat vor dem Europarat in Strassburg über die Bearbeitung von Patientendaten

Der Europarat hat uns eingeladen, im Rahmen einer Versammlung des Komitees für bioethische Fragestellungen ein Referat über die Bearbeitung von Patientendaten zu halten. Im Zentrum stand die Frage, ob Regelwerke erforderlich sind, und wenn ja, welche. Es gelang uns, deutlich zu machen, dass der Umgang mit Gesundheitsdaten ohne gültige Regeln nicht zum Vorteil eines nationalen Gesundheitswesens sein kann.

Das Interesse an Gesundheitsdaten ist gross. Verschiedene Institutionen melden ihre Ansprüche für unterschiedliche Zwecke an. Diese Ansprüche können sich konkurrenzieren und sind nicht immer zu Gunsten der Patienten. Zwei Elemente sind für die Beurteilung der Notwendigkeit eines Regelwerks ausschlaggebend: Das erste ist die Motivation, die hinter solchen Begehrlichkeiten steht. Das zweite Element betrifft den Detaillierungsgrad der Gesundheitsdaten, der zur Erfüllung der jeweiligen Ansprüche erforderlich ist.

Die Motivation medizinischer und nicht-medizinischer Natur sein. Beim medizinischen Interesse steht im Vordergrund, Schäden an der Gesundheit einzelner Individuen oder einer Gruppe von Menschen zu erkennen und zu beheben. Das nicht-medizinische Motiv steht hinter Produkten, Verfahren und Systemen, die das Handeln im Interesse der Gesundheit des Einzelnen ermöglichen und unterstützen. Die Grenze zwischen den beiden Bereichen ist zwar fliessend, jedoch lassen sich die meisten Institutionen im Gesundheitswesen der Schweiz mindestens einem dieser Motive zuordnen. Die Ärztin, die bei einem Patienten eine Influenza diagnostiziert und behandelt, ist etwa dem ersten Bereich zuzuordnen. Das Informatikunternehmen, das ein System für die Verwaltung von Patientendaten entwickelt und vertreibt, handelt nach dem zweiten Motiv. Ein

Grundversicherer gehört grundsätzlich zur zweiten Gruppe, da er die Patientin nicht im eigentlichen Sinn medizinisch betreut, sondern für die Finanzierung von Leistungen zuständig ist. Allerdings nehmen sich die Versicherer vermehrt auch das Recht heraus, Behandlungsverfahren direkt zum Zweck der Kostenoptimierung zu beeinflussen. Dieses Beispiel zeigt, dass ein und dieselbe Institution sowohl aufgrund eines nicht-medizinischen als auch eines medizinischen Antriebs ein Interesse an Gesundheitsdaten haben kann.

Das zweite Element, der Detaillierungsgrad der (und damit die Menge an) Gesundheitsdaten, ist wesentlich schwieriger zu erfassen. Zu den begründeten Ansprüchen gesellen sich auch unnötige Begehrlichkeiten. Neben den für einen bestimmten Zweck wesentlichen Daten wird mit grosser Anstrengung ein Berg von unwesentlichen und überflüssigen Daten gehortet, und dies häufig nur aus einem Grund: Die Reduktion auf die notwendigen Daten ist mit Aufwand oder Prestigeverlust verbunden. Der Datenbearbeiter, ob Behandelnder, Informatikunternehmen oder Grundversicherer, muss sich auf die für den angestrebten Zweck absolut notwendigen Daten beschränken. Diese Beschränkung muss aber sowohl für den Datenbearbeiter als auch für die Patientin nachvollziehbar sein und darf nicht willkürlich erfolgen.

Wenn die Gesellschaft nicht akzeptieren will, dass Zugriff auf die Gesundheitsdaten erhält, wer ihn nur nachdrücklich genug fordert, muss sie verbindliche Regeln zu den Rechten und Pflichten bei der Bearbeitung der besonders schützenswerten Gesundheitsdaten erlassen.

1.5.5 Datenschutzaspekte bei Versandhandelsapotheken

Sachverhaltsabklärungen bei zwei Versandhandelsapotheken haben gezeigt, dass bei den kontrollierten Unternehmen ein gutes Verständnis für den Datenschutz herrscht und die notwendigen Vorkehrungen für den Schutz der Patientendaten getroffen werden. Hingegen bestehen Unklarheiten, welche Gesundheitsdaten die Versandhandelsapotheken zwingend bearbeiten müssen.

Im Berichtsjahr haben wir Sachverhaltsabklärungen bei zwei Versandhandelsapotheken durchgeführt. Ein Verfahren konnte vollständig abgeschlossen werden, während das zweite Verfahren kurz vor dem Abschluss steht. In beiden Fällen konstatierten wir, dass die Unternehmen sich der Sensibilität der von ihnen bearbeiteten Personendaten bewusst sind und entsprechend auch die notwendigen Vorkehrungen für die Gewährleistung von Datenschutz und Datensicherheit getroffen haben. Insbesondere konnten wir feststellen, dass bei beiden Unternehmen eine klare Trennung von administrativen Daten und Gesundheitsdaten erfolgt. So haben Mitarbeiterinnen und

Mitarbeiter nur Zugriff auf Gesundheitsdaten, wenn es für ihre Aufgabe wirklich notwendig ist. Hingegen erkannten wir, dass Unklarheiten bestehen, welche Gesundheitsdaten aufgrund der gesetzlichen Qualitäts- und Sicherheitsbestimmungen zwingend bearbeitet werden müssen. Diese Frage ist entscheidend für die Beurteilung der Pflicht zur Anmeldung einer Datensammlung in unserem öffentlich zugänglichen Register (www.datareg.admin.ch).

1.5.6 DVD eines Privatspitals mit Operationsbildern

Ein Privatspital hat unbeabsichtigt einem Patienten eine DVD ausgehändigt, die nicht nur die ihn betreffenden Bilddaten, sondern auch diejenigen von 17 weiteren Patientinnen und Patienten enthielt. Die Bilddaten waren mit ergänzenden Angaben wie Name der Betroffenen, operierender Arzt, Art des Eingriffs und Datum versehen.

Der Angehörige eines Privatklinik-Patienten hat uns schriftlich darüber in Kenntnis gesetzt, dass dem Patienten eine DVD ausgehändigt worden war, die nicht nur seine Operationsdaten enthält, sondern auch die Operationsdaten von 17 weiteren Patienten. Er hat uns die DVD zugestellt. Aufgrund der schweren Datenschutzverletzung haben wir sofort eine Sachverhaltsabklärung mit Augenschein vor Ort durchgeführt.

Die Sachverhaltsabklärung und insbesondere der Augenschein zeigten, dass der Datenschutzverletzung eine unbeabsichtigte Fehlbearbeitung der Operationsdaten durch das Pflegepersonal am Videoturm im Operationssaal zugrunde lag. Ein Mitarbeiter des Spitals hatte unabsichtlich alle auf dem Videoturm gespeicherten Daten selektioniert und auf die DVD kopiert, die dem Patienten nach der Operation abgegeben wurde. Der Augenschein zeigte uns, dass eine derartige Fehlbearbeitung aufgrund der Benutzeroberfläche des Videosystems sehr leicht erfolgen kann. Die Privatklinik hat in der Folge sämtliches Personal, das an den Videotürmen eingesetzt wird, einer spezifischen Schulung unterzogen und dabei konkret auf die Gefahr der unbeabsichtigten Selektion von Bilddateien hingewiesen. Aufgrund unserer Intervention hat die Klinik zudem alle betroffenen Patientinnen und Patienten über den Vorfall informiert.

Aufgrund der Vorkehrungen der Privatklinik zwecks Verhinderung von derartigen Datenschutzverletzungen haben wir auf eine Empfehlung verzichtet. Der Vorfall zeigt jedoch, dass wir von «security by design» bei Datenbearbeitungssystemen noch weit entfernt sind. Dies ist angesichts der Tatsache, dass solche Videotürme in zahlreichen Kliniken in der Schweiz verwendet werden, besonders bedenklich.

1.5.7 Outsourcing trotz Patientengeheimnis?

Gemäss Datenschutzgesetz kann eine Auftragsdatenbearbeitung – oftmals als Outsourcing bezeichnet – nur dann stattfinden, wenn keine gesetzliche Geheimhaltungspflicht es verbietet. Gerade im medizinischen Bereich stellt sich die Frage, ob das Patientengeheimnis eine Auftragsdatenbearbeitung zulässt.

Das Patientengeheimnis, verankert im Schweizerischen Strafgesetzbuch, stellt eine gesetzliche Geheimhaltungspflicht dar. Trotzdem ist die Auftragsdatenbearbeitung bei Ärzten und Kliniken eine alltägliche Praxis. Wir analysierten die gesetzlichen Grundlagen intensiv und baten schliesslich das Bundesamt für Justiz (BJ) um eine Stellungnahme zur Klärung.

Das BJ stellte sich auf den Standpunkt, dass die von Ärztinnen und Ärzten oder Kliniken beauftragten Datenbearbeiter als Hilfspersonen zu betrachten sind. Dieser Blickwinkel führt dazu, dass es sich gar nicht um eine Auftragsdatenbearbeitung im Sinn des Datenschutzgesetzes handelt und damit auch das Patientengeheimnis nicht tangiert wird. Somit braucht es für die Übertragung der Datenbearbeitung an die Hilfsperson auch keine Einwilligung des Patienten. Immerhin definierte das BJ in seiner Stellungnahme die Voraussetzungen, unter denen die beauftragte Person als Hilfsperson betrachtet werden kann, nämlich eine sorgfältige Auswahl, Instruktion und die konkrete Möglichkeit zur Überwachung und zum Erteilen von Weisungen. Sind diese Voraussetzungen erfüllt, gilt die beauftragte Person als Hilfsperson.

Wir erachten diese Lösung als problematisch und für die Ärztinnen und Ärzte oder Kliniken als risikoreich. Sie führt dazu, dass die konkreten Mitarbeiterinnen und Mitarbeiter eines Unternehmens als Hilfspersonen des Arztes betrachtet werden sollten, obwohl der Arzt diese Personen mit grösster Wahrscheinlichkeit gar nicht kennt. Es muss jedoch davon ausgegangen werden, dass juristische Personen grundsätzlich nicht als Hilfspersonen betrachtet werden können. Wir empfehlen Ärzten und Kliniken daher das Einholen der Einwilligung der Patienten für die Auftragsdatenbearbeitung.

1.5.8 Anforderungen an ein Diagnoseregister

Der Bund plant die gesetzliche Regelung eines Diagnoseregisters, das in einem ersten Schritt die Diagnose Krebs berücksichtigen soll. Die Planung eines solchen Registers stellt hohe datenschutzrechtliche Anforderungen. Wir haben uns in der Arbeitsgruppe entsprechend engagiert.

Wir haben in den letzten zwei Jahren in einer Arbeitsgruppe mitgearbeitet, welche die Schaffung bundesgesetzlicher Grundlagen für die Führung von Diagnoseregistern durch den Bund geprüft hat.

Dabei steht in einem ersten Schritt vor allem die Registrierung von Krebserkrankungen im Vordergrund. Die rechtliche Situation ist diesbezüglich in den Kantonen sehr heterogen. Nur die Krebsregister in den Kantonen Tessin, Jura und Luzern verfügen über eine gesetzliche Grundlage. Insgesamt bestehen aber laut Bundesamt für Gesundheit zurzeit elf kantonale bzw. regionale Register, welche 22 Kantone umfassen. Alle Register verfügen über eine generelle Registerbewilligung der Eidgenössischen Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung.

Register, welche flächendeckend alle Neuerkrankungen einer bestimmten Krankheit erfassen und ihren Verlauf verfolgen, erlauben einerseits zuverlässige Angaben zur Häufigkeit bestimmter Erkrankungen im Zeitverlauf und zur Veränderung von Risikoprofilen (krankheitsverursachende Kombination von Risikofaktoren). Anderseits bilden sie für verschiedene Erkrankungen die Grundlage für die Ermittlung von Qualitätsindikatoren. Insbesondere bei Krebs, aber auch bei anderen chronischen Erkrankungen, in deren Behandlung und Betreuung verschiedene Leistungserbringer involviert sind, kann mit Hilfe von Registern die Qualität der ganzen Behandlungskette abgebildet werden. In den Arbeiten wurde dabei die Notwendigkeit der Meldepflicht eines Mindestdatensatzes festgehalten, damit der angestrebte Erfassungsgrad von mindestens 90 % aller Neuerkrankungen erreicht werden kann.

Die Schaffung eines Diagnoseregisters birgt viele datenschutzrechtliche Herausforderungen, und wir haben uns in der Arbeitsgruppe entsprechend eingebracht. Die Persönlichkeit der betroffenen Menschen muss gut geschützt und bei der technischen Ausgestaltung berücksichtigt werden.

Wir hatten die Gelegenheit, uns auch in der Ämterkonsultation zum Bundesratsantrag betreffend Registrierung von Krebs und anderen Diagnosen zu äussern. Wir vertraten dabei die Ansicht, dass die Entscheidung über die Aufnahme weiterer Diagnosen Aufgabe des Gesetzgebers ist. Nur so erachten wir den politischen Diskurs unter Einbezug

der betroffenen Interessenvertreter als gewährleistet und die mit einem Monitoring (Meldepflicht des Mindestdatensatzes) verbundenen Einschränkungen der Persönlichkeitsrechte als demokratisch legitimiert. Dieses Anliegen ist für uns zentral.

Weiter haben wir uns zur Formulierung der Zweckbestimmung geäussert. Sie muss sorgfältig vorgenommen werden. Wir widersetzen uns einer zu weiten Fassung; je weiter nämlich die Zweckbestimmung in einem Gesetz formuliert wird, desto mehr Datenbearbeitungen können darunter fallen, ohne dass dies für die betroffenen Personen klar ersichtlich wäre.

Der Mindestdatensatz, der einer Meldepflicht unterliegen soll, muss möglichst klein gehalten werden. Wir vertreten dabei die Ansicht, dass hierzu ein rollenbasierter Ansatz gewählt werden müsste: Je nach Leistungserbringer (Labor, Arzt, Spital etc.) muss der minimale Datensatz angepasst werden.

Der Bundesrat hat am 03. Dezember 2010 dem Eidgenössischen Departement des Innern den Auftrag erteilt, bis im Frühjahr 2012 einen Vorentwurf für das Gesetz zu erarbeiten. Wir werden diese Arbeiten weiter beobachten und gegebenenfalls Stellung dazu nehmen.

1.5.9 Kontrolle eines Krebsregisters

Auch wenn ein Krebsregister im Besitz einer generellen Bewilligung der Expertenkommission ist, muss der Arzt die Einwilligung bei den betroffenen Krebspatienten einholen, soweit dies möglich und zumutbar ist. Nur in den Fällen, in denen bspw. der Patient nicht mehr auffindbar ist oder die Einholung seiner Einwilligung für ihn unzumutbar wäre, darf sich der Arzt, welcher die Daten an das Krebsregister weiterleitet, auf die generelle Bewilligung der Expertenkommission abstützen. Bei der Kontrolle des Registers konnten wir auch feststellen, dass nur ein Teil der Aufgabenerfüllungsprozesse dokumentiert war und nicht alle Datensicherheitsmassnahmen dem Stand der Technik entsprachen.

Bei der Kontrolle eines Krebsregisters haben wir festgestellt, dass die Betreiber irrtümlich davon ausgegangen sind, die generelle Registerbewilligung der Expertenkommission erlaube es, die Personendaten der Krebspatienten ohne deren Einwilligung zu erheben. Dies entspricht aber nicht den normativen Vorgaben. Die behandelnde Ärztin muss den Patienten über die Forschungstätigkeiten aufklären; nach einer Bedenkfrist kann dann seine Einwilligung eingeholt werden. Antwortet ein Patient auf eine entsprechende Anfrage nicht, darf dies als stillschweigende Einwilligung ausgelegt werden. Können Patienten nicht persönlich kontaktiert werden, bspw. weil ihre Adressen nicht mehr auffindbar sind oder eine grosse Anzahl von Personen betroffen ist, so gilt es als

nicht möglich bzw. nicht zumutbar, die Einwilligung einzuholen. In solchen Fällen gilt lediglich die erwähnte Aufklärungspflicht, in der auf die Möglichkeit hingewiesen wird, die Verwendung von Daten zu Forschungszwecken zu untersagen. Dann kann sich das Krebsregister (bzw. der behandelnde Arzt für die Weitergabe der Patientendaten an das Krebsregister) auf eine generelle Registerbewilligung der Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung berufen und die Daten dieser Patienten zu Forschungszwecken verwenden, sofern diese nicht ihr Veto eingelegt haben. Zu diesem Aspekt nahm die Expertenkommission in ihrem Tätigkeitsbericht der Jahre 2001-2004 unter dem Titel «Verwechslungsgefahr zwischen Pflicht zur Aufklärung und Pflicht zur Einholung der Einwilligung» Stellung (www.bag.admin.ch).

Wir haben auch darauf hingewiesen, dass die Krebspatienten nur dann rechtsgültig einwilligen können, wenn für sie erkennbar ist, wie ihre Daten bearbeitet werden. Die Aufklärung muss deshalb verständlich erfolgen. Dem betroffenen Patienten muss namentlich aufgezeigt werden, wie seine Daten erhoben und pseudonymisiert werden und dass danach die Forschungsarbeiten mit den anonymen Daten durchgeführt werden. Zusätzlich muss der Betroffene darüber informiert werden, dass der Abgleich mit den anderen Krebsregistern mit den identifizierenden Daten vorgenommen wird. Eine Zuordnung der Daten wäre aber auch mit Pseudonymisierungsverfahren möglich. Auf diese Möglichkeit haben wir schon in den vorhergehenden Tätigkeitsberichten aufmerksam gemacht. Kann ein Forschungsprojekt nicht mit anonymen Daten durchgeführt werden, weil bspw. noch zusätzliche Daten beim Krebspatienten erhoben werden müssen, ist die Einwilligung bei den Betroffenen für dieses Forschungsprojekt einzuholen. Den betroffenen Patienten müssen mindestens die folgenden Informationen unterbreitet werden, damit sie eine rechtsgültige Einwilligung unterzeichnen können: der Verantwortliche und Leiter des Forschungsprojekts, dessen Zweck, die Art und Weise der Datenbearbeitung, der Personenkreis, der von den personenbezogenen Daten Kenntnis erhält, und das Datum der Anonymisierung oder Vernichtung der Daten.

Im Weiteren sind die betroffenen Patienten auf ihr Recht, die Einwilligung zu widerrufen und Auskunft über bzw. Einsicht in die sie betreffenden Daten zu erlangen, hinzuweisen. Wir haben auch gefordert, dass die Prozesse von der Erhebung der Personendaten bis zu deren Anonymisierung oder Löschung zu dokumentieren sind. Sonst ist nicht nachvollziehbar, wie die Aufgabenerfüllung und die Datenbearbeitung abläuft (mangelnde Transparenz).

Für die Bearbeitung von besonders schützenswerten Personendaten ist bei den Sicherheitsmassnahmen der Stand der Technik umzusetzen. In diesem Bereich haben wir festgestellt, dass bei der elektronischen Datenübermittlung die Daten nicht immer

verschlüsselt wurden oder ein Verschlüsselungssystem eingesetzt wurde, das noch Schwächen aufwies. Zusätzlich haben wir auch darauf aufmerksam gemacht, dass die Personendaten (identifizierende Daten) auf den Datenspeichern (insb. Festplatten) zu verschlüsseln sind und dass beim Einloggen in das System eine zwei-Faktoren-Authentifizierung vorzusehen ist, bspw. durch den Einsatz einer Chipkarte (Besitz) und der Eingabe einer PIN (Wissen). Zudem ist es auch sinnvoll, dem Benutzer beim Einloggen am Bildschirm anzuzeigen, wann er das letzte Mal ausgeloggt hat. Mit Hilfe dieser Information kann er feststellen, ob jemand seinen Account benutzt hat.

Bezüglich Protokollierung mussten wir feststellen, dass diese zuwenig umfassend gestaltet war. Ihr Zweck besteht darin, die Nachvollziehbarkeit der Bearbeitung der Personendaten zu gewährleisten. Aus Sicht des Datenschutzes geht es insbesondere darum, wer wann welche personenbezogenen Daten zu welchem Zweck in welcher Weise bearbeitet hat. Überdies müssen die Protokolldaten so aufgezeichnet werden, dass sie durch Analysewerkzeuge ausgewertet werden können. Es ist auch darauf zu achten, dass die Protokollierung möglichst pseudonym und revisionssicher erfolgt.

1.5.10 Forschung und Datenschutz

Wir haben an einer Konferenz in Brüssel teilgenommen, an der wir uns mit dem Datenschutz in der medizinischen Forschung befassten. In diesem Bereich werden in den nächsten Jahren neue Herausforderungen auf uns zukommen.

Häufig stellt das internationale Umfeld von Forschungsprojekten in rechtlicher Hinsicht komplexe Anforderungen an die Projektleitenden. Auch in diesem Berichtsjahr konnten wir verschiedene Unternehmen bei der Umsetzung der datenschutzrechtlichen Bedingungen in diesem Bereich beraten.

Im November nahmen wir an der internationalen Konferenz «Privacy and Scientific Research: from obstruction to construction» in Brüssel teil. Die Konferenz wurde von der belgischen Datenschutzbehörde im Rahmen des belgischen Vorsitzes des EU-Rates organisiert. Das Programm legte zwei Schwerpunkte fest: Datenschutz einerseits in der medizinischen, anderseits in der historischen Forschung. Wir haben uns auf die medizinischen Aspekte der Konferenz beschränkt, da geschichtliche Forschung in der Schweiz vor allem durch Universitäten betrieben wird, welche im Zuständigkeitsbereich der kantonalen Datenschutzbehörden liegen.

In den Arbeitsgruppen wünschten einige Vertreter von Unternehmen der Pharmabranche wenigstens für den europäischen Raum eine gewisse Vereinheitlichung in der nationalen Umsetzung der EU-Datenschutzrichtlinien, beispielsweise bei der Durchführung

von klinischen Versuchen. Ebenfalls wurde die höchst unterschiedliche Qualität der Beratung durch lokale Datenschutzbehörden kritisiert.

Interessant waren auch die Vorträge über die genetische Forschung. Die Entwicklungen in diesem Bereich sind enorm, während die Kosten für genetische Untersuchungen immer mehr sinken. Dies stellt den Datenschutz vor neue Herausforderungen.

Die Konferenz wurde mit Empfehlungen an die gesetzgebenden Behörden, die Forschenden, die Archive und die Datenschutzbehörden geschlossen. Von den gesetzgebenden Behörden wurde gefordert, die Bestimmung der Begriffe Identität, Anonymität, Identifizierung international zu harmonisieren. Im Kontext der medizinischen Forschung sei das Konzept der absoluten Anonymität Unsinn.

Forschende sollten sich Kenntnisse darüber aneignen, wie Personendaten im medizinischen Bereich datenschutzkonform bearbeitet werden, und sich bei Bedarf von den zuständigen Datenschutzbehörden beraten lassen. Diese Behörden wurden zur Koordination ihrer Tätigkeit mit derjenigen der Ethikkommissionen aufgefordert.

Dies sind nur einige Bemerkungen zur Konferenz, bei der wir auch praktische Umsetzungshilfen erfahren haben. Die Dokumentation der Konferenz ist unter folgendem Link im Internet publiziert: www.privacyandresearch.be

1.5.11 Datenschutz im Bereich der genealogischen Forschung

Ein Forschungsprojekt verfolgt das Ziel, den Stammbaum (Genealogie) von Personen mit einer seltenen genetischen Krankheit zu erstellen. Wir haben die Projektverantwortlichen auf gewisse problematische Punkte aufmerksam gemacht, die unter dem Gesichtspunkt des Datenschutzes zu berücksichtigen sind.

Wir sind zu einem Forschungsprojekt um Rat angegangen worden, bei dem die Genealogie von Personen mit einer bestimmten seltenen genetischen Krankheit erstellt werden soll. Ziel des Projekts ist es, über genealogische Nachforschungen die Verwandten solcher Patienten zu finden, um sie über etwaige Risiken für ihre Gesundheit zu informieren. Diese Krankheit ist schwierig zu diagnostizieren, kann jedoch medikamentös behandelt werden. Ohne eine Behandlung sinkt die Lebenserwartung der an dieser Krankheit leidenden Personen deutlich.

Das Bundesgesetz über den Datenschutz sieht vor, dass der Inhaber der Datensammlung verpflichtet ist, die betroffene Person über die Beschaffung von besonders schützenswerten Daten zu informieren. Die Tatsache, dass die für das Projekt verantwortliche Gesellschaft den Stammbaum eines Patienten mit dieser genetischen Krankheit erstellt und die Familienangehörigen potentiell Träger dieser Krankheit sind, bedeutet,

dass besonders schützenswerte Daten anfallen. In diesem Fall muss die Benachrichtigung der Personen spätestens bei der Erfassung der Daten erfolgen oder, wenn sie nicht erfasst werden, bei der ersten Bekanntgabe der Daten an einen Dritten. Das fragliche Projekt sieht indessen eine Information über ein Rundschreiben erst bei Abschluss des Projekts vor, also nach dem gesetzlich vorgeschriebenen Zeitpunkt. Überdies führt dies zu einem Konflikt mit dem Recht einer Person auf Nichtwissen bezüglich ihrer genetischen Konstitution, wie es im Bundesgesetz über genetische Untersuchungen beim Menschen vorgesehen ist. Die Kenntnisnahme von solchen Informationen kann nämlich äusserst schwerwiegende Folgen für den psychischen Gesundheitszustand der Person haben und ihre Lebensweise und ihren Lebensplan nachhaltig beeinflussen.

Wir haben den Projektverantwortlichen auf diese Problematik aufmerksam gemacht und werden das Projekt weiter begleiten.

1.6 Versicherungen

1.6.1 Missbrauchsbekämpfung bei Motorfahrzeugversicherungen

Die Motorfahrzeugversicherungen betreiben eine elektronische Datenplattform zur Bekämpfung des Versicherungsmissbrauchs. Wir haben diese Plattform geprüft und konnten feststellen, dass das System grundsätzlich datenschutzkonform angelegt ist. Sind bei bestimmten Punkten noch Verbesserungen nötig, erarbeiten wir mit den Beteiligten pragmatische Lösungen.

Der «Car Claims Information Pool» (CC-Info) ist eine Plattform für den elektronischen Datenaustausch. Er bezweckt die Bekämpfung des Missbrauchs im Bereich der Motorfahrzeugversicherung. CC-Info wurde von einer dem Schweizerischen Versicherungsverband nahe stehenden Gesellschaft konzipiert. Diverse grosse Motorfahrzeugversicherungen sind an dem Pool beteiligt. Die informatiktechnische Umsetzung findet im Rechenzentrum der Bedag Informatik AG in Bern statt, wobei die teilnehmenden Versicherungen über das Internet Zugriff auf die Daten haben.

Wir haben die Datenbearbeitung im Rahmen von CC-Info einer vertieften Sachverhaltsabklärung unterzogen und können als positives Zwischenfazit festhalten, dass alle Beteiligten ein adäquates Verständnis für datenschutzrechtliche Anliegen zeigen und insbesondere geeignete technische und organisatorische Massnahmen ergriffen haben.

Wir stehen weiter in Kontakt mit den Beteiligten, um zusammen sachgerechte und sinnvolle Antworten auf Detailfragen zu finden, bei denen wir noch Verbesserungspotential sehen.

1.6.2 Videoaufzeichnungen im öffentlichen Verkehr: Weitergabe an Haftpflichtversicherer

Die mittlerweile in vielen Transportmitteln installierten Kameras sollen dem Schutz der Reisenden, des Betriebs und der Infrastruktur dienen. Die dabei gesammelten Daten wecken jedoch weitere Begehrlichkeiten. Der gesetzliche Rahmen setzt hier klare Grenzen.

Ein Haftpflichtversicherer zahlreicher öffentlicher Verkehrsbetriebe erbat unsere Stellungnahme zur Frage, ob ihm Transportunternehmungen zur Beurteilung der Haftung bei Fahrgastunfällen Einsicht in die Aufzeichnungen von in den Verkehrsmitteln installierten Videoanlagen gewähren dürfen.

Die gesetzliche Regelung der Videoüberwachung in öffentlichen Verkehrsmitteln findet sich im Eisenbahngesetz, im Bundesgesetz über die Personenbeförderung und insbesondere in der Verordnung über die Videoüberwachung im öffentlichen Verkehr. Obwohl die dort getroffene Regelung grundsätzlich abschliessend ist und als Spezialvorschrift allfällig abweichenden generelleren Erlassen vorgeht, ist sie doch im Licht der Prinzipien und Wertungen des Datenschutzgesetzes zu interpretieren.

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Damit soll sichergestellt werden, dass bereits bei der Datenbeschaffung für die betroffene Person feststeht, wie und wozu die sie betreffenden Daten bearbeitet werden. Nur so kann sie überhaupt entscheiden, ob sie sich dieser Bearbeitung unterziehen will; nur so kann sie ihr Grundrecht auf informationelle Selbstbestimmung wirksam ausüben.

Der Gesetzgeber hat festgelegt, dass in öffentlichen Verkehrsmitteln Videoüberwachung zum Schutz der Reisenden, des Betriebs und der Infrastruktur zulässig ist. Die Beurteilung von Haftpflichtansprüchen aus Fahrgastunfällen wird von dieser Zweckbestimmung klar nicht umfasst, und die gesetzliche Regelung sieht eine Bekanntgabe der Videoaufzeichnungen an private Dritte (wie etwa eine Haftpflichtversicherung) folgerichtig auch nicht vor. Die Aufzeichnungen dürfen nur den Strafverfolgungsbehörden sowie den Behörden, bei denen die Unternehmen Anzeige erstatten oder Rechtsansprüche verfolgen, zugänglich gemacht werden, soweit dies für ein Verfahren erforderlich ist. Wer Videosignale unter Verletzung dieser Vorschriften nutzt oder bekannt gibt, macht sich sogar strafbar.

Eine Weitergabe von Videoaufzeichnungen durch Transportunternehmen an ihre Haftpflichtversicherer ist nach geltendem Recht daher nicht zulässig. Hingegen dürfen die Aufzeichnungen in Verfahren betreffend die Verfolgung (bzw. Abwehr) von Rechtsansprüchen den zuständigen Behörden (namentlich: Gerichten) soweit erforderlich im Rahmen des anwendbaren Verfahrensrechts zugänglich gemacht werden.

Ein weiterer Bericht zum Thema Videoüberwachung im öffentlichen Verkehr befindet sich in Ziff. 1.2.3 des vorliegenden Tätigkeitsberichts.

1.6.3 Missbrauch von Kundendaten für Marketingzwecke durch Krankenversicherer

Mehrere Krankenversicherer haben versicherte Personen mit einer bestimmten Medikation direkt angeschrieben und sie auf günstigere gleichartige Medikamente hingewiesen. Dieses Vorgehen mag aufgrund des Kostendrucks im Gesundheitswesen zwar als sinnvoll erscheinen, stellt aber eine Datenschutzverletzung dar.

Aufgrund des Hinweises des rechtlichen Vertreters eines Pharmaherstellers führten wir bei mehreren Krankenversicherern Sachverhaltsabklärungen durch. Der Vorwurf ging dahin, dass die Versicherer die Personendaten von Versicherten mit einer bestimmten Medikation verwendeten, um sie schriftlich auf günstigere Medikamente hinzuweisen, die für sie ebenfalls geeignet sein könnten.

Krankenkassen, die im Bereich der obligatorischen Krankenversicherung tätig sind, gelten als Bundesbehörden, weil sie eine öffentliche Aufgabe des Bundes vollziehen. Entsprechend gilt für sie das Legalitätsprinzip; sie dürfen Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. Besonders schützenswerte Personendaten dürfen sie nur bearbeiten, wenn ein Gesetz im formellen Sinn das ausdrücklich vorsieht. Das Bundesgesetz über die Krankenversicherung hält fest, für welche Zwecke die Krankenversicherer Personendaten (auch besonders schützenswerte) bearbeiten dürfen. Das direkte Anpreisen von Medikamenten gehört nicht zu den gesetzlich vorgesehenen Bearbeitungszwecken und stellt somit eine Datenschutzverletzung dar.

Aufgrund unserer Intervention stellten fast alle Krankenversicherer, die tatsächlich derartige Marketingaktionen durchgeführt hatten, diese Praxis ein. Mit einer Krankenkasse musste unter Beizug der verantwortlichen Personen des Bundesamtes für Gesundheit eine klärende Sitzung durchgeführt werden. Danach verzichtete auch sie auf diese Art von Marketing.

1.7 Arbeitsbereich

1.7.1 Zentralisierung von Human Resources im Ausland

Internationale Unternehmen führen vermehrt zentralisierte Human-Resources-Abteilungen. Als Folge davon werden schweizerische Tochtergesellschaften immer häufiger dazu aufgefordert, die Personendaten ihrer Angestellten an die Muttergesellschaft ins Ausland bekannt zu geben.

Zahlreiche internationale Unternehmen gehen dazu über, nur noch eine Personalabteilung zu führen oder zumindest bestimmte Teile der Personaladministration durch einen zentralen Dienst erledigen zu lassen. Zahlreiche für die Personaladministration zuständige Mitarbeiterinnen und Mitarbeiter in schweizerischen Tochtergesellschaften waren mit dieser Entwicklung konfrontiert und erkundigten sich bei uns, ob und unter welchen Voraussetzungen die Übermittlung von Personaldaten ins Ausland zulässig ist.

Die Übermittlung von Personendaten von der Tochtergesellschaft an die Muttergesellschaft stellt eine Datenbekanntgabe an eine dritte Person dar, und die Regeln des Datenschutzgesetzes für die grenzüberschreitende Bekanntgabe von Personendaten müssen befolgt werden. Je nach Standort der Muttergesellschaft müssen für die Datenbekanntgabe aus der Schweiz unterschiedliche Vorkehrungen getroffen werden. Gerade bei der Datenbekanntgabe in die USA, welche besonders oft Inhalt der Anfragen war, müssen alternativ drei Voraussetzungen erfüllt sein, weil die USA keinen ausreichenden Datenschutz gewährleistet. Entweder hat sich das datenempfangende Unternehmen beim Handelsministerium der USA gemäss «U.S.-Swiss Safer Harbor Framework» zertifiziert, oder es wurde ein Vertrag geschlossen, der einen angemessenen Datenschutz gewährleistet, oder die betroffenen Personen haben eingewilligt. Befindet sich das datenempfangende Unternehmen in einem Staat, der einen angemessenen Datenschutz gewährleistet, so kann die Bekanntgabe aus der Schweiz ohne diese Vorkehrungen erfolgen. Grundsätzlich gilt aber auch hier das Transparenzprinzip. Die Angestellten der schweizerischen Tochtergesellschaft müssen über die Datenbekanntgabe ins Ausland informiert werden.

1.7.2 Biometrisches Erkennungssystem für Mitarbeitende

Ein Unternehmen hat ein neues Badge-System mit biometrischer Erkennung mittels Fingerabdrücken eingeführt. Dabei soll der Badge einerseits zur Zutrittskontrolle eingesetzt werden, andererseits auch den Zugang zu allen passwortgeschützten IT-Anwendungen ermöglichen. Wir haben das System, das sich in der Pilotphase befindet, vor Ort angeschaut und konnten dabei feststellen, dass es die datenschutzrechtlichen Anforderungen erfüllt.

Das Unternehmen mit mehreren tausend Mitarbeitenden verfügt über besonders klassifizierte Räumlichkeiten bis hin zu Hochsicherheitsbereichen, die nur wenigen Mitarbeitenden zugänglich sein sollten. Mit dem bisherigen Badge-System (RFID-Karte mit aufgedruckter Gesichtsfotografie) war eine zuverlässige Zutrittskontrolle sehr aufwendig. Das Unternehmen hat daher eine Lösung erarbeitet, die mit möglichst geringem Aufwand eine zuverlässige Verifizierung der Zutrittsberechtigten ermöglicht. Die Wahl fiel auf ein biometrisches Erkennungssystem, da ein solches eine automatisierte und höchst zuverlässige Verifizierung erlaubt.

Für die Zutrittskontrolle wird das Fingerabdrucktemplate nach dem Einlesen verschlüsselt und anschliessend zweigeteilt. Ein Teil wird zentral gespeichert, der zweite Teil dezentral auf dem Badge (wiederum einer RFID-Karte) abgelegt. Einzeln sind die Teile unbrauchbar, d.h. die zentral gespeicherten Daten können nicht ohne den Badge des Mitarbeiters verwendet werden. Das System ist schneller als ein vollkommen dezentrales System, da nur ein Bruchteil der Datenmenge (nur das Teiltemplate) über die drahtlose Schnittstelle ausgetauscht werden muss. Als Nebeneffekt ist es zudem unmöglich, brauchbare biometrische Daten aus der RFID-Karte auszulesen. Damit erfüllt das biometrische Zutrittssystem die datenschutzrechtlichen Anforderungen vollumfänglich.

Nebst der Zutrittskontrolle kann der neue Badge auch für das Computer-Login verwendet werden, und zwar nach dem Prinzip des Single-Sign-On (SSO). Für sämtliche passwortgeschützten IT-Anwendungen ist also nur noch ein einziges Login notwendig. Für das SSO wird das als Ganzes verschlüsselte Fingerabdruck-Template auf demselben Badge gespeichert, der auch für die Zutrittskontrolle verwendet wird; es werden aber keine biometrischen Daten zentral gespeichert. Bei jedem Arbeitsterminal kann der Badge ins Lesegerät eingelegt und das Login durchgeführt werden, ohne dass dabei biometrische Daten drahtlos übertragen werden. Damit erfüllt auch das SSO die datenschutzrechtlichen Anforderungen.

Mit dieser Systemarchitektur kann das Unternehmen die Vorteile eines biometrischen Erkennungssystems so nutzen, dass die Persönlichkeitsrechte der Mitarbeiter, insbesondere das Recht auf informationelle Selbstbestimmung, gewahrt bleiben.

Unser Leitfaden zum Thema befindet sich unter www.derbeauftragte.ch, Dokumentation – Datenschutz – Leitfäden – Leitfaden zu biometrischen Erkennungssystemen.

1.7.3 Zustellung von Pensionskassenausweisen

Das Eidgenössische Departement des Innern (EDI) zögert, die gesetzeswidrige Praxis der offenen Zustellung von Pensionskassenausweisen über den Arbeitgeber zu unterbinden.

In unserem 17. Tätigkeitsbericht 2009/2010, Ziff. 1.7.8, hatten wir bereits über die Praxis von einigen Vorsorgeeinrichtungen berichtet, Pensionskassenausweise offen über den Arbeitgeber zuzustellen. Da wir selber keine Verfügungsgewalt besitzen, haben wir beim zuständigen EDI im August 2009 beantragt, diese unseres Erachtens gesetzeswidrige Praxis zu unterbinden.

Seither ist leider nicht viel passiert: Auf eine erste Verfahrensstandsanfrage im Februar 2010 wurde uns immerhin Gelegenheit geboten, uns zu einer vom Bundesamt für Sozialversicherungen (BSV, der Aufsichtsbehörde der Vorsorgeeinrichtungen) zusammen mit der konkret betroffenen Pensionskasse verfassten Stellungnahme vernehmen zu lassen. Diese Gelegenheit nahmen wir wahr und stellten unsere Eingabe dem BSV zu. Seit Juni 2010 ist der Schriftenwechsel abgeschlossen. Der Entscheid des EDI war bei Redaktionsschluss dieses Tätigkeitsberichts immer noch ausstehend.

Nachdem aus unserer Sicht die Rechtslage klar ist und zahlreiche von der beanstandeten Zustellpraxis betroffene Personen bis heute regelmässig eine Verletzung ihrer Persönlichkeitsrechte hinnehmen müssen, solange die Sache nicht verbindlich entschieden ist, können wir das zögerliche Vorgehen des EDI schwerlich nachvollziehen.

1.7.4 Kontrollen im Rahmen paritätischer Berufskommissionen

Die Lohnbuchkontrollen paritätischer Berufskommissionen, wie sie in Gesamtarbeitsverträgen (GAV) vorgesehen sind, haben entsprechend reglementarisch festgelegtem Ablauf zu erfolgen. Arbeitgeber sind rechtzeitig und transparent über Umfang und Ablauf der Kontrolle sowie ihre Pflichten ins Bild zu setzen.

In den letzten Jahren haben wir uns wiederholt mit dem Problemkreis der Lohnbuchkontrollen im Bereich der GAV befasst. Die Lohnbuchkontrolle durch paritätische Berufskommissionen dient dazu, die Einhaltung von Lohnschutzbestimmungen durch die

Vertragsparteien zu überwachen. Dabei soll stets der Persönlichkeitsschutz der Arbeitnehmer gewährleistet bleiben. Er überwiegt die Interessen einer einzelnen Firma an der Geheimhaltung der Lohnbewirtschaftungsdaten. Weil also das Interesse an der fraglichen Datenbekanntgabe höher zu werten ist, haben wir unmissverständlich dargelegt, dass ein Bedürfnis zur Einholung einer expliziten Einwilligung der Arbeitnehmer und deren Verankerung im GAV entfalle. Diese Aussagen, mit welchen die Abwicklung der Kontrollen erleichtert werden soll, haben wir aber stets in der Annahme gemacht, dass die von den paritätischen Berufskommissionen durchgeführten Kontrollen verhältnismässig und wenn immer möglich innert nützlicher Frist vor Ort durchgeführt würden.

Es hat sich nun aber gezeigt, dass unsere Annahme durch die Realität der Automatisierung und Digitalisierung auch der Lohnbuchhaltungen überholt wurde. Solche Kontrollen erfolgen heute wohl nur noch in seltenen Fällen vor Ort und unter Einsichtnahme in die entsprechenden Ordner durch Mitglieder von paritätischen Berufskommissionen oder durch von diesen bestimmte Dritte zwecks Vermeidung der Kontrolle von direkten Mitkonkurrenten. Heute werden Lohnbuchkontrollen grossmehrheitlich von professionellen Kontrollern oder spezialisierten Treuhändern durchgeführt. Diese lassen sich die nötigen Unterlagen zur Lohnbuchkontrolle auf elektronischem Weg geben. Mittels Kontrollprogrammen erfolgt die Überprüfung sämtlicher Daten viel minutiöser, und eine gezielte Auswertung kann zu Resultaten führen, die früher aus rein zeitlichen Gründen ausser Reichweite lagen. An konkreten Fällen hat sich jedoch gezeigt, dass elektronische Lohnbuchkontrollen durch professionelle Kontroller ausserhalb der Geschäftsräume eines Unternehmens vor allem bei Arbeitgebern ungute Gefühle bezüglich Datenschutz und Datensicherheit aufkommen lassen. Damit verbunden besteht die latente Angst, diese neue Art der Kontrollen könnte zu viele Betriebsdaten offen legen.

Wir sehen deshalb Handlungsbedarf dahingehend, dass die von den paritätischen Berufskommissionen angeordneten Lohnbuchkontrollen transparent in einem Reglement festgelegt werden müssen. Arbeitgeber sind rechtzeitig über Umfang, Ablauf sowie ihre Pflichten zu orientieren. Wo die einverlangte Datenmenge ungeahnte Auswertungsmöglichkeiten zulässt, werden zwecks Einhaltung der Datensicherheit und des Datenschutzes allenfalls weitere gesetzliche Grundlagen und Schranken notwendig. In den GAV sind zwar bereits heute entsprechende Kontrollreglemente erwähnt. Wie sich uns gezeigt hat, bestehen diese jedoch nur in rudimentärer Form. Zumindest eine paritätische Berufskommission hat uns nun versichert, dass sie eine Arbeitsgruppe eingesetzt hat, welche die Ausarbeitung eines entsprechenden Kontrollreglements an die Hand nehmen werde.

1.7.5 Elektronisches Personaldossier in der Bundesverwaltung

Innerhalb der Bundesverwaltung besteht der Wunsch nach elektronischen Personaldossiers. Da bisher keine gesetzlichen Grundlagen dafür bestehen, mussten wir in zwei Fällen intervenieren.

Bundesorgane benötigen für das Bearbeiten von besonders schützenswerten Personendaten und Persönlichkeitsprofilen eine gesetzliche Grundlage, und zwar in Form eines Bundesgesetzes. Ein Personaldossier stellt in sich ein Persönlichkeitsprofil dar und enthält auch besonders schützenswerte Personendaten. Die geltenden Bestimmungen bilden keine ausreichende gesetzliche Grundlage für das Führen von elektronischen Personaldossiers in der Bundesverwaltung. Bei zwei Projekten mussten wir deshalb intervenieren. Einerseits handelte es sich um ein System für elektronische Personaldossiers innerhalb des VBS, anderseits um einen online-Bewerbungsdienst des EPA, der zu elektronischen Bewerbungsdossiers geführt hätte. Auch dafür besteht jedoch zurzeit keine ausreichende gesetzliche Grundlage im Bund. Aufgrund unserer Intervention wurden beide Projekte gestoppt respektive deren Einführung verschoben, bis das revidierte Bundespersonalgesetz in Kraft tritt (voraussichtlich am 1. Januar 2012).

1.7.6 Bearbeitung von Personaldossiers in GEVER-Systemen

Die Bearbeitung von Personaldossiers in GEVER-Systemen bedarf aufgrund datenschutzrechtlicher Anforderungen einer gesetzlichen Grundlage im Bundespersonalgesetz. Mit der Revision der entsprechenden Artikel wird eine solche Grundlage geschaffen.

Im Rahmen einer Anfrage der Bundeskanzlei haben wir die momentane Rechtslage für die Bearbeitung von Personaldossiers in GEVER-Sytemen aus datenschutzrechtlicher Sicht beurteilt und Stellung genommen.

Das Datenschutzgesetz (DSG) bestimmt, dass Bundesorgane besonders schützenswerte Personendaten und Persönlichkeitsprofile nur bearbeiten dürfen, wenn eine gesetzliche Grundlage im formellen Sinn es ausdrücklich vorsieht. Die Grundlage für die Geschäftsverwaltungssysteme der Bundesbehörden befindet sich in Artikel 57h des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG), nach welchem jedes Bundesorgan ein Informations- und Dokumentationssystem mit besonders schützenswerten Daten und Persönlichkeitsprofilen führen kann, «soweit sich diese aus dem Schriftverkehr oder aus der Art des Geschäftes ergeben».

Da sich die Bearbeitung von Personaldossiers nicht «aus der Art des Geschäfts» ergibt, schafft Artikel 57h in diesem Fall keine gesetzliche Grundlage. Vielmehr regelt das Bundespersonalgesetz (BPG) in Ergänzung zum DSG die Bearbeitung von Personaldossiers durch die Arbeitgeber beim Bund.

Die geltende Regelung in Artikel 27 BPG reicht allerdings nicht zur Führung von elektronischen Personaldossiers. Der Bundesrat hat dies erkannt und mit dem Beschluss vom 1. September 2010 zum Konsolidierungsprogramm 12/13 die Revision von Artikel 27 a-c BPG verabschiedet. Darin sollen die gesetzlichen Grundlagen für die Führung von elektronischen Dossiers von Stellenbewerberinnen und -bewerbern sowie von Angestellten geschaffen werden. So wird dem immer stärker werdenden Bedürfnis nach automatisierten Bearbeitungssystemen Rechnung getragen. Ein solches System muss zudem geschlossen, also nicht mit anderen elektronischen Datenbearbeitungssystemen verbunden sein, wenn im Rahmen von Personaldossiers Gesundheitsdaten bearbeitet werden. Dies schreibt die Verordnung über den Schutz von Personaldaten in der Bundesverwaltung vor.

1.7.7 Kontrolle des Personalinformationssystems des Bundes: Stand der Dinge

Das Bearbeitungsreglement des Personalinformationssystems des Bundes (BV PLUS) entspricht noch nicht den Vorgaben und soll deshalb angepasst werden. Gewisse Aspekte müssen noch verbessert oder dokumentiert werden; insbesondere der Up- und Download von Daten, die Protokollierung sowie die Kontrollverfahren.

Grundsätzlich mussten wir bei der Kontrolle des BV PLUS feststellen, dass die Dokumentation im Bereich Datenschutz- und Datensicherheit nicht sehr umfangreich war. So wurde bspw. das Bearbeitungsreglement vor Jahren einmal erstellt, dann aber kaum noch nachgeführt. Wir machten deshalb die Verantwortlichen auf unsere Erläuterungen zur Erstellung eines solchen Reglements aufmerksam (siehe www.derbeauftragte.ch unter Dokumentation – Datenschutz – Leitfäden – Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes).

Im Weiteren konnten wir auch feststellen, dass zu Beginn der Kontrolle ein Daten- oder Informationssicherheitssachverständiger im SAP-Bereich fehlte, auf welchem das BV PLUS betrieben wird. Eine sachkundige Person ist u. E. unerlässlich beim Einsatz eines solch sensitiven Systems in der gesamten Bundesverwaltung. Dieser Sachverständige müsste Ansprechperson sowohl für die Leistungserbringer (bspw. Rechenzentren) als auch für die Leistungsbezüger (bspw. HR-Abteilungen) sein und sollte seine Aufgaben möglichst unabhängig wahrnehmen können.

Die Benutzer authentifizierten sich alle, ausser die einer grösseren Organisationseinheit, mit Hilfe von Smartcards der Klasse B. Wir haben darauf aufmerksam gemacht, dass aufgrund der Sensitivität des Systems die Smartcardlösung flächendeckend eingesetzt werden sollte. Dies wurde in der Folge auch umgesetzt.

SAP bzw. BV PLUS erlaubt es, Daten auf den Computer am Arbeitsplatz herunter- oder von diesem auf das SAP-System hochzuladen. Durch das Herunterladen von Daten können die Zugriffsrestriktionen des zentralen SAP-Systems aufgehoben werden. Wir haben im Bearbeitungsreglement keine abschliessenden Angaben zu diesen Up- und Downloads gefunden. Aus Sicht des Datenschutzes muss festgestellt werden können, wer warum (zu welchem Zweck) befugt ist, solche Operationen durchzuführen. Es ist auch aufzuzeigen, welche Daten dafür benötigt und wie sie auf den Computern bearbeitet werden. Erfolgt dies in allen Organisationseinheiten gleich, genügt eine einmalige Umschreibung. Alle bundesweiten Abweichungen sind entsprechend zu dokumentieren. Während unserer Kontrolle wurde uns mitgeteilt, dass es keine sinnvollen technischen Möglichkeiten für die Protokollierung der Up- und Downloads gebe. Im Prüfleitfaden Datenschutz SAP ERP 6.0 der DSAG Arbeitsgruppe Datenschutz ist eine solche Protokollierung mit Hilfe des Security Audit Logs jedoch aufgeführt.

Weiter teilte man uns mit, dass es keine sinnvollen technischen Möglichkeiten gebe, sensitive Query/BW-Abfragen zu protokollieren. Im oben aufgeführten Leitfaden (Punkt 4.2.1.9.6) wird jedoch auch aufgezeigt, dass Ad-hoc-Query-Protokollierungen möglich sind. Aufgrund der uns zur Verfügung gestellten Unterlagen und dieser Mangelpunkte mussten wir davon ausgehen, dass u. a. auch bei der Protokollierung Handlungsbedarf besteht. Wir haben deshalb die Verantwortlichen gebeten, ein Protokollierungskonzept zu erstellen, welches die notwendigen Anforderungen des Datenschutzes abdeckt. Dabei ist neben der Sicht des Leistungserbringers insbesondere auch diejenige der Leistungsbezüger einzubringen.

Als Kontrollverfahren im laufenden Betrieb wurde die stichprobenweise Auswertung von Protokollen auf der Systemebene durch den Leistungserbringer festgehalten. Kontrollen müssen aber im laufenden Betrieb auch vom Inhaber der Datensammlung durchgeführt werden. Die entsprechenden Kontrollverfahren sind zu dokumentieren.

Die Verantwortlichen haben uns mitgeteilt, dass die Umsetzung der noch offenen Punkte bis Ende 2011 dauern wird.

1.8 Handel und Wirtschaft

1.8.1 Datenschutz beim Einsatz von Smart Meter

Mit dem neuen Stromversorgungsgesetz wird der Elektrizitätsmarkt seit 1. Januar 2008 schrittweise liberalisiert. Dies erfordert eine neue Verbrauchserfassung. Mittels digitalen Zählern können sehr viele Daten gespeichert und online übermittelt werden, was einerseits den Stromkunden Energiesparmöglichkeiten aufzeigt, andererseits aber auch Risiken für die Privatsphäre birgt.

Vor dem Start eines Pilotprojektes mit 480 digitalen Zählern, so genannten Smart Meter, wurden wir von einem Energielieferanten kontaktiert, um die datenschutzrechtliche Ausgestaltung des Projektes zu beurteilen. Wir sind dabei zum Schluss gekommen, dass es eine umfassende Information der betroffenen Haushalte braucht, wenn im Rahmen des Pilotprojektes der komplette Lastgang (der Stromverbrauch über eine bestimmte Zeitspanne) aufgezeichnet, an den Energielieferanten übermittelt und von diesem gespeichert sowie ausgewertet werden soll. Die Betroffenen dürfen verlangen, dass wie bis anhin nur ihr gesamter Stromverbrauch zu Hoch- und Niedertarifzeiten aufgezeichnet wird, da die Aufzeichnung des Lastgangs im 15-Minuten-Takt für die Rechnungsstellung nicht notwendig ist.

Unabhängig von diesem Pilotprojekt haben wir die Datenschutzrisiken beim Einsatz von Smart Meter im Hinblick auf die kommende zweite Etappe der Strommarktöffnung evaluiert. Die intelligenten Energiezähler ermöglichen, je nach Konfiguration, die mehr oder weniger detaillierte Aufzeichnung von Lastprofilen (d.h. der Verlauf des Stromverbrauchs pro Erfassungsintervall) eines Haushaltes sowie die Fernauslesung. Bei einem Intervall von 15 Minuten ergibt das rund 35'000 Messpunkte pro Jahr. Ein solches Energienutzungsprofil enthält für die Stromkunden wichtige Informationen über den Energieverbrauch und entsprechende Einsparungsmöglichkeiten. Es gibt jedoch auch Auskunft über Geschäftstätigkeiten, Produktionsprozesse, persönliche Aktivitäten, Tagesablauf, Krankheiten etc. Das Energienutzungsprofil stellt demnach ein Persönlichkeitsprofil dar, das nicht generell ausgelesen werden darf. Für die Netzplanung und die Rechnungsstellung ist eine automatische Weitergabe solch detaillierter Informationen aus unserer Sicht denn auch nicht zwingend notwendig.

Die Erläuterungen dazu befinden sich im Anhang Ziff. 4.1.1 und können auf unserer Webseite www.derbeauftragte.ch unter Themen – Datenschutz – Sonstige Themen abgerufen werden.

1.8.2 Datenübermittlung ins Ausland im Rahmen eines «Outsourcing»

In Zeiten der Globalisierung gewinnt die Datenübermittlung ins Ausland im Rahmen eines «Outsourcing» – gerade bei internationalen Konzernen – zunehmend an Bedeutung. Aus Gründen der Arbeitsteilung wird heutzutage zudem oftmals für die Bearbeitung der Daten ein Unterauftragnehmer beigezogen. Es stellt sich daher die Frage, unter welchen datenschutzrechtlichen Voraussetzungen die Datenübertragung und damit auch die Übermittlung an einen Auftragnehmer und Unterauftragnehmer im Ausland zulässig sind.

Das Datenschutzgesetz sieht vor, dass die Bearbeitung von Personendaten durch Vereinbarung einem Dritten, d.h. einem Auftragnehmer, übertragen werden kann. Gemäss Gesetz darf dieser die Daten aber nur so bearbeiten, wie der Auftraggeber selbst es tun dürfte. Aus dieser Verpflichtung lässt sich ableiten, dass ein Auftragnehmer, falls er für die Datenbearbeitung einen Unterauftragnehmer beiziehen will, mit diesem eine Vereinbarung abschliessen muss, und dass auch der Unterauftragnehmer die Daten nur so bearbeiten darf, wie es Auftraggeber bzw. Auftragnehmer selbst tun dürften. Diese gesetzlichen Anforderungen gelten unabhängig davon, ob die Datenbearbeitung durch einen (Unter-) Auftragnehmer im In- oder im Ausland erfolgt. Wenn er sich im Ausland befindet, gelten zusätzlich die Vorgaben von Art. 6 DSG.

Wir haben zum Thema Datenübermittlung ins Ausland im Rahmen eines «Outsourcing» auf unserer Webseite Unterlagen aufgeschaltet. Darin sind die wichtigsten «Outsourcing»-Konstellationen und die entsprechenden datenschutzrechtlichen Vorgaben dargestellt (siehe www.derbeauftragte.ch, Themen – Übermittlung ins Ausland – Outsourcing).

Des Weiteren haben wir den Mustervertrag für das Outsorucing von Datenbearbeitungen ins Ausland («Swiss Transborder Data Flow Agreement») überarbeitet und mit zusätzlichen Bestimmungen bezüglich der Datenbearbeitung durch einen Unterauftragnehmer ergänzt. Demnach ist eine solche Übertragung der Datenbearbeitung nur mit vorgängiger schriftlicher Zustimmung des Auftraggebers zulässig. Überdies wird der Auftragnehmer verpflichtet, mit dem Unterauftragnehmer einen schriftlichen Vertrag zu schliessen, worin sich dieser verpflichtet, dieselben Datenschutzstandards einzuhalten, wie sein (direkter) Auftraggeber. Der Vertrag kann auf Englisch auf unserer Webseite (www.derbeauftragte.ch, Themen – Übermittlung ins Ausland – Outsourcing) abgerufen werden.

Schliesslich sei erwähnt, dass sich auch die EU-Kommission mit dieser Thematik beschäftigt hat. Sie hat ihre bisherigen EU-Standardvertragsklauseln «Data Controller to Data Processor» revidiert und per 15. Mai 2010 neue Klauseln in Kraft gesetzt.

1.8.3 Verwendung von gesperrten Kundendaten zu Werbezwecken

Wir sind durch eine Bürgeranfrage darauf aufmerksam gemacht worden, dass eine Schweizer Bank zusammen mit den periodischen Kontoauszügen Informationsmaterial auch dann verschickt, wenn der betreffende Kunde die Verwendung seiner Adresse zu Werbezwecken ausdrücklich untersagt hat. Wir haben daraufhin die technischen und organisatorischen Massnahmen der Bank zur Durchsetzung von Adresssperren überprüft. Wie wir feststellen konnten, versendet die Bank bei bestehender Adresssperre keine Werbung, sondern einzig das aufgrund der bankrechtlichen Sorgfaltspflicht notwendige Informationsmaterial. Der Versand ist damit gerechtfertigt.

Eine Kundenadresse darf so lange zu Werbezwecken verwendet werden, als die Kundin sie nicht gesperrt hat. Eine Unternehmung hat technisch und organisatorisch sicherzustellen, dass eine solche Sperre auch entsprechend respektiert wird. Von Werbematerial zu unterscheiden sind aber Informationsschreiben, welche für Bankkunden wichtige Informationen enthalten, bspw. zu Änderungen von Vertragsbedingungen oder Hintergrundinformationen zu von der Kundin gehaltenen Anlagen. Die Bank hat hier einen Rechtfertigungsgrund, Kundendaten auch gegen den Willen der Betroffenen zu verwenden. Dies jedoch nur so weit, als es zur Erfüllung der Sorgfaltspflicht notwendig ist.

Wie wir feststellen konnten, macht die fragliche Bank eine klare Unterscheidung zwischen reinen Werbesendungen und den Informationsschreiben, zu denen sie gesetzlich verpflichtet ist. Für erstere gewährt sie die Möglichkeit eines Opt-outs: Wünscht eine Kundin oder ein Kunde, vom Versand von Werbematerial ausgeschlossen zu werden, so kann sie oder er dies der Bank mitteilen. Diese kann in ihrer Kundendatenbank allgemein oder themenspezifisch Werbung für jeden einzelnen Kunden unterdrücken oder auf Wunsch auch zusätzlich aufschalten. Die Kunden erhalten so Werbesendungen nur im gewünschten Umfang. Sendungen im Rahmen der Informationspflicht können dagegen nicht abbestellt werden.

Damit kommt die Bank ihren datenschutzrechtlichen Verpflichtungen im Umgang mit Kundendaten zu Werbezwecken nach, so dass wir diesbezüglich keine Beanstandungen haben.

1.8.4 Bearbeitung von Personendaten im Adresshandel

Auf den Adresshandel spezialisierte Firmen beschaffen verschiedene Verbraucherdaten, um sie an Dritte zu verkaufen. Eine solche Datenbearbeitung ist zulässig, soweit sie die Vorschriften der Datenschutzgesetzgebung, namentlich die Grundsätze der Zweckbindung und der Transparenz, einhält. Die betroffenen Personen müssen sich gegen die Verwendung ihrer persönlichen Informationen zu kommerziellen Zwecken wehren und Auskunft über alle sie betreffenden Daten erhalten können.

Handelsgesellschaften, Verbände, Zeitungen oder Zeitschriften bemühen sich, neue Kunden, neue Geldgeber oder neue Abonnenten zu gewinnen. Sie versuchen auch, mehr über ihre tatsächliche oder potentielle Kundschaft zu erfahren, um sie an sich zu binden oder mehr Gewinn aus den Kunden mit dem grössten Potential herauszuschlagen. Zu diesem Zweck ist es nützlich – beispielsweise für eine Versandhandelsfirma –, über möglichst viele solcher Daten zu verfügen. Je besser nämlich ein Unternehmen seine Kundschaft kennt, umso eher wird es in der Lage sein, Produkte oder Dienstleistungen anzubieten, die den Bedürfnissen dieser Kunden entsprechen und auf ihr Interesse stossen könnten, und umso besser wird es ihre Produkte oder Leistungen verkaufen können.

Manche Firmen haben sich auf die Bearbeitung von Adressen und Kundenregister spezialisiert und beschaffen dazu eine Vielzahl von Verbraucherinformationen. Sie stellen interessierten Personen oder Firmen diese Dateien zur Verfügung, indem sie ihnen die Adressen einer Zielgruppe verkaufen oder vermieten (Adresshandel) oder die Kundendateien der Person/Firma mit zusätzlichen Informationen anreichern (Datenanreicherung).

Abgesehen von den Adressen, die den Telefonbüchern entnommen oder von Dritten geliefert werden, verfügen die auf Adresshandel spezialisierten Firmen über zahlreiche weitere Informationen zu Privatpersonen oder Gesellschaften, beschafft aus den verschiedensten Quellen (Wettbewerbe, Fragebogen zu den Konsumgewohnheiten usw.) oder geliefert von Partnerfirmen. Sie verknüpfen sie mit wieder anderen Daten – bspw. Baukosten für das Grundstück an einer bestimmten Adresse oder auch statistische Daten –, bevor sie ihre gebündelten Dateien ihren Kunden zur Verfügung stellen.

Ausgehend von verschiedenen Kriterien (wie Geschlecht, Alter, Region oder Beruf) oder auch von Angaben über die Konsumgewohnheiten (wie etwa die Kaufkraft, die Tendenz, im Versandhandel einzukaufen oder die Freizeitbeschäftigungen) kann so bspw. eine Versandhandelsfirma, die Luxusbekleidung für Säuglinge anbietet, die Adressen und Telefonnummern ihres Zielpublikums kaufen, in diesem Fall Frauen zwischen 30

und 40 Jahren, die in einer bestimmten Region leben, Kleinkinder haben, über ein hohes Einkommen verfügen und gerne im Versandhandel einkaufen. Diese Versandhandelsfirma kann die Profile ihrer Kundschaft auch ergänzen, indem sie die ihr bereits vorliegenden durch neue Angaben vervollständigt, wie etwa das Geburtsdatum, die Zahl der Kinder oder die Telefonnummer, um auf die Interessen ihrer Kunden zugeschnittene Angebote zu machen und die Vermarktungskanäle zu diversifizieren.

Selbstverständlich fällt die Beschaffung von Daten über bestimmte Personen oder die Erstellung von Personenprofilen in den Geltungsbereich des Bundesgesetzes über den Datenschutz. Dieses untersagt die Verfügbarmachung solcher Personenregister nicht, stellt aber eine Anzahl verbindlicher Regeln auf.

Wir sind dabei zu prüfen, ob in der Praxis die im Bereich des Adresshandels vorgenommenen Datenbearbeitungen wirklich den Bestimmungen des DSG entsprechen, insbesondere dem Grundsatz der Zweckbindung und der Erkennbarkeit (namentlich bezüglich der Herkunft der beschafften Daten). Ebenso untersuchen wir, ob die Personen, die ihr Auskunftsrecht bei Firmen aus dieser Sparte wahrnehmen, sämtliche in den Registern enthaltenen Informationen bekommen, und ob ihr Einspruchsrecht angemessen respektiert wird.

1.8.5 Altersnachweis bei Zigarettenautomaten

Ein Kartenlesesystem für Zigarettenautomaten zur Altersüberprüfung löst an ausgewählten Standorten in der Schweiz das bisherige mit den Jetons ab. Aus datenschutzrechtlicher Sicht ist das System in der uns präsentierten Form unproblematisch.

Die British American Tobacco präsentierte uns ihr neues Kartenlesesystem für Zigarettenautomaten. Es wird an ausgewählten Standorten eingesetzt und soll das bisherige Token-System (Jetons) ablösen, bei dem die Alterskontrolle entweder durch den Wirt oder das Personal des Lokals, in dem der Zigarettenautomat stand, erfolgte. Das neue System hingegen ist fähig, die Identitätskarte oder den Führerausweis zu lesen. Für die Altersüberprüfung werden Geburtsdatum, Dokumententyp und Echtheit erfasst und ausgewertet. Der Kartenleser erkennt, ob der (potentielle) Käufer das gesetzliche Mindestalter erreicht hat und schaltet in diesem Fall den Automaten für den Zigarettenkauf frei.

Das Kartenlesesystem kann nicht vor Missbrauch schützen, z.B. indem ein fremder Ausweis verwendet wird. Aus datenschutzrechtlicher Sicht ist das System in der uns präsentierten Funktionsweise jedoch unproblematisch, da alle temporär gespeicherten Daten unwiderruflich gelöscht werden und keine personenbezogene Auswertung von Daten erfolgt.

1.8.6 Datenbeschaffung für Prepaid-Karten

Informationen über das Einkommen sind nur für Kreditkarten erforderlich. Diese Daten für eine Prepaid-Karte zu verlangen, ist unverhältnismässig und entspricht nicht dem Bundesgesetz über den Datenschutz. Auf unser Ansuchen hin hat ein Kartenanbieter seine Formulare entsprechend angepasst.

Aufgrund von Informationen einer betroffenen Person haben wir das Antragsformular für ein Halbtax-Abonnement in Kombination mit einer Kreditkarte oder einer Prepaid-Karte geprüft. Der Antragsteller musste hierbei auf dem Formular diverse persönliche und berufliche Informationen erteilen. Es wurde insbesondere klar erwähnt, dass alle diese Daten – namentlich über die Herkunft und die Höhe seiner Einkünfte – zwingend angegeben werden müssten und dass bei Fehlen dieser Informationen das Gesuch nicht bearbeitet würde.

Gemäss dem Konsumkreditkreditgesetz hat die kreditgebende Person (beziehungsweise der Kreditkartenanbieter) zu prüfen, ob der Konsument tatsächlich kreditfähig ist. Die Überprüfung der Einkommensquellen hat zum Ziel, eine mögliche Überschuldung infolge eines solchen Vertrags zu vermeiden. Diese gesetzliche Verpflichtung gilt jedoch nur für Konsumkreditverträge. Im Falle einer Prepaid-Karte ist die Erhebung von Informationen über das Einkommen nicht notwendig, da der Betrag im Voraus auf die Karte einbezahlt wird und der Karteninhaber somit ohne Risiko einer Überschuldung darüber verfügen kann. Es entspricht daher nicht den Grundsätzen der Zweckbindung und der Verhältnismässigkeit, solche Informationen zu verlangen, ja es steht in Ermangelung eines Rechtfertigungsgrundes sogar im Widerspruch zum Bundesgesetz über den Datenschutz.

Auf unser Ansuchen hin hat der Kartenanbieter sich bereit erklärt, seine Formulare entsprechend anzupassen und darauf hinzuweisen, dass die Angaben über die Einkünfte nur für einen Kreditkartenantrag erforderlich sind.

1.9 Finanzen

1.9.1 Uneinheitliche Handhabung von Betreibungsregisterauszügen

Die Praxis der kantonalen Betreibungsämter in Bezug auf die Bekanntgabe von Betreibungsregisterauszügen ist uneinheitlich. Gewisse Ämter geben nur Daten der vergangenen zwei Jahre bekannt, andere wiederum der letzten fünf Jahre. Und einige informieren über Betreibungsdaten, die sie von Gesetzes wegen nicht mehr offen legen dürften.

Im Rahmen von Abklärungen über die Bearbeitung von Bonitäts- und Wirtschaftsdaten durch Kredit- und Wirtschaftsauskunfteien haben wir ein externes Gutachten erstellen lassen, welches die Verhältnismässigkeit solcher Bearbeitungen untersuchte (vgl. unseren 17. Tätigkeitsbericht 2009/2010, Ziff. 1.9.5.). Der Gutachter stellte darin fest, dass die kantonalen Betreibungsämter die Bekanntgabe von Betreibungsregisterauszügen im Sinne von Artikel 8a Schuldbetreibungs- und Konkursgesetz (SchKG) in zeitlicher und sachlicher Hinsicht unterschiedlich handhaben. Gewisse Ämter geben nur Daten der letzten zwei Jahre bekannt, andere wiederum der vergangenen fünf Jahre. Überdies informieren gewisse Betreibungsämter über Betreibungsdaten, die sie offensichtlich gemäss SchKG nicht (mehr) mitteilen dürften. Aufgrund ihrer wirtschaftlichen Bedeutung sind solche Daten als heikel einzustufen. Für betroffene Personen können diese Praktiken im Einzelfall kreditschädigende Folgen nach sich ziehen, weil ihnen Kreditverträge möglicherweise zu Unrecht verweigert oder nur zu schlechten Konditionen gewährt werden.

Da das Datenschutzgesetz für öffentliche Register des Privatrechtsverkehrs, zu denen auch das Betreibungsregister zählt, nicht anwendbar ist, sind wir mit dem Bundesamt für Justiz (BJ), welches die Oberaufsicht über die Betreibungsämter ausübt, in Kontakt getreten. Wir haben dem Amt die Ausgangslage und Probleme, die rund um diese uneinheitlichen Praktiken entstehen können, dargelegt. Dem BJ ist die uneinheitliche Handhabung der Betreibungsregisterauszüge bekannt.

1.9.2 Bearbeitung von Bonitäts- und Wirtschaftsdaten durch Auskunfteien

Bei der Bearbeitung von Bonitätsdaten durch Kredit- und Wirtschaftsauskunfteien stehen zwei Themenbereiche im Vordergrund. Zum Einen geht es um die Korrektur und Löschung falscher Daten, ein Unterfangen, das sich in der Praxis als sehr schwierig und zeitraubend erweist. Zum Anderen werden dank der heutigen technischen Möglichkeiten immer mehr Personendaten gesammelt und miteinander verknüpft, so dass daraus Persönlichkeitsprofile entstehen können.

Die Bearbeitung von Bonitäts- und Wirtschaftsdaten durch Kredit- und Wirtschaftsauskunfteien ist nach wie vor eines jener Themen, zu denen wir viele Bürgeranfragen erhalten. In den meisten Fällen geht es um die Löschung und Korrektur falscher Daten, um den zulässigen Inhalt und Umfang der bearbeiteten Daten sowie um das Auskunftsrecht.

Wir müssen feststellen, dass bei der Bearbeitung von Bonitätsdaten nach wie vor Fehler passieren. Sei es, dass Personen verwechselt werden oder aufgrund von falschen Daten einen negativen Scorewert erhalten, ihre Kreditwürdigkeit also als schlecht eingestuft wird. Dies kann für betroffene Personen im Einzelfall einschneidende, wenn nicht sogar kreditschädigende Folgen haben. Die Korrektur bzw. Löschung falscher Daten erweist sich in der Praxis als schwieriges und zeitraubendes Unterfangen, das mit viel Aufwand verbunden ist, da die Daten sehr oft in mehreren Datensammlungen bei verschiedenen Auskunfteien korrigiert werden müssen und eine betroffene Person manchmal gar nicht weiss, wo überall falsche Daten über sie gespeichert sind.

Des Weiteren beobachten wir die Tendenz, dass Kredit- und Wirtschaftsauskunfteien – dank der heutigen technischen Möglichkeiten – immer umfangreichere und detailliertere Datenbestände über Personen sammeln und sie dann miteinander verknüpfen. So werden heutzutage fast standardmässig Bonitätsdaten mit sozio-demografischen und geografischen Informationen angereichert, und es stellt sich die Frage, ob daraus nicht Persönlichkeitsprofile entstehen.

Angesichts dieser Entwicklung werden wir bei den Kredit- und Wirtschaftsauskunfteien im Rahmen unserer Aufsichtstätigkeit weitere Abklärungen vornehmen.

1.9.3 Doppelbesteuerungsabkommen

Das Datenschutzgesetz ist auch bei der grenzüberschreitenden Amtshilfe in Steuersachen zu beachten. Die neu abgeschlossenen internationalen Doppelbesteuerungsabkommen, die dem OECD-Standard angepasst wurden, schliessen den automatischen Informationsaustausch sowie «fishing expeditions» aus. Überdies wird keine Amtshilfe bei illegal beschafften Daten geleistet.

Seit dem Beschluss des Bundesrates vom 13. März 2009, die internationale Amtshilfe in Steuersachen auszubauen und den OECD-Standard (insbesondere den Informationsaustausch) zu übernehmen, wurden zahlreiche Doppelbesteuerungsabkommen (DBA) revidiert oder neu abgeschlossen. Da das Datenschutzgesetz auch bei der grenzüberschreitenden Amtshilfe zu beachten ist, erhalten wir im Rahmen von Ämterkonsultationen jeweils Gelegenheit, uns zu diesen Abkommen zu äussern.

Aus datenschutzrechtlicher Sicht interessieren jene DBA, die dem OECD-Standard angepasst wurden, in denen also die Regelung bezüglich des Informationsaustausches in Steuersachen (Art. 26 OECD-Musterabkommen) übernommen wurde. Diese Bestimmung legt unter anderem fest, dass Steuerinformationen nur ausgetauscht werden, wenn der ersuchende Staat in einem Amtshilfebegehren die betroffene steuerpflichtige Person und die Stelle/Person (z.B. Bank), in deren Besitz die gewünschten Daten vermutet werden, eindeutig identifiziert. Zudem muss der ersuchende Staat darlegen, welche Informationen er für welche Steuerperioden und zu welchen steuerlichen Zwecken benötigt. Daraus folgt, dass sich der Informationsaustausch auf konkrete Anfragen im Einzelfall beschränkt und so genannte «fishing expeditions», d.h. Ermittlungen, die ohne präzises Ermittlungsobjekt in der Hoffnung vorgenommen werden, steuerlich relevante Informationen zu erhalten, ausdrücklich ausgeschlossen sind. Schliesslich wird in den neu abgeschlossenen DBA ausdrücklich festgehalten, dass bei illegal beschafften Daten keine Amtshilfe geleistet wird.

Aufgrund dieser Sachlage sind wir der Meinung, dass der Informationsaustausch mit dem Ausland in Steuersachen in Übereinstimmung mit dem Datenschutzgesetz erfolgt.

1.10 International

1.10.1 Internationale Zusammenarbeit

Die internationale Dimension der Fragen im Zusammenhang mit dem Datenschutz nimmt stetig zu. Sie erfordert eine Intensivierung der Zusammenarbeit zwischen den Datenschutzbehörden in Europa und weltweit. Sie verstärkt auch den Willen, zu einer verbindlichen universellen Rechtsurkunde zu gelangen. Beteiligt haben wir uns aktiv an den Arbeiten des Europarates, der OECD, der europäischen und der internationalen Konferenz der Datenschutzbeauftragten, der gemeinsamen Kontrollinstanzen Schengen und Eurodac und der französischsprachigen Vereinigung der Datenschutzbehörden.

Europarat

Der Ministerausschuss des Europarates hat am 23. November 2010 die Empfehlung R (2010) 13 zum Schutz des Menschen bei der automatischen Verarbeitung von Personendaten im Rahmen der Profilierung verabschiedet (www.coe.int). Diese vom beratenden Ausschuss (T-PD) für das entsprechende Übereinkommen 108 vorbereitete Empfehlung ist die erste Rechtsurkunde, die Mindestnormen für den Datenschutz im Bereich von Persönlichkeitsprofilen von Privatpersonen enthält. Die Mitgliedstaaten des Europarates sind damit aufgefordert, die Grundsätze der Empfehlung über die innerstaatliche Gesetzgebung und durch Selbstregulierung umzusetzen. Das Erstellen von Persönlichkeitsprofilen besteht in der Beobachtung des Verhaltens von Einzelpersonen, der Beschaffung und der Verwertung ihrer Personendaten. Diese Technik wird in zahlreichen Tätigkeitsbereichen zunehmend angewendet, insbesondere im Zusammenhang mit der Informationsgesellschaft und dem Internet. Die Empfehlung R zielt nicht auf ein generelles Verbot der Erstellung von Persönlichkeitsprofilen ab, sondern soll einen kohärenten und ausgewogenen Regelungsrahmen für diese Praktiken und Techniken abstecken. Sie nennt die Voraussetzungen, die erfüllt sein müssen, um Verletzungen des Datenschutzes und der Privatsphäre zu verhindern, namentlich das Risiko einer Diskriminierung. Angesichts der Komplexität, ja sogar der Undurchsichtigkeit dieser Datenbearbeitungstechnik ist es wichtig, Transparenz zu gewährleisten, indem die Anforderungen an die Information der betroffenen Personen verstärkt und diesen zusätzliche Rechte gewährt werden. So können sie die vollständige Kontrolle über ihre Daten behalten und in Kenntnis der Sachlage handeln. Zudem ist es wichtig, die Pflicht zur Verwendung datenschutzkonformer Technologien gesetzlich zu verankern.

Der T-PD hat seinen Vorstand erneuert und den schweizerischen Vertreter in der Person des stellvertretenden eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

zu seinem Vorsitzenden gewählt. Ausserdem hat er seine Arbeiten zur Modernisierung der Rechtsurkunden des Europarates betreffend den Datenschutz und namentlich des Übereinkommens 108 und seines Zusatzprotokolls, der Empfehlung R (89) 2 über den Schutz persönlicher Daten, die für Beschäftigungszwecke verwendet werden, und der Empfehlung R (87) 15 über die Nutzung personenbezogener Daten im Polizeibereich aufgenommen. Diese Arbeiten sollten zu einer Änderung des Übereinkommens in Form einer Ergänzung oder eines Zusatzprotokolls führen. Durch die Bekräftigung des Rechts auf die Kontrolle über die Daten und des Rechts auf Menschenwürde und Nichtdiskriminierung bei der Bearbeitung von Personendaten soll die Stellung der betroffenen Personen gestärkt werden. Die Grundprinzipien des Datenschutzes sollten ergänzt oder präzisiert werden (namentlich durch die Grundsätze der Datensparsamkeit, der datenschutzkonformen Entwicklung schon bei der Planung der Systeme, Dienstleistungen oder Produkte – «privacy by design» – und der «verstärkten» Verantwortlichkeit). So könnte eine Informationspflicht bei Sicherheitspannen eingeführt werden. Darüber hinaus sollten die Rechte der betroffenen Personen gestärkt werden, namentlich durch die ausdrückliche Einführung des Auskunftsrechts, des Rechts auf Löschung oder des Rechts, nicht einer automatisierten (d.h. computer- bzw. softwarebasierten) Entscheidung unterworfen zu werden. Besonderes Augenmerk müsste auf die Geltendmachung der Rechte durch die betroffenen Personen gerichtet werden. Die allgemeine, einfache und technologisch neutrale Formulierung des Übereinkommens sollte beibehalten werden. Ebenso sollte die Zielsetzung berücksichtigt werden, Drittstaaten, die nicht Mitglied des Europarates sind, die Möglichkeit zum Beitritt zu dieser Urkunde einzuräumen. Diese Modernisierungsarbeit wurde vom Ministerkomitee am 10. März 2010 gutgeheissen und war Gegenstand einer Resolution über den Datenschutz und den Schutz der Privatsphäre im dritten Jahrtausend, die am 26. November 2010 auf der 30. Konferenz des Europarates der Justizminister angenommen wurde (www.coe.int). Wir haben den Entwurf zur Modernisierung des Übereinkommens bei einer Konferenz vorgelegt, die gemeinsam vom Europarat und der Europäischen Kommission am 28. Januar 2011 anlässlich des 30. Jahrestages des Übereinkommens 108 und des 5. Europäischen Tages des Datenschutzes organisiert worden war.

Schliesslich setzt sich der Europarat auch weiterhin für den Beitritt von Drittstaaten zum Übereinkommen 108 und seinem Zusatzprotokoll ein; ein erster Beitritt könnte im Jahr 2011 erfolgen.

Europäische Konferenz der Datenschutzbeauftragten

Die europäische Frühjahrskonferenz der Datenschutzbeauftragten fand vom 29. bis 30. April 2010 in Prag statt und wurde vom tschechischen Datenschutzamt ausgerichtet. Unter dem Motto «Penser le passé, en pensant à l'avenir» («Vor dem Hintergrund der

Vergangenheit an die Zukunft denken») behandelte die Konferenz insbesondere Fragen im Zusammenhang mit dem Internet der Dinge und dem Schutz der Privatsphäre von Kindern und prüfte namentlich mehrere nationale Sensibilisierungskampagnen. Sie befasste sich auch mit der Zukunft des rechtlichen Rahmens des Datenschutzes innerhalb der Europäischen Union und des Europarates. Die Konferenz verabschiedete vier Resolutionen über die Zukunft des Datenschutzes, den Entwurf einer Übereinkunft zwischen der Europäischen Union und den Vereinigten Staaten über Datenschutzstandards im Bereich polizeiliche und justizielle Zusammenarbeit in Strafsachen, den Einsatz von Body-Scannern und über den Jugendschutz, insbesondere durch die Planung gemeinsamer Sensibilisierungs- und Bildungsmassnahmen (siehe unsere Webseite www.derbeauftragte.ch, Themen – Datenschutz – Internationale Zusammenarbeit).

Arbeitsgruppe Polizei und Justiz

Die Arbeitsgruppe Polizei und Justiz der Europäischen Konferenz der Datenschutzbeauftragten hat die Aufgabe, die den Bereich Polizei betreffenden gesetzlichen Entwicklungen, namentlich im Zusammenhang mit dem Schengen-Besitzstand, zu verfolgen und die Aufsichtstätigkeiten zwischen den nationalen Datenschutzbehörden zu koordinieren. In diesem Kontext gibt sie Gutachten und Stellungnahmen ab. Wir haben an den verschiedenen Tagungen im Juni, Oktober und Dezember 2010 teilgenommen. Die Arbeitsgruppe erstellte insbesondere eine gemeinsame Methodik für die Risikobeurteilung vor den Dateninspektionen, um so die Wirksamkeit der Aufsicht zu verstärken.

Die Arbeitsgruppe gab eine Stellungnahme ab zur Schaffung eines europäischen Rahmens für die Bekanntgabe der Fluggastdatensätze (PNR) an Drittländer und für die Nutzung der PNR zu Strafverfolgungszwecken. Eine weitere Stellungnahme äussert sich zu den datenschutzrechtlichen Unzulänglichkeiten des Rahmenabkommens über den Austausch personenbezogener Daten, das zwischen der EU und den Vereinigten Staaten vorgesehen ist. Überdies hat die Arbeitsgruppe verschiedene Resolutionen verabschiedet, namentlich betreffend die Internet-Kriminalität, die zu Kontrollzwecken an den Flughäfen eingesetzten Body-Scanner sowie die mit Drittstaaten geschlossenen bilateralen Abkommen im Bereich Strafverfolgung. Sie äusserte sich auch zur Überarbeitung des durch den Vertrag von Lissabon geschaffenen rechtlichen Rahmens des Datenschutzes in der EU. Derzeit prüft sie die in Frage kommenden Formen der koordinierten Aufsicht sowie die Zukunft der Arbeitsgruppe.

Europäische Arbeitsgruppe für die Behandlung von datenschutzrelevanten Fällen

Bei ihren früheren Sitzungen konzentrierte sich die von der Europäischen Konferenz der Datenschutzbeauftragten eingesetzte europäische Arbeitsgruppe für die Behandlung von datenschutzrelevanten Fällen («Case Handling Workshop») auf die Kontrollmethoden, die von den Datenschutzbehörden entsprechend ihren jeweiligen gesetzlichen Kompetenzen verwendet werden. Im September 2010 untersuchte die Gruppe, der 25 nationale Datenschutzbehörden angehören, nun die verschiedenen für die reibungslose Abwicklung eines Kontrollverfahrens oder der Behandlung einer Beschwerde unerlässlichen Etappen.

Vier Etappen konnten auf diese Weise aufgezeigt werden: Der erste Kontakt mit dem zu kontrollierenden Datenbearbeiter, die Beurteilung des Falles und die Vorbereitung der Kontrolle, ihre Durchführung und schliesslich der Vollzug der Massnahmen oder der ausgesprochenen Sanktionen.

Die erste Etappe, der erste Kontakt mit dem Datenbearbeiter, ist für den Erfolg der geplanten Kontrolle entscheidend, zumindest was die Schaffung der bestmöglichen Voraussetzungen für ihre Durchführung betrifft. Dies ergab sich aus den Arbeiten der Gruppe und dem Erfahrungsaustausch zwischen den Teilnehmern. Die Gesetzgebung sieht für zahlreiche nationale Behörden Kontrollen in Form von Sachverhaltsabklärungen vor und erlaubt es ihnen, die Herausgabe von Schriftstücken oder Auskünften und die Vorführung der Bearbeitungen zu verlangen. Die Sachverhaltsabklärung erfordert die Mitarbeit des Datenbearbeiters. Es ist daher äusserst wichtig, dass der erste Kontakt unter guten Voraussetzungen stattfindet und dass der Datenbearbeiter klar und vollständig über den Rahmen und den Umfang der bevorstehenden Kontrolle sowie über die diesbezüglichen Rechtsgrundlagen informiert wird.

In einer zweite Phase des Kontrollverfahrens oder der Behandlung einer Beschwerde werden der Fall beurteilt und die Kontrolle vorbereitet. Ab einem gewissen Umfang braucht es einen Projektentwurf, der die Grenzen der Kontrolle, die zu stellenden Fragen, die betroffenen Akteure sowie die vorgesehene Planung festlegt. Anhand des Projektentwurfs lässt sich der Umfang der Kontrolle sowohl materiell als auch zeitlich abgrenzen. Die Erfahrungen der verschiedenen Teilnehmer haben deutlich gemacht, dass diese Vorbereitungsphase je nach Kontrolle von sehr unterschiedlicher Dauer sein kann. Es wurde auch hervorgehoben, dass manche Behörden einen Plan der im Laufe des Jahres vorgesehenen Kontrollen aufstellen und sich dabei auf bestimmte Bereiche oder Problemfälle konzentrieren, während andere Behörden ihre Kontrolltätigkeiten

vor allem in Abhängigkeit von den eingegangenen Beschwerden organisieren. Alle Teilnehmer der Arbeitsgruppe betonten, wie schwierig es sei, angesichts begrenzter Mittel bei den Kontrolltätigkeiten Prioritäten zu setzen.

In der dritten Etappe wird die Kontrolle durchgeführt. Sie umfasst grundsätzlich die Analyse der vom Datenbearbeiter gelieferten Dokumentation, den Besuch vor Ort und die Abfassung eines Kontrollberichts. Den Diskussionen der Arbeitsgruppe war zu entnehmen, dass der Besuch vor Ort ein grundlegendes Element im Kontrollablauf ist und dass nur sehr wenige Aufsichtstätigkeiten allein auf dem Korrespondenzweg wahrgenommen werden können. Vertreter anderer nationaler Behörden haben, wie wir auch, festgestellt, dass sich die Kontrollbehörde vor Ort begeben, die Fakten am Ort der Datenbearbeitung prüfen und die Fragen gestützt auf einen direkten Augenschein stellen muss, um ihre Aufgabe gründlich wahrnehmen und problematische Praktiken bei der Datenbearbeitung aufdecken zu können, die auf der Grundlage eines schriftlichen Austauschs alleine nicht erkannt worden wären.

Die vierte und letzte Etappe ist der Vollzug der Massnahmen oder der ausgesprochenen Sanktionen – es geht also um die Umsetzung der im Schlussbericht vorgesehenen Massnahmen. So geben wir im Anschluss an unsere Berichte Empfehlungen ab, wenn Verfehlungen festgestellt oder Datenschutzvorschriften verletzt wurden. Die Diskussionen haben ergeben, dass viele Datenschutzbehörden in ihrer innerstaatlichen Gesetzgebung über Massnahmen und Sanktionen in Form von Geldstrafen gegen den Datenbearbeiter verfügen, was im schweizerischen Recht bisher unbekannt ist. Im Rahmen einer weiteren Revision des Bundesgesetzes über den Datenschutz, allenfalls im Anschluss an die laufende Evaluation dieses Gesetzes, werden dieser Realität Rechnung zu tragen und derartige Möglichkeiten in Betracht zu ziehen sein (siehe auch Ziff. 3.1. des vorliegenden Tätigkeitsberichts).

Aufsichts-Koordinationsgruppe Eurodac

Die Koordinationsgruppe Eurodac überwacht die im Rahmen des Informationssystems Eurodac im Asylbereich bearbeiteten Daten. Sie koordiniert die Aufsichtstätigkeiten zwischen den nationalen Datenschutzbehörden und dem europäischen Datenschutzbeauftragten und verfolgt die Gesetzgebung. Wir haben an den Sitzungen im März, Oktober und Dezember 2010 teilgenommen.

Die Koordinationsgruppe inspiziert derzeit die vorzeitige Datenvernichtung im Eurodac-System, das heisst die endgültige Entfernung von Daten vor Ablauf der gesetzlichen Frist für ihre automatische Löschung. Wir beteiligen uns an dieser koordinierten Inspektion mit einer Kontrolle beim Bundesamt für Migration.

Bezüglich der Kontrolle der Gesetzgebung hat die Koordinationsgruppe zur Revision der Eurodac- und Dublin-Verordnungen Stellung genommen. Die Neufassung gab in diesem Stadium Anlass zu einer Resolution des europäischen Rates und des europäischen Parlaments, mit welcher das Zugriffsrecht auf das Eurodac-System im Falle von schweren Straftaten oder Terrorismus auf die Strafverfolgungsbehörden ausgeweitet wird. Die Gruppe äusserte sich auch zum Gesetzesvorschlag der Kommission zur Festlegung der Kompetenzen der neuen Agentur für das Betriebsmanagement von IT-Grosssystemen im Bereich Freiheit, Sicherheit und Recht betreffend Eurodac. Überdies hat die Koordinationsgruppe Vertreter der Zivilgesellschaft zu Asylfragen angehört, um Probleme und optimale Praktiken auszuwerten.

Gemeinsame Kontrollbehörde Schengen

Die gemeinsame Kontrollbehörde Schengen (GK) traf im Jahr 2010 vier Mal zusammen. Sie erarbeitete insbesondere Stellungnahmen, um die Bestimmungen des Übereinkommens zur Durchführung der Schengen-Abkommen auszulegen, setzte ihre Kontrolltätigkeiten fort und plante neue Inspektionen. Sie verabschiedete den Fortschrittsbericht zu den Empfehlungen, die sie anlässlich der Inspektion betreffend Warnmeldungen im Zusammenhang mit Personenbeschreibungen von Ausländern zum Zwecke der Nicht-Aufnahme ausgesprochen hatte. Die GK stellt fest, dass eine Folgekontrolle zweckmässig ist und die Unterschiede zwischen den Mitgliedstaaten bei der Befolgung der herausgegebenen Empfehlungen aufzeigt. Sie fordert die zuständigen Behörden auf, wachsam zu bleiben und eine wirksame Kontrolle zu gewährleisten. Auf unseren Wunsch hat sich die GK über die Praxis gewisser kantonaler Polizeibehörden unterhalten, die systematisch die Hotelanmeldeformulare mit den SIS-Personenbeschreibungen vergleichen, und sie vereinbarte, ein Gutachten zur Auslegung von Artikel 45 des Durchführungsübereinkommens vorzubereiten, der die Meldepflicht in den Beherbergungsstätten und die Bereitstellung der ausgefüllten Formulare für die zuständigen Behörden regelt. In ihren ersten Schlussfolgerungen vertritt die GK die Auffassung, dass eine automatische und systematische Überprüfung aller Personenbeschreibungen des SIS anhand der Meldevordrucke nicht im Einklang mit dem Durchführungsübereinkommen steht. Die GK wird im Jahre 2011 eine Folgeinspektion zu den Empfehlungen durchführen, die sie anlässlich der Kontrolle der Personen- oder Fahrzeugdaten erlassen hat, welche zum Zwecke der verdeckten Überwachung oder der gezielten Kontrolle ins SIS aufgenommen worden waren. Ebenso wird sie eine Inspektion betreffend Warnungen zu Personen durchführen, die zur Festnahme für eine Auslieferung ausgeschrieben sind.

Internationale Konferenz der Datenschutzbeauftragten

Die 32. Internationale Konferenz der Datenschutzbeauftragten fand auf Einladung der israelischen Datenschutzbehörde vom 26. bis 29. Oktober 2010 in Jerusalem statt (www.privacyconference2010.org). Zu dieser Konferenz versammelten sich rund 600 Vertreter der Datenschutzbehörden, der Regierungen, des Privatsektors, der akademischen Kreise und der Zivilgesellschaft. Die Diskussionen unter dem Thema «Privatleben: Generationen» drehten sich um die Verhaltensweisen der Menschen, die sich unter dem Einfluss der stetigen, grenzüberschreitenden Entwicklung der Informations- und Kommunikationstechnologien verändert haben. Die Konferenz befasste sich auch mit den Risiken, die diese Technologien für die Achtung der Rechte und Grundfreiheiten, namentlich das Recht auf Privatsphäre, mit sich bringen. So behandelten die Teilnehmer zahlreiche Themen im Zusammenhang mit dem Internet der Dinge, den sozialen Netzwerken, den Entwicklungen des datenschutzrechtlichen Rahmens, der Rolle der verschiedenen Akteure und ihren Verantwortlichkeiten und Pflichten im Bereich des Datenschutzes, und den Technologien und Instrumenten, welche die Achtung der Privatsphäre im Internet ermöglichen. Heikle Fragen zum geltenden Recht, zu Einwilligung, Anspruch auf Löschung oder Zugriff der Regierungen auf die Personendaten des Privatsektors wurden ebenfalls erörtert. Die Konferenz hat gezeigt, dass sich zwar die Verhaltensweisen ändern, die Anliegen des Schutzes der Privatsphäre unabhängig von den Generationen aber weiter bestehen. Die Technologie muss mehr denn je im Dienste der Privatpersonen stehen, insbesondere durch eine standardmässige Beachtung der Privatsphäre. Die Datenschutzbeauftragten bekräftigten erneut ihren Willen zu einer verstärkten Zusammenarbeit und zur Fortsetzung ihrer Bemühungen für die Annahme eines verbindlichen internationalen Instrumentariums auf weltweiter Ebene. Zu diesem Zweck verabschiedeten sie zwei Resolutionen. Die erste hat die Einrichtung einer Zusammenarbeitsstruktur innerhalb der internationalen Konferenz zum Ziel und beauftragt eine Arbeitsgruppe, im Jahr 2011 Vorschläge in diesem Sinne zu unterbreiten. Die zweite Resolution fordert die Regierungen der ganzen Welt auf, eine zwischenstaatliche Konferenz mit dem Ziel einer Übereinkunft über eine solche internationale Urkunde zu organisieren Mit dieser Resolution unterstützen die Datenschutzbeauftragten auch aktiv die Initiativen zur Suche nach geeigneten Lösungen, um den wirksamen Schutz der Grundrechte und Grundfreiheiten und die Ausübung dieser Rechte, namentlich das Recht auf die Privatsphäre bei der Verarbeitung von personenbezogenen Daten weiterhin zu gewährleisten. Die Datenschutzbeauftragten verabschiedeten auch eine Resolution zu «privacy by design», dem Grundsatz der datenschutzkonformen Entwicklung schon ab der Planung von Systemen, Dienstleistungen oder Produkten. Die Resolutionen sind zu finden auf unserer Website www.edoeb.admin.ch unter Themen – Datenschutz – Internationale Zusammenarbeit.

Arbeitsgruppe über die Informationssicherheit und den Schutz der Privatsphäre (OECD)

Die Arbeitsgruppe über die Informationssicherheit und den Schutz der Privatsphäre beschäftigte sich mit den technischen Innovationen, welche die grenzüberschreitende Speicherung und Auswertung von enormen Mengen von Personendaten ermöglichen, und mit der Revision der Richtlinien zu Sicherheit und Datenschutz. Weitere Themen waren die Entwicklung im Bereich von digitalen Signaturen, der Schutz von Kindern und Jugendlichen im Internet und die internationale Durchsetzung von Rechtsansprüchen in Sachen Datenschutz.

Zweifelsfrei hat sich mit der Entwicklung des Internets die Bearbeitung von Personendaten rasch und radikal geändert. Ein nie zuvor mögliches Volumen von Personendaten kann gespeichert und beliebig bearbeitet werden. Für die Bearbeitung dieser enormen Datenmengen stehen technische Verfahren zur Verfügung, welche praktisch jede vorstellbare Auswertung zulassen. Gleichzeitig können die Daten und die daraus gewonnenen Informationen praktisch an jedem Ort der Welt und in vielen Fällen ohne Wissen der betroffenen Personen bearbeitet und gespeichert werden. Damit stellen sich schwierige Fragen über das anwendbare Recht und die Durchsetzbarkeit von Rechtsansprüchen. Die Privatsphäre steht vor nie gekannten Herausforderungen, welche im heutigen globalen Umfeld gelöst werden müssen.

Angesichts dessen hat die Arbeitsgruppe angeregt zu prüfen, ob die 30-jährigen Richtlinien der OECD in Sachen Sicherheit und Datenschutz den neuen Gegebenheiten noch entsprechen. Im Laufe des vergangenen Jahres erschien ein Expertenbericht, der die neuen Herausforderungen aufzeigt. Es wird nun geprüft, inwiefern die acht Grundprinzipien der Richtlinie noch aktuell sind. Mittels eines Fragenkatalogs erhalten die Mitgliedsländer die Möglichkeit, Revisionsvorschläge zu unterbreiten.

Im Bereich des Identitätsmanagements und der digitalen Signaturen wurde ein vergleichender Bericht zu den bestehenden Modellen vorgestellt. Darin wird das österreichische Modell als optimale Lösung für eine digitale Identifikation, aber auch als Basismodell für e-Gov-Applikationen genannt. Vermehrt wird auf die fehlende Interoperabilität der Systeme hingewiesen, die trotz einiger Fortschritte das Haupthindernis für einen Durchbruch solcher Anwendungen darstellt.

Im gleichen Zeitraum wurden auch zwei Berichte der Arbeitsgruppe zu den Verantwortlichkeiten von Telekommunikationsdienstleistern (ISP) vorgestellt. Zurzeit besteht unter den Mitgliedländern keine Einigkeit, wie diese Verantwortlichkeiten festzulegen sind. Es ist strittig, inwieweit den ISP auch staatliche Aufsichts- und Kontrollaufgaben (zur Bekämpfung von Piraterie, Pädophilie etc.) auferlegt werden können. Zwei Standpunkte

zeichnen sich ab: Eine Seite bevorzugt eine detaillierte Formulierung der Verantwortlichkeiten von ISPs, während die andere Seite das Problem mittels Selbstregulierung angehen möchte. Das Thema wird noch einige Zeit für Diskussionen sorgen, da die verschiedenen nationalen Ansätze stark divergieren; für Wirtschaft und Benutzer aber wäre es von Vorteil, wenn ein gemeinsamer Lösungsansatz gefunden würde.

Zum Kinder- und Jugendschutz im Internet wurde ein umfangreicher Bericht vorgestellt. Er wurde mit Informationen aus den Mitgliedsländern ergänzt und soll im nächsten Jahr publiziert werden. Einige Länder vertreten die Auffassung, zum Schutz von Kindern und Jugendlichen im Internet solle eine OECD-Richtlinie erlassen werden.

Zur praktischen Umsetzung und Vereinfachung der grenzüberschreitenden Zusammenarbeit und Rechtsdurchsetzung in Datenschutzfragen wurde eine OECD-Webseite eröffnet (Global Privacy Enforcement Network, GPEN). Datenschutzbehörden aus der Schweiz und verschiedenen weiteren Ländern (u. a. Frankreich, Deutschland, Italien, Spanien, Kanada oder die USA) sind daran beteiligt. Der formlose Austausch von behördlichen Informationen stösst dabei aber an Grenzen, weil nationale Gesetze ihn nicht ohne Weiteres zulassen.

Schliesslich wurden im Laufe des letzten Jahres auch die Beitrittsgesuche von Chile, Israel, Estland und Slowenien geprüft und vom Ministerrat gutgeheissen. Grundsätzlich möchte der Rat zudem mit Ländern (u. a. Brasilien oder Indien), die eine schnelle wirtschaftliche Entwicklung aufweisen, enger zusammenarbeiten.

Französischsprachige Vereinigung der Datenschutzbehörden

Die französischsprachige Vereinigung der Datenschutzbehörden (Association francophone des autorités de protection des données personnelles, AFAPDP) hielt ihre 4. Konferenz am 30. November 2010 in Paris ab. Im Anschluss daran fanden die Generalversammlung der Vereinigung und ein Schulungsseminar für die Mitglieder der französischsprachigen Datenschutzbehörden statt. Die Konferenz befasste sich namentlich mit den Entwicklungen des Datenschutzrechts auf internationaler Ebene und innerhalb der Mitgliedsländer der Frankophonie. So haben wir die Rolle des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten unter dem Blickwinkel der Verabschiedung eines universellen Rechtsinstrumentariums vorgestellt. Die AFAPDP verabschiedete zwei Resolutionen. Die erste bezieht sich auf die Förderung der Verwendung der französischen Sprache als offizielle Arbeitssprache bei den internationalen Instanzen. Nach Auffassung der Vereinigung muss der multilaterale und mehrsprachige Charakter in den verschiedenen internationalen Instanzen und insbesondere innerhalb der internationalen Konferenz der Datenschutzbeauftragten gewahrt bleiben. Die zweite Resolution betrifft

die Förderung der «Annahme von Gesetzen über den Datenschutz und die Einrichtung von unabhängigen Kontrollbehörden in den französischsprachigen Staaten, in denen es keine solchen Behörden gibt», sowie die Unterstützung von «Initiativen im Hinblick auf die Annahme oder Änderung einer verbindlichen internationalen Urkunde über den Schutz der Privatsphäre und den Datenschutz und für die Verstärkung der internationalen Zusammenarbeit zwischen den Datenschutzbehörden». Die Vereinigung unterstützt insbesondere die Durchführung einer zwischenstaatlichen Konferenz mit dem Ziel, die Entwicklung eines solchen internationalen Instrumentariums zu fördern. Wir haben auch einen aktiven Beitrag zum Schulungsseminar geleistet, indem wir namentlich zwei Workshops leiteten, die den Grundprinzipien des Datenschutzes und der Organisation und der Arbeitsweise der Datenschutzbehörden gewidmet waren.

2. Öffentlichkeitsprinzip

2.1 Zugangsgesuche

2.1.1 Departemente und Bundesämter

Die Anzahl der eingereichten Zugangsgesuche bewegt sich auch 2010 im Rahmen der Vorjahre. Seit in Krafttreten des Öffentlichkeitsgesetzes zeigen sich zwei Tendenzen: Zum Einen wird der Zugang in immer weniger Fällen vollständig verweigert, zum Anderen wird vermehrt Einblick zumindest in Teilen gewährt. In gut einem Viertel aller Fälle, in denen die Verwaltung den Zugang eingeschränkt hatte, wurde ein Schlichtungsantrag eingereicht.

Gemäss den uns mitgeteilten Zahlen sind im Jahr 2010 bei den Bundesbehörden insgesamt 239 Zugangsgesuche eingereicht worden. In 106 Fällen gewährten die Behörden einen vollständigen, bei 63 Gesuchen einen teilweisen Zugang. In 62 Fällen wurde die Einsichtnahme komplett verweigert. Acht Fälle wurden als hängig gemeldet. Die statistischen Werte haben sich gegenüber den Vorjahren nicht grundlegend verändert (vgl. Statistik Ziff. 3.7).

Positiv kann erneut vermerkt werden, dass der Prozentsatz der vollständigen Verweigerungen seit Inkrafttreten des Öffentlichkeitsgesetzes kontinuierlich gesunken ist: Von 43 % (2006) über 33 % (2007) resp. 32 % (2008) und 29 % (2009) auf 26 % im Jahr 2010. Der Anteil der teilweise gewährten Zugänge ist innerhalb eines Jahres von 17 % (2009) auf den bisherigen Höchststand von 26 % (2010) gestiegen. Im Gegenzug dazu wurde im Berichtsjahr «lediglich» in 44 % Prozent aller Fälle ein vollständiger Zugang gewährt – so wenig wie noch nie seit Inkrafttreten des Öffentlichkeitsgesetzes (Durchschnittswert der Vorjahre: 54 %).

Interessant sind die grossen Unterschiede betreffend die Anzahl der gemeldeten Zugangsgesuche nach Bundesbehörden. So meldete beispielsweise das BAG deren 32. Demgegenüber teilten uns 20 Bundesbehörden mit, dass bei ihnen im Berichtsjahr 2010 keine Zugangsgesuche eingegangen sind. Dies zeigt erneut, dass die Aussagekraft der gemeldeten Zahlen eher gering ist. Es fehlt nach wie vor an einer systematischen Erfassung jedes einzelnen Zugangsgesuchs. Zudem ist davon auszugehen, dass in der Mehrheit aller Fälle gar nicht erst erkannt wird, dass es sich bei einer Anfrage überhaupt um ein Zugangsgesuch im Sinne des Öffentlichkeitsgesetzes handelt. In Wirklichkeit muss von einer weitaus grösseren Anzahl solcher Gesuche ausgegangen werden.

Im Berichtsjahr 2010 wurde den Gesuchstellern in 8 Fällen (2009: 6 Fälle) eine Gebühr in Rechnung gestellt. Der uns gemeldete Gesamtbetrag von Fr. 3460.– ist nur wenig geringer als jener aus dem Vorjahr (Fr. 3850.–). Aufgrund der eingereichten Schlichtungsanträge lässt sich jedoch festhalten, dass vereinzelt Ämter begonnen haben, deutlich höhere Gebühren zu verlangen.

Die Ämter und Departemente sind nicht verpflichtet, den zeitlichen Aufwand für die Bearbeitung von Zugangsgesuchen und die Mitwirkung bei Schlichtungsverfahren zu erfassen. Der Zeitaufwand wird in den verschiedenen Departementen zudem nicht einheitlich erfasst. Die uns auf freiwilliger Basis übermittelten Angaben sind daher nur bedingt aussagekräftig. Gemäss diesen hat der gemeldete Zeitaufwand erneut zugenommen (2007: 273 Stunden; 2008: 509 Stunden; 2009: 748 Stunden; 2010: 815 Stunden).

Die einzelnen Öffentlichkeitsberater der Ämter und Departemente beurteilen ihren Aufwand für die mit dem Öffentlichkeitsgesetz in Zusammenhang stehenden Arbeiten (Zugangsgesuche, Schlichtungsverfahren, amtsinterne Ausbildung, begleitende Rechtssetzung etc.) sehr unterschiedlich. Einige beurteilen ihn als eher gering, andere – insbesondere Berater bei Ämtern mit gesellschaftspolitisch relevanten Themen – melden einen beträchtlichen Arbeitsanfall. Einig sind sie sich alle darin, dass die Durchführung von Anhörungen bei Dritten und insbesondere die Teilnahme an Schlichtungsverfahren schnell mit grossem Zeitaufwand verbunden sind.

2.1.2 Parlamentsdienste

Gemäss Angaben der Parlamentsdienste wurde im Jahr 2010 kein Zugangsgesuch eingereicht.

2.2 Schlichtungsanträge

Im 2010 wurden insgesamt 32 Schlichtungsanträge eingereicht (vgl. Statistik Ziff. 3.9). Im Vorjahr waren es 41 gewesen. Insgesamt konnten 34 Schlichtungsanträge abgeschlossen werden. In zehn Fällen wurde zwischen den Beteiligten eine Schlichtung erzielt. In 14 Fällen erliessen wir – da keine einvernehmliche Lösung möglich oder von vornherein ersichtlich war – Empfehlungen. Zum Teil wurden mehrere Schlichtungsanträge mit einer Empfehlung oder einer Schlichtung erledigt. In je einem Fall kam es während des laufenden Schlichtungsverfahrens zum Rückzug eines Antrags bzw. gewährte das Amt von sich aus den Zugang. In drei Fällen wurde Zugang zu Dokumenten verlangt, die nicht in den persönlichen Geltungsbereich des Öffentlichkeitsgesetzes fallen. Interessanterweise wurden diese Gesuche allesamt von Rechtsanwälten gestellt. Einmal wurde der Schlichtungsantrag nicht fristgerecht eingereicht.

Diese Zahlen lassen folgende Schlüsse und Bemerkungen zu:

In 125 Fällen wurde der Zugang vollständig (62) respektive teilweise (63) verweigert. Dem stehen 32 beim Beauftragten eingereichte Schlichtungsanträge gegenüber. Mit anderen Worten wird im Berichtsjahr in knapp 26 % aller Fälle von ganz oder teilweise abgelehnten Zugangsgesuchen ein Schlichtungsantrag eingereicht. Im Vorjahr betrug diese Zahl 38 %.

Insgesamt führten wiederum zwei Drittel der abgeschlossenen Schlichtungsverfahren (Schlichtungen und Empfehlungen) zu einer für den Gesuchsteller günstigeren Lösung, d.h. zu einer Schlichtung respektive einem weitergehenden Zugang als ursprünglich vom Bundesamt zugestanden).

Unverändert bleibt der grosse Rückstand bei der Bearbeitung von Zugangsgesuchen und die damit für die Antragstellenden unbefriedigende Tatsache, dass sie zu lange auf die Durchführung ihres Schlichtungsverfahrens warten müssen. Das Bundesverwaltungsgericht hat den Beauftragten im Berichtsjahr erneut wegen Rechtsverzögerung gerügt (Urteil vom 01.03.2010, A-363/2010).

2.3 Abgeschlossene Schlichtungsverfahren

2.3.1 Empfehlungen

Nachfolgend werden die im Berichtsjahr erlassenen Empfehlungen im Bereich des Öffentlichkeitsgesetzes kurz zusammengefasst. Die vollständigen Versionen sind im Original auf unserer Webseite www.derbeauftragte.ch, Dokumentation – Öffentlichkeitsprinzip – Empfehlungen, zu finden. Fünf wichtige Empfehlungen werden im Anhang unter Ziff. 4.2. integral veröffentlicht.

Empfehlung BAG – EKIF / Interessenerklärungen (12. Februar 2010)

Die Antragstellerin verlangte Zugang zu den Interessenerklärungen der Mitglieder der Eidgenössischen Impfkommission (EKIF) und der Arbeitsgruppe «Impfung gegen humane Papillomaviren». Das BAG, welches das Sekretariat für die EKIF führt, verweigerte den Zugang mit Verweis auf die Botschaft des Bundesrates, gemäss der beratende Verwaltungskommissionen dem Öffentlichkeitsgesetz nicht unterstellt seien. Der Beauftragte wies in seiner Empfehlung darauf hin, dass laut Regierungs- und Verwaltungsorganisationsverordnung ausserparlamentarische Kommissionen, zu denen auch Verwaltungskommissionen gehören, der dezentralen Bundesverwaltung zugeordnet werden, und daher das Öffentlichkeitsgesetz zur Anwendung gelange. Er empfahl, den Zugang zu den Interessenerklärungen aufgrund eines überwiegenden öffentlichen Interesses (Schutz der öffentlichen Gesundheit) zu gewähren. Die vollständige Empfehlung befindet sich im Anhang unter Ziff. 4.2.1.

Empfehlungen BSV / IV-Checkliste I und II (16. März 2010)

Zwei Antragsteller verlangten unabhängig voneinander Zugang zur IV-Checkliste, die das Bundesamt für Sozialversicherungen (BSV) den kantonalen IV-Stellen zusammen mit einem Konzept zur Betrugsbekämpfung zugestellt hatte. Das BSV verweigerte den Zugang zur gesamten Liste mit der Begründung, die Bekanntgabe verhindere die zielkonforme Durchführung einer konkreten behördlichen Massnahme – nämlich die effiziente Triage von möglichen Missbrauchsfällen. Dieser Sichtweise konnte sich der Beauftragte nicht anschliessen. Zum Einen sind bereits seit längerem Teile der Checkliste in der Öffentlichkeit bekannt (und dennoch hat das BSV auf den Rückzug der Liste verzichtet). Zum Andern qualifizierte der Beauftragte den Einsatz der IV-Checkliste nicht als konkrete behördliche Massnahme. Vielmehr sei sie einfach ein standardisierter Fragenkatalog und diene als Hilfsmittel zur Vorausscheidung von mutmasslichen Missbrauchsfällen zuhanden der internen IV-Betrugsspezialisten. Das Bekanntwerden der Liste habe kein ernsthaftes Schadensrisiko zur Folge. Darum empfahl der Beauftragte

den Zugang zur gesamten IV-Checkliste zu gewähren. Die vollständige Empfehlung Checkliste I befindet sich im Anhang unter Ziff. 4.2.2. Zum Entscheid des Bundesverwaltungsgerichts siehe auch Ziff. 2.4.1 des vorliegenden Tätigkeitsberichts.

Empfehlung VBS / Grad und Funktion (26. März 2010)

Der Antragsteller verlangte vom Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) Auskunft darüber, ob Rechtsradikale als Vorgesetzte in der Schweizer Armee dienen. Dazu reichte er eine Liste mit Personennamen ein und wollte wissen, ob diese Personen einen Unteroffiziers- oder Offiziersgrad bekleideten. Diese Informationen sind im Personalinformationssystem (PISA) der Armee enthalten. Das VBS verweigerte dem Antragsteller aber aus Gründen des Datenschutzes den Zugang zu den Auszügen aus PISA. Der Beauftragte gelangte ebenfalls zum Schluss, dass im konkreten Fall die gewünschten Angaben weder gestützt auf eine Spezialbestimmung noch gestützt auf das Öffentlichkeitsgesetz und das Datenschutzgesetz bekannt gegeben werden könnten. Er empfahl daher dem VBS, den Zugang zu den PISA-Auszügen nicht zu gewähren.

Empfehlung Swissmedic / Zulassungsdossiers (30. März 2010)

Zwei Antragstellerinnen verlangten bei Swissmedic Zugang zu zahlreichen Dokumenten betreffend die Zulassung von Medikamenten. Da Swissmedic einen teilweisen Zugang zu den Zulassungsdossiers in Betracht zog, hörte es die betroffenen Unternehmen an. Diese sprachen sich einerseits aufgrund von Geschäfts- und Fabrikationsgeheimnissen und anderseits zum Schutz ihrer Privatsphäre dagegen aus. Weil Swissmedic an der teilweisen Zugangsgewährung festhielt, reichten sowohl die Antragsstellerinnen als auch die betroffenen Unternehmen Schlichtungsanträge ein. Der Beauftragte beurteilte das Vorgehen und die Einschätzung von Swissmedic in Bezug auf das Vorliegen von Fabrikations- und Geschäftsgeheimnissen sowie in Bezug auf den Schutz von Persondaten Dritter insgesamt als rechtmässig und angemessen. Er empfahl Swissmedic, an dem vom ihm vorgeschlagenen teilweisen Zugang zu den Zulassungsdossiers festzuhalten. Die vollständige Empfehlung befindet sich im Anhang unter Ziff. 4.2.3.

Empfehlung BJ / Loterie Romande (28. April 2010)

Der Antragsteller reichte beim Bundesamt für Justiz (BJ) ein Gesuch um Zugang zu den Zahlen nicht verkaufter Lose der Loterie Romande für 2008 ein. Das BJ antwortete, die entsprechenden Zahlen seien leider nicht übermittelt worden. Der Beauftragte stellte in seiner Empfehlung fest, dass sich das Öffentlichkeitsgesetz ausschliesslich auf Dokumente bezieht, die sich im Besitz der Behörde befinden, von der sie stammen oder der sie mitgeteilt worden sind. Mit anderen Worten kann ein Gesuchsteller auf der

Basis des Öffentlichkeitsgesetzes nicht verlangen, dass das BJ ein Dokument erstelle. Die vollständige Empfehlung befindet sich im Anhang des französischen Teils unter Ziff. 4.2.4.

Empfehlung BAG / Zugang Verträge Pandemieimpfstoffe (12. Mai 2010)

Der Antragsteller verlangte Zugang zu drei Verträgen (Kauf von Pandemie-Impfstoffen), welche die Eidgenossenschaft mit zwei Pharmaunternehmen abgeschlossen hatte. Das Bundesamt für Gesundheit (BAG) gewährte den teilweisen Zugang zu den Verträgen, wovon einer bereits zweimal Gegenstand einer Empfehlung des Beauftragten gewesen war. Der Beauftragte stützte die Einschätzung der Vertragsinhalte als Geschäfts- und Fabrikationsgeheimnis durch das BAG mit Ausnahme einer Seite eines Vertrages, die allgemein bekannt ist.

Empfehlung BLW / Erweiterung der Liste nicht bewilligungspflichtiger Pflanzenschutzmittel (8. Juni 2010)

Ein Unternehmen verlangte beim Bundesamt für Landwirtschaft (BLW) Zugang zu zwei Briefen, in welchen im Rahmen eines Verfahrens um die Aufnahme von Produkten in die Liste nicht bewilligungspflichtiger Pflanzenschutzmittel Vorbehalte erhoben wurden. Das Amt beabsichtigte, den teilweisen Zugang zu den beiden Briefen zu gewähren, und hörte daher die betroffene Drittperson an. Diese war grundsätzlich einverstanden, begehrte jedoch die Einschwärzung einer Textpassage, welche Personendaten einer weiteren Drittperson enthielten. Der Beauftragte stützte die Auffassung des BLW hinsichtlich der Einschätzung des Geschäftsgeheimnisses und der fehlenden Zusicherung der Geheimhaltung von mitgeteilten Informationen. In Bezug auf die fragliche Textpassage empfahl er jedoch die Durchführung einer Anhörung der betroffenen Drittperson.

Empfehlung BJ / Faxschreiben an die USA in der Sache Roman Polanski (9. Juni 2010)

Der Antragsteller stellte beim Bundesamt für Justiz (BJ) ein Gesuch um Zugang zum Fax des BJ an das Office of International Affairs vom 21. September 2009 betreffend Roman Polanski, sowie zu Dokumenten, die zur Versendung dieses Fax führten und die sich auf dessen Inhalt bezogen. Das BJ lehnte das Zugangsgesuch mit der Begründung ab, die verlangten Dokumente seien Teil eines Verfahrens der internationalen Rechtshilfe. Der Beauftragte stützte in seiner Empfehlung diese Einschätzung und hielt fest, dass das Öffentlichkeitsgesetz nicht für den Zugang zu Dokumenten eines Verfahrens der internationalen Rechtshilfe gilt.

Empfehlung VBS / Bericht «Islamistische Imame» (21. Oktober 2010)

Zwei Journalisten verlangten vom Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) Zugang zu einem Bericht mit dem Titel «Islamistische Imame», der vom Stab des Sicherheitsausschusses des Bundesrates erstellt worden war. Das VBS teilte den Antragstellern mit, dass der Bericht als vertraulich klassifiziert sei – es verweigerte den Zugang zum Bericht, weil sonst die innere oder äussere Sicherheit gefährdet sowie die aussenpolitischen Interessen oder die internationalen Beziehungen der Schweiz beeinträchtigt werden könnten. Der Beauftragte teilte diese Einschätzung nicht und empfahl daher, den Bericht in weiten Teilen zugänglich zu machen. Die vollständige Empfehlung befindet sich im Anhang unter Ziff. 4.2.5.

Empfehlung VBS / Inspektionsberichte ND-Aufsicht (18. November 2010)

Ein Journalist reichte beim Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) ein Gesuch um Zugang zu zwei Inspektionsberichten der Nachrichtendienstlichen Aufsicht VBS betreffend Staatsschutz ein. Das VBS lehnte das Gesuch mit der Begründung ab, die Inspektionsberichte seien als vertraulich klassifiziert und dienten den zuständigen Aufsichtsbehörden als Grundlage für den Entscheid weiterer Massnahmen. Weiter begründete es seinen ablehnenden Entscheid auch damit, dass die Zugangsgewährung die Sicherheit der Schweiz, die aussenpolitischen Interessen des Landes sowie die Beziehungen zwischen Bund und den Kantonen beeinträchtigen könnte. Der Beauftragte wies das VBS darauf hin, dass das Öffentlichkeitsgesetz nicht auf jenen Inspektionsbericht anwendbar sei, der im unmittelbaren und besonderen Auftrag der Geschäftsprüfungsdelegation erstellt worden war und damit nach Parlamentsgesetz explizit als vertraulich qualifiziert wird. In Bezug auf den zweiten Inspektionsbericht stützte der Beauftragte die Argumentation des VBS, wonach die vollumfängliche Zugänglichmachung des Berichts die innere und äussere Sicherheit der Schweiz ernsthaft gefährden könnte. Folglich empfahl der Beauftragte eine teilweise Veröffentlichung.

Empfehlung EDA / Autorisiertes Interview (9. Dezember 2010)

Der Antragsteller verlangte vom Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) Zugang zu Dokumenten im Zusammenhang mit einem Interview, welches die Departementsvorsteherin einer Tageszeitung gewährt hatte. Das EDA lehnte das Zugangsgesuch mit den Begründungen ab, die Dokumente seien nicht fertig gestellt bzw. zum persönlichen Gebrauch bestimmt. Aus seiner Sicht handelt es sich erst bei dem in der Tageszeitung publizierten autorisierten Interview um ein definitives

Dokument. Der Beauftragte qualifizierte hingegen nicht erst das publizierte Interview, sondern bereits das Dokument mit dem autorisierten Interview als fertig gestelltes Dokument, da es den letzten und definitiven Arbeitsschritt verwaltungsrechtlichen Handelns darstellt. Er empfahl dem EDA, dieses Dokument herauszugeben.

Empfehlung EDA / Akkreditierung eines Botschafters (22. Dezember 2010)

Der Antragsteller verlangte vom Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) Zugang zum Beglaubigungsschreiben des deutschen Botschafters in der Schweiz sowie zu Kopien seines Diplomatenpasses. Das EDA lehnte dies ab, weil ganz allgemein die Beziehungen mit anderen Staaten und im Besonderen jene mit Deutschland beeinträchtigt würden, wenn Dokumente, die entsprechend der diplomatischen Gewohnheit einem anderen Staat vertraulich übergeben wurden, zugänglich gemacht würden. Demgegenüber ging der Beauftragte nicht davon aus, dass die Zugänglichmachung des Beglaubigungsschreibens zu einer Beeinträchtigung der Beziehungen mit Deutschland führen würde, und empfahl den Zugang dazu zu gewähren. Die Herausgabe der Kopien des Diplomatenpasses lehnte er aus datenschutzrechtlichen Gründen ab.

Empfehlung BLW / Vom EVD eingesetzte Arbeitsgruppe (23. Dezember 2010)

Die Antragstellerin begehrte beim BLW Einsicht in eine Liste mit 250 Vorschlägen («Synopsis») der Arbeitsgruppe «Begleitmassnahmen Freihandelsabkommen». Das BLW verweigerte die Einsicht mit der Begründung, die Arbeitsgruppe gehöre nicht der Bundesverwaltung an und unterstehe damit nicht dem Öffentlichkeitsgesetz. Zudem habe die Arbeitsgruppe entschieden, keine Zwischenergebnisse zu veröffentlichen. In seiner Empfehlung wies der Beauftragte vorweg auf zwei grundlegende Tatsachen hin: Erstens untersteht jede von der Bundesverwaltung eingesetzte Arbeitsgruppe dem Öffentlichkeitsgesetz. Zweitens können die dem Transparenzprinzip unterliegenden Stellen (Departemente, Ämter, alle Arbeits- und Expertengruppen, Gutachter etc.) nicht in eigener Kompetenz von ihnen erstellte Dokumente vom Öffentlichkeitsgesetz ausschliessen – vielmehr sind die Dokumente nach den Vorgaben dieses Gesetzes zu beurteilen. Nach erfolgter Schlichtungsverhandlung qualifizierte der Beauftragte das Dokument «Synopsis» als amtliches Dokument und empfahl dessen Zugänglichmachung in anonymisierter Form. Die vollständige Empfehlung befindet sich im Anhang unter Ziff. 4.2.6.

2.3.2 Schlichtungen

In folgenden Fällen konnte eine Schlichtung erzielt werden:

Schlichtung BAG / Verträge H1N1

Der Antragssteller ersuchte das BAG um die Zustellung von Kopien der Verträge über den Kauf von Pandemieimpfstoffen. Da die Behörde nicht innerhalb der gesetzlichen Frist Stellung genommen hatte, reichte der Antragssteller ein Schlichtungsgesuch ein. Auf Intervention des Beauftragten stellte das BAG die Verträge zu.

Schlichtung BFS / Bericht Bodenpreisstatistik

Der Antragsteller ersuchte das BFS um Zustellung eines Berichtes zur Vernehmlassung der schweizerischen Bodenpreisstatistik mit Erscheinungsdatum vom Mai 1997. Das BFS teilt dem Antragsteller mit, dass das Dokument vor Inkrafttreten des Öffentlichkeitsgesetzes erstellt worden und daher nicht zugänglich sei («Amtsgeheimnis»). Nach Intervention des Beauftragten erklärte sich das BFS bereit, den Bericht dem Antragsteller trotzdem zuzustellen.

Schlichtung SAS / Auditbericht

Der Antragssteller ersuchte die Schweizerische Akkreditierungsstelle (SAS) um Zugang zu einem Auditbericht. In einer Schlichtungsverhandlung beim Beauftragten einigten sich die Beteiligten über das weitere Vorgehen, insbesondere über die Anhörung der betroffenen Drittperson.

Schlichtung BAV / Expertenbericht Lärmbelastung Hafenbahn

Die Antragsstellerin ersuchte das Bundesamt für Verkehr (BAV) um Zugang zu einem Expertenbericht, der sich mit der Lärmbelastung durch den Betrieb der Hafenbahn (Basel) für die Anwohnerinnen und Anwohner befasste. Das BAV reagierte auf die Zugangsgesuche der Antragstellerin nicht. Nach Intervention des Beauftragten wurde der Bericht der Antragstellerin umgehend zugestellt.

Schlichtung BIT / Liste Datensammlungen

Der Antragssteller ersuchte das Bundesamt für Informatik und Telekommunikation (BIT) um Zugang zu einer Liste über die vom BIT im Auftrag von Dritten verwalteten sowie die selber betriebenen Datensammlungen. Das BIT verweigerte in einem Fall den Zugang und teilte dem Antragsteller die Höhe der Gebühren mit. Nach Intervention des Beauftragten wurden dem Antragsteller die verlangten Listen kostenlos zugestellt.

Schlichtung EDA / Visa-Weisungen Libyen

Der Antragssteller verlangte die Herausgabe der Weisungen zur Visumerteilung an libysche Staatsangehörige, was das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) mit Verweis auf die bilateralen Probleme mit Libyen ablehnte.

Im Schlichtungsverfahren einigten sich die Beteiligten darauf, dass das EDA die Frage der Herausgabe der Weisungen entweder nach der Veröffentlichung des Berichts der parlamentarischen Geschäftsprüfungskommission zur Akte «Libyen» oder nach Beendigung des Schiedsgerichtsverfahrens zwischen den beiden Ländern nochmals prüft.

Schlichtung BAZL / Audits und Inspektionsberichte

Der Antragssteller verlangte Zugang zum Geschäftsverwaltungssystem bzw. die Erstellung einer detaillierten Auflistung der Audits und Inspektionen der Bereiche Flugzeugtechnik, Flugsicherheit und Infrastruktur in elektronischer Form. Das Bundesamt für Zivilluftfahrt (BAZL) verweigerte den Zugang u. a. mit dem Argument, das Gesuch sei nicht hinreichend genau formuliert. Auf Anregung des Beauftragten erstellte das BAZL eine Liste der durchgeführten Audits und Inspektionen. Damit zeigte sich der Antragsteller zufrieden.

Schlichtung SBF / Raumfahrtforschung

Der Antragssteller verlangte Zugang zu zahlreichen Unterlagen betreffend die internationale Zusammenarbeit im Bereich der Raumfahrt. Nach Einreichung des Schlichtungsantrags blieb das Staatssekretariat für Bildung und Forschung (SBF) mit dem Antragsteller in Kontakt. In der Folge teilte dieser dem Beauftragten mit, dass aufgrund der positiven Entwicklung der Gespräche mit dem SBF das Schlichtungsverfahren eingestellt werden könne.

Schlichtung BAFU / Steuererleichterungen Treibstoffökobilanz

Der Antragssteller verlangte Zugang zu den Unterlagen über die Gesuche um Steuererleichterungen im Zusammenhang mit der Treibstoffökobilanz-Verordnung. Das Bundesamt für Umwelt (BAFU) teilte dem Antragsteller mit, das Prüfungsverfahren sei noch nicht abgeschlossen, und erklärte darüber hinaus, ein Zugang könne aufgrund von Geschäftsgeheimnissen und zum Schutz von Personendaten nicht gewährt werden. An der Schlichtungsverhandlung, an der auch die für den definitiven Entscheid betreffend Steuererleichterungen zuständige Oberzolldirektion teilnahm, stellte sich heraus, dass der Antragsteller nicht die ganzen Dossiers, sondern nur bestimmte Informationen wollte. Die beiden Bundesämter erteilten diese Auskünfte und der Antragsteller zeigte sich ob dem Resultat sehr zufrieden.

Schlichtung BFS / Gutachten des Methodendienstes

Die Antragsstellerin ersuchte um Zugang zum Gutachten des Methodendienstes des Bundesamtes für Statistik (BFS) zur Repräsentativität der Zentralen Auswertung von Buchhaltungsdaten. Nach Intervention des Beauftragten kam das BFS auf seinen ursprünglichen Entscheid zurück und stellte der Antragstellerin das verlangte Gutachten zu.

2.4 Gerichtsentscheide zum Öffentlichkeitsgesetz

2.4.1 Bundesverwaltungsgericht

Das Bundesverwaltungsgericht (BVGer) hat entschieden, dass die IV-Checkliste des Bundesamtes für Sozialversicherungen (BSV) öffentlich zugänglich sein muss. Das Gericht stützte sich dabei auch auf die Argumentation des Beauftragten in seiner Empfehlung vom 16. März 2010. Gemäss Urteil ist es unwahrscheinlich, dass die standardisierte Checkliste nach ihrer Publikation nicht mehr als Arbeitsinstrument eingesetzt werden könne. Damit folgte das Gericht nicht der Argumentation des BSV, wonach die Veröffentlichung der Checkliste die Aufdeckung von möglichen IV-Missbrauchsfällen ernsthaft gefährde, wohl aber der Empfehlung des Beauftragten (siehe Urteil vom 18. Oktober 2010, Ref. A-3269/2010).

In Zusammenhang mit einer Empfehlung des Beauftragten vom 22. April 2009 zuhanden des Bundesamtes für Gesundheit (vgl. unseren 17. Tätigkeitsbericht 2009/2010, Ziff. 2.3.1) konkretisierte das BVGer, dass Dokumente, welche die Verwaltung im Hinblick auf die Vorbereitung eines Bundesratsantrags erstellt, nicht unter das Mitberichtsverfahren fallen, das vom Öffentlichkeitsgesetz ausgenommen ist. Somit unterliegen Dokumente, die der verwaltungsinternen Meinungs- und Willensbildung vor dem Mitberichtsverfahren dienen, grundsätzlich dem Öffentlichkeitsprinzip, unabhängig davon, ob die Verwaltung sie selber erstellt oder von Dritten erhalten hat. Diese Dokumente bleiben grundsätzlich zugänglich, selbst wenn sie dem Bundesratsantrag als Anhang beigefügt worden sind (siehe Urteil vom 3. Mai 2010, Ref. A-4049/2009).

Der Beauftragte wurde im Berichtsjahr vom BVGer erneut wegen Rechtsverzögerung gerügt (siehe Urteil vom 1. März 2010, Ref. A-363/2010).

2.4.2 Bundesgericht

Das Bundesgericht (BGer) definierte in seinem Entscheid vom 19. Mai 2010 (Ref. 1C_522/2009) definiert, welche amtlichen Dokumente zum Mitberichtsverfahren gehören. Konkret ging es um die Auflösungsvereinbarungen betreffend die Arbeitsverträge des ehemaligen Generalsekretärs des Eidgenössischen Justiz- und Polizeidepartements (EJPD) und seines Stellvertreters. Das Bundesverwaltungsgericht (BVGer) hatte zuvor entschieden, diese Vereinbarungen seien – da Teil eines Bundesratsantrags –, als Dokumente des Mitberichtsverfahrens zu qualifizieren und somit gemäss dem Öffentlichkeitsgesetz nicht zugänglich. Das BGer hielt fest, dass diese Bestimmung restriktiv zu interpretieren ist: Zum Mitberichtsverfahren gehören nur Dokumente, die zwischen der Unterzeichnung des Bundesratsantrags durch den Departementschef und dem Entscheid des Gesamtbundesrates erstellt werden. Indirekt entschied das BGer

damit auch, dass Auflösungsvereinbarungen von hohen Verwaltungsangestellten des Bundes der Öffentlichkeit grundsätzlich zugänglich sind. Zudem machte es deutlich, dass Transparenz nunmehr die Regel, Geheimhaltung jedoch nur noch in Ausnahmefällen möglich ist. Es hob den angefochtenen Entscheid auf und wies die Vorinstanz an, den Fall neu zu beurteilen und die Interessenabwägung vorzunehmen. Das BVGer kam nun zum Schluss, dass das Interesse des Gesuchstellers – und damit im weiteren Sinne der Öffentlichkeit – am Einblick in die Vereinbarungen jenes der beiden Betroffenen am Schutz ihrer Privatsphäre überwiegt (siehe Entscheid des BVGer vom 17. Februar 2011; Ref: A3609/2010). Somit sind die fraglichen Dokumente öffentlich zugänglich. Der Beauftragte hatte dies in seiner Empfehlung vom 9. Februar 2009 ebenso gesehen (vgl. unseren 17. Tätigkeitsbericht 2009/2010, Ziff. 2.3.1).

2.5 Ämterkonsultationen

2.5.1 Revision des Lebensmittelgesetzes

Der Beauftragte hat zur Revision des Lebensmittelgesetzes Stellung genommen. Gemäss Entwurf sollen in bestimmten Bereichen gewisse Dokumente nicht dem Öffentlichkeitsprinzip unterliegen. Nach Ansicht des Beauftragten gibt es indes stets gute Gründe für eine weitergehende Transparenz. Sollte sich der Gesetzgeber für eine Spezialbestimmung im Sinne von Art. 4 BGÖ aussprechen, ist es in den Augen des EDÖB notwendig, die einzelnen amtlichen Dokumente, die vom Öffentlichkeitsgesetz ausgenommen werden sollen, inhaltlich klar und eindeutig zu definieren. Nur so hätten Konsumentinnen und Konsumenten Klarheit darüber, dass sie kein Recht auf Zugang zu bestimmten Informationen (wie Kontroll- und Testberichte) haben.

Weiter sah der Entwurf eine Bestimmung mit dem Titel «Schweigepflicht» vor, die sämtliche Personen, die amtliche Funktionen wahrnehmen, dem Amtsgeheimnis unterstellen soll. Laut den erklärenden Ausführungen sollte damit in erster Linie die Verschwiegenheit der externen Auftragnehmer festgeschrieben werden. Der Beauftragte hat in diesem Zusammenhang darauf hingewiesen, dass diese Schweigepflichtnorm keinen anderen Zweck hat, als die Geltung des Amtsgeheimnisses gemäss Artikel 22 des Bundespersonalgesetzes auch auf verwaltungsexterne Personen auszudehnen. Da das Amtsgeheimnis mit Inkrafttreten des Öffentlichkeitsgesetzes in seiner Tragweite neu definiert worden ist, umfasst es heute nur (noch) Informationen, die nicht dem Geltungsbereich des Öffentlichkeitsgesetzes unterstehen, die durch spezialgesetzliche Bestimmungen als geheim erklärt werden oder die unter eine der im Öffentlichkeitsgesetz selbst vorgesehenen Ausnahmebestimmungen fallen. Weder das Amtsgeheimnis noch die im Entwurf des Lebensmittelgesetzes vorgeschlagene Schweigepflichtnorm stellen somit eine Spezialbestimmung im Sinne von Artikel 4 BGÖ dar. Weiter wies der Beauftragte darauf hin, dass das Öffentlichkeitsgesetz zum Schutz von Geschäfts- und Fabrikationsgeheimnissen sowie der Privatsphäre und der Personendaten Dritter entsprechende Massnahmen vorsehe und seines Erachtens die Schweigepflicht in der vorgeschlagenen Form nicht notwendig sei.

2.5.2 Informationsschutz

Im Rahmen der Ämterkonsultation zum Bericht des Bundesrates über die Umsetzung der Informationsschutzverordnung und zur Schaffung einer formell-gesetzlichen Grundlage für den Informationsschutz gab der Beauftragte seinen grundsätzlichen Zweifeln darüber Ausdruck, dass die Schaffung einer solchen Grundlage innerhalb der Verwaltung unbestritten sei. Weiter vertrat er die Ansicht, dass zum Einen der Bedarf nach einem Ausbau des Informationsschutzes nicht nachvollziehbar dargelegt worden

sei und zum Anderen der Gesetzgeber mit Einführung des Öffentlichkeitsgesetzes klar gemacht hatte, dass sich die Bundesverwaltung in ihrem Handeln an der Transparenz orientieren müsse. Der Beauftragte zeigte sich daher erstaunt darüber, in welchem Ausmass und Umfang der Informationenschutz in der Verwaltung, insbesondere im zivilen Bereich, nun wieder gestärkt werden sollte. Zudem rügte er, dass die Aussagen zum Öffentlichkeitsgesetz wenig präzis und in der Sache verschiedentlich nicht fundiert seien.

3. Der EDÖB

3.1 Evaluation des Bundesgesetzes über den Datenschutz

Das Bundesamt für Justiz (BJ) beauftragte das Büro Vatter AG, das Institut für Europarecht der Universität Freiburg und das Meinungsforschungsinstitut Demoscope AG mit einer Evaluation der Wirksamkeit des Bundesgesetzes über den Datenschutz (DSG). Um die Evaluationsarbeit zu begleiten, setzte das BJ eine aus Vertretern der Bundesverwaltung, des EDÖB, der kantonalen Datenschutzbehörden und der Wirtschaft sowie aus unabhängigen Experten bestehende Arbeitsgruppe ein. Ihr Bericht sollte im Laufe des Jahres 2011 veröffentlicht werden. Diese Evaluation könnte eine Revision des DSG nach sich ziehen. Sie bietet dem EDÖB die Gelegenheit, sich Fragen nach der Sachdienlichkeit des geltenden Rechts zu stellen und einige Denkanstösse zu geben.

Die vom Büro Vatter AG in Zusammenarbeit mit dem Institut für Europarecht der Universität Freiburg und dem Meinungsforschungsinstitut Demoscope AG durchgeführte Evaluation hat zum Ziel, die Effektivität und Wirksamkeit gewisser Bestimmungen des Gesetzes zu analysieren und gegebenenfalls Änderungsvorschläge zu machen. Die Evaluation legt das Schwergewicht hauptsächlich auf die Bekanntheit des Gesetzes und auf die Durchsetzungsmechanismen. Die Evaluatoren prüfen insbesondere, wie weit die Rechte der betroffenen Personen und das Verfahren zur Geltendmachung dieser Rechte tatsächlich ermöglichen, die Achtung der Grundrechte und der Privatsphäre zu gewährleisten. Die Evaluation bezieht sich auch auf die Rolle, die Aufgaben und die Befugnisse des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten. Die Resultate sollten im Laufe des Jahres 2011 veröffentlicht werden. Diese Evaluation bietet auch Gelegenheit zu Überlegungen betreffend die Sachdienlichkeit des geltenden Rechts, wenn es darum geht, sich den Herausforderungen der Informations- und Kommunikationstechnologien zu stellen.

Das Bundesgesetz über den Datenschutz ist ein Rahmengesetz, das die Bearbeitung von Personendaten in ihrer Gesamtheit regelt, ungeachtet der Art der Daten und ihrer Bearbeitungsweise. Es ist technologisch neutral. Obwohl die ab Artikel 4 aufgeführten Grundprinzipien des Datenschutzes für die modernen Datenbearbeitungstechnologien weiterhin anwendbar sind, kann man sich angesichts der neuen Informations- und Kommunikationstechnologien, die insbesondere auf der Allgegenwart, der Überwachung, der Geolokalisierung, der Miniaturisierung, der Nutzernähe (Internet der Dinge), der Erstellung von Personenprofilen, der Ablaufverfolgung und dem ständigen Kontakt beruhen, durchaus Fragen nach der Effektivität des Gesetzes stellen. Der Einzelne hat

immer weniger Gelegenheit, allein und vor fremden Blicken geschützt zu leben, und all sein Tun und Handeln kann registriert, analysiert und verwertet werden. Er ist nicht nur Subjekt von ihn betreffenden Bearbeitungen von Personendaten, er ist auch Verantwortlicher für die Bearbeitung, namentlich durch die Nutzung von sozialen Netzwerken. Er ist sich wohl der Bedeutung der Informationen bewusst und schätzt die Vorteile und Möglichkeiten der heutigen Technologien, aber er ermisst oft nicht genügend die Risiken, die mit diesen Technologien verbunden sind, und ist immer weniger in der Lage, die Kontrolle über die ihn betreffenden Informationen zu behalten. Die Datenbearbeitung geht weit über die nationalen Grenzen hinaus und erfordert internationale Antworten, um die Achtung der Grundrechte und -freiheiten, namentlich den Schutz der Privatsphäre, zu gewährleisten.

So betrachtet, und ohne deswegen den technologisch neutralen Ansatz oder andere Grundlagen des Gesetzes ändern zu wollen, sind wir der Ansicht, dass einige Anpassungen notwendig sind, um einerseits unsere Gesetzgebung mit dem europäischen Recht in Einklang zu bringen und so den Erwartungen der international tätigen Unternehmen gerecht zu werden, und um andererseits auf die neuen technologischen Herausforderungen zu reagieren. Insbesondere wäre es angebracht, für eine grössere Transparenz der Bearbeitung von Personendaten zu sorgen, die Pflichten und Verantwortlichkeiten der Datenbearbeiter auszubauen, die Kontrolle der Privatpersonen über ihre Daten zu gewährleisten und die Effektivität des Gesetzes zu verstärken.

Unseres Erachtens ist es auch notwendig, den Geltungsbereich des Gesetzes auf sämtliche von Bundesinstanzen vorgenommene Bearbeitungen auszudehnen und die Begriffsbestimmungen denen des europäischen Rechts anzugleichen. Überdies wird der Unterschied zwischen öffentlichem und privatem Sektor geringer, weshalb man sich zu Recht fragen kann, ob es noch zweckmässig sei, sie unterschiedlichen Datenschutzregelungen zu unterwerfen.

Nach unserem Dafürhalten wären auch eine Ergänzung und Präzisierung der Grundprinzipien des Datenschutzes erforderlich. So sollte der Grundsatz der Verhältnismässigkeit durch das Prinzip der Datensparsamkeit vervollständigt werden. Es sollte nämlich vermieden werden, dass Personendaten in einer Form beschafft und bearbeitet werden, die die Person identifiziert, wenn dies für den Zweck der Bearbeitung nicht notwendig ist. Das Angebot anonymer oder unter Verwendung von Pseudonymen verfügbarer Dienste sollte gefördert werden, ebenso wie die Schaffung von Systemen für eine datenschutzkonforme Verwaltung der Identitäten (die Identitätsverwaltung sollte auf der Anwendung anonymer Verfahren oder von Pseudonymen beruhen, wobei die dezentralisiert aufbewahrten Identifikationsdaten einer möglichst weit reichenden Kontrolle durch die betroffene Person unterstellt würde). Die Transparenz der Bearbeitungen sollte ausserdem verstärkt werden, namentlich durch die Ausdehnung

der Informationspflicht für jegliche Datenbeschaffung, unabhängig von der Art der Daten, und durch die Erweiterung der Auskunftspflicht insbesondere bei der Erstellung von Persönlichkeitsprofilen.

Immer mehr Entscheidungen oder Massnahmen, die Personen tangieren, sind heute das Ergebnis automatisierter Verfahren, bei denen der Einfluss durch den Menschen relativ begrenzt ist. Wie sämtliche europäische Gesetzgebungen sollte auch das DSG durch Bestimmungen über den Einsatz automatisierter Entscheidungen ergänzt werden.

Die Komplexität der Datenbearbeitungen, ihr undurchsichtiges Umfeld, namentlich bei Operationen im Internet, die Streuung der Informationen durch mobile Datenbearbeitung (Cloud Computing) oder die Vielzahl der Akteure, die Zugriff auf die Informationen haben, schwächt die Position der betroffenen Personen, ihre Möglichkeit, ihre Rechte geltend zu machen, und die Effektivität des Datenschutzes. Es drängen sich daher Fragen nach den Mitteln auf, mit denen das Vertrauen der Personen in Systeme, welche sie betreffende Daten bearbeiten, gestärkt werden kann. So halten wir es für notwendig, die Verantwortlichkeit derer zu verstärken, die Personendaten bearbeiten oder die Bearbeitungssysteme und Produkte entwickeln. Die Beachtung der Datenschutzprinzipien bei der Organisation (namentlich Risikobeurteilung, Prüfung der Auswirkungen auf die Privatsphäre, Definition der Bearbeitungsabläufe, Datenschutz-Audit, verbindliches Datenschutzkonzept, Öffentlichkeit der Politik betreffend die Privatsphäre und interne Verfahren für die Behandlung von Beschwerden) und bei der Entwicklung von Informationssystemen (standardmässiger Datenschutz, «privacy by default») sollten verbindlich vorgeschrieben werden, um die Beschaffung und die Bearbeitung von überflüssigen Daten zu vermeiden und den Betroffenen die Möglichkeit einer besseren Kontrolle über ihre Personendaten zu bieten. Neu könnten Datenbearbeiter dazu verpflichtet werden, Lücken in der Datensicherheit zu melden, einen Vertreter in der Schweiz zu bestimmen, der für die Anforderungen des Datenschutzes verantwortlich ist, wenn Bearbeitungen hier erfolgen, oder auch einen Datenschutzberater einzusetzen.

Um die Effektivität des Gesetzes zu verbessern und die Kontrollmöglichkeiten zu verstärken, befürworten wir die Einführung einer vorgängigen Kontrolle von risikobehafteten Bearbeitungen (erhebliche Gefährdung des Rechts auf Datenschutz) in Form einer Vorausmeldung an den EDÖB und eine vermehrte Anwendung der Zertifizierung. Die Möglichkeit einer der behördlichen Genehmigung unterstellten Form der Selbstregulierung (zwingende sektorale Normen) wäre ebenfalls zu erwägen. Parallel dazu könnten die Kompetenzen des EDÖB erweitert und seine Ermittlungsbefugnisse verstärkt werden (namentlich Recht auf Beschlagnahme, Recht auf Einsichtnahme in die Daten, Recht, Geldstrafen zu verhängen). Die Wahrnehmung der Rechte der betroffenen Personen sollte ebenfalls verbessert werden, indem (beispielsweise durch unentgeltliche

Verfahren) der Zugang zur Justiz erleichtert oder ein Verbandsbeschwerderecht eingeführt wird, oder indem andere Mechanismen für die Beilegung von Streitigkeiten, wie etwa Schlichtungsverfahren, geprüft werden.

Eine der grossen Herausforderungen des Internet und der virtuellen Welt liegt in der Verwaltung und der Kontrolle der Daten. Einmal im Netz, bleiben sie u. U. ewig erhalten, und können Gegenstand einer Vielzahl von Bearbeitungen in unterschiedlichen Kontexten werden. Alle Handlungen des Users können ungeachtet seines Aufenthaltsorts registriert und nachverfolgt werden: die rasante Entwicklung der Smartphones verstärkt dieses Phänomen zusätzlich. Man müsste sich überlegen, wie in der virtuellen Welt der realen vergleichbare Rechte garantiert werden können, indem insbesondere das Recht auf Vergessen in den Netzwerken bekräftigt wird und die Mittel zu dessen Gewährleistung bereitgestellt werden (Verfallsfrist der Daten, Desindexierungspflicht, Regelung der Geolokalisierung, das Recht zu surfen, ohne beobachtet und profiliert zu werden, das Recht, sich der Veröffentlichung oder Indexierung von Daten im Internet zu widersetzen usw.).

Auch andere Elemente könnten mit Blick auf eine Modernisierung des Datenschutzrechts in Betracht gezogen werden, wie etwa ein verstärkter Datenschutz für Jugendliche, die Einführung der Einwilligung zu Kundenakquisition und Werbung im Netz, eine Kausalhaftung aufgrund der Bearbeitung, die Ausübung des Auskunftsrechts und des Rechts auf Berichtigung von Online-Inhalten.

Schliesslich würde das Gesetz besser lesbar und leichter zugänglich, wenn die allgemeinen und sektorspezifischen Bestimmungen über den Datenschutz und das Öffentlichkeitsprinzip in einem einzigen Text zusammengeführt würden (Gesetz über den Datenschutz und den Zugang zu amtlichen Dokumenten).

3.2 Projekt für die Migration des Geschäftsverwaltungssystems

Wir planen die Migration auf eines der standardisierten Geschäftverwaltungssysteme (GEVER). Zu diesem Zweck konzentrieren wir uns insbesondere auf die damit verbundenen organisatorischen, technischen und finanziellen Anforderungen.

Wie alle Bundesämter arbeiten wir an der Einführung eines neuen GEVER-Systems an Stelle unseres bisherigen Geschäftsverwaltungssystems (EDÖB-Office), das seit über zehn Jahren die Vertraulichkeit unserer Dokumente dank einer integralen Verschlüsselung besonders schützenswerter und vertraulicher Inhalte gewährleistet.

Eine solche Migration erfordert eine intensive organisatorische, technische und finanzielle Planung. So haben wir unseren Aktenablageplan völlig neu definiert (vom Schweizerischen Bundesarchiv noch zu genehmigen) und unsere organisatorischen Arbeitsvorschriften aktualisiert. Parallel dazu haben wir uns die beiden Standard-Produkte vorführen lassen und insbesondere ihre Eignung zur Gewährleistung einer hohen Datenvertraulichkeit untersucht. Daraus hat sich klar ergeben, dass keines der verfügbaren Produkte eine vergleichbare Vertraulichkeit bietet, wie wir sie seit über einem Jahrzehnt kennen; aus diesem Grund haben wir unsere Entscheidung aufgeschoben. Zusammen mit budgetären Gründen hat dies zu einer leichten Verzögerung bei der Planung der Schulung der Nutzer vor der eigentlichen GEVER-Migration geführt.

In diesem Kontext richteten sich unsere Bemühungen daher auf die Definition der minimalen technischen Anforderungen, denen ein GEVER-System im Bereich des Datenschutzes und der Öffentlichkeit der Verwaltung genügen muss (siehe auch Ziff. 1.2.11 des vorliegenden Tätigkeitsberichts).

3.3 5. Europäischer Datenschutztag – Kampagne für Kinder

Die Sensibilisierung von Kindern und Jugendlichen bildete auch in diesem Jahr unseren Ausbildungsschwerpunkt. In diesem Zusammenhang haben wir gemeinsam mit dem Rat für Persönlichkeitsschutz die multimediale Kampagne «NetLa – meine Daten gehören mir!» lanciert. Sie bringt Kindern von 5 bis 14 Jahren die Bedeutung der Persönlichkeit und des Persönlichkeitsschutzes näher. Die Kampagne wurde anlässlich des 5. Europäischen Datenschutztages der Öffentlichkeit präsentiert.

Heutzutage nutzen Kinder das Internet häufig schon im Vorschulalter, ohne sich der damit verbundenen Risiken bewusst zu sein. Sie geben bereitwillig Informationen preis, melden sich bei verschiedenen Communities an und veröffentlichen z. B. eigene Fotos. NetLa will Kinder und Jugendliche für einen verantwortungsvollen Umgang mit den eigenen Daten im Internet sensibilisieren.

Ausgangspunkt der Kampagne, die am 28. Januar 2011, dem 5. Europäischen Datenschutztag, im Rahmen einer Medienkonferenz lanciert wurde, ist die Website www.netla.ch, die Comics und Spiele für drei verschiedene Altersgruppen (Vorschule, 7-10 Jahre und 11-14 Jahre) bereithält. Eltern wiederum erfahren in der Rubrik «Tipps», welche Risiken bei der Nutzung der digitalen Medien für ihre Kinder bestehen und was sie für ihren Schutz tun können. Für den Unterricht bietet NetLa ein Lehrmittel, mit dem das Thema Persönlichkeits- und Datenschutz behandelt werden kann.

3.4 Datenschutzlehrmittel für Jugendliche

Um Jugendliche für den Umgang mit ihren persönlichen Daten zu sensibilisieren, haben wir ein Lehrmittel erstellt, das Lehrerinnen und Lehrer seit Juli 2010 im Schulunterricht einsetzen können. Besonderes Augenmerk richteten wir auf die Risiken bei der Nutzung digitaler Medien.

Junge Menschen wachsen mit den Geräten und Anwendungen der Informations- und Kommunikationstechnologien auf und nutzen sie spielerisch und mit grosser Selbstverständlichkeit. So chatten sie mit Internetbekanntschaften, stellen Fotos von sich und ihren Freunden in ihre sozialen Netzwerkprofile oder registrieren sich mit ihren persönlichen Angaben für Onlinespiele. Auch Konflikte werden gerne im Internet ausgetragen, wobei Beleidigungen, Anschuldigungen und Verunglimpfungen, anders als auf dem Pausenplatz, einem weltweiten Publikum zugänglich sind.

Dieser selbstverständliche Umgang mit Mobiltelefon und Computer birgt Gefahren: Sind persönliche Angaben einmal im Internet, können theoretisch Millionen von Menschen darauf zugreifen und sie zu Zwecken verwenden, die die betroffenen Personen in ihrer Persönlichkeit verletzen (z.B. Belästigungen, Diffamierungen, Identitätsdiebstahl, Stalking oder Pädophilie). Mit unserem gemeinsam mit der Fachagentur Kik erstellten Lehrmittel für Jugendliche zwischen 15 und 18 Jahren erhalten Lehrer eine Grundlage, um den Daten- und Persönlichkeitsschutz im Unterricht zu behandeln. Es enthält zehn voneinander unabhängige Lektionen, in denen sich die Schülerinnen und Schüler aktiv mit ihrem Verhältnis zur Privatsphäre, zu ihren Daten und den Risiken der digitalen Medien auseinandersetzen. Die Tücken sozialer Netzwerke wie Facebook und myspace kommen ebenso zur Sprache wie die Wichtigkeit sicherer Passwörter oder die Datenspuren, die wir beim Surfen unbewusst hinterlassen, und was sie über uns verraten.

Das in den Sprachen Deutsch, Französisch und Italienisch verfasste Lehrmittel steht allen Interessierten auf unserer Webseite www.derbeauftragte.ch unter Themen – Datenschutz – Internet – Kinder und Jugendliche kostenlos zur Verfügung.

3.5 Publikationen des EDÖB im laufenden Geschäftsjahr

Informationen zu unseren Tätigkeiten in den Bereichen Datenschutz und Öffentlichkeitsprinzip publizieren wir auf unserer Webseite. Zu den neu aufgeschalteten Inhalten zählen die Erläuterungen zum digitalen Stromzähler (Smart Meter), eine Übersicht über die möglichen Konstellationen bei der Auslagerung von Datenbearbeitungen ins Ausland, und eine Comic-Broschüre, welche die mit den digitalen Medien verbundenen Risiken in Erinnerung ruft.

Mit dem neuen Stromversorgungsgesetz wird der Elektrizitätsmarkt seit 1.1.2008 schrittweise dereguliert. Mit dieser Öffnung verbunden ist die Trennung von Netz und Energie. Zur Planung der Energiebereitstellung und des Angebots von kostengünstigen Tarifen benötigen die Energielieferanten genauere Informationen zum Stromverbrauch, welche digitale Energiezähler, sogenannte «Smart Meter», liefern sollen. Unsere Erläuterungen dazu beleuchten die Risiken der digitalen Verbrauchsmessung für die Privatsphäre der Konsumenten und nennen die Massnahmen, die für einen datenschutzkonformen Einsatz solcher Stromzähler notwendig sind (siehe auch Ziff. 1.8.1 des vorliegenden Tätigkeitsberichts). Sie finden diese Informationen auf unserer Webseite www.derbeauftragte.ch unter Themen – Datenschutz – Sonstige Themen.

Zum Thema Outsourcing haben wir Erläuterungen verfasst, welche die möglichen Konstellationen bei der Auslagerung von Datenbearbeitungen ins Ausland unter die Lupe nehmen und die jeweiligen rechtlichen Anforderungen aufführen. Nach Datenschutzgesetz muss der Auftraggeber dabei mit dem Auftragnehmer einen Vertrag abschliessen, der die Art und Weise der Datenbearbeitung und -bekanntgabe durch letzteren regelt. Den entsprechenden Mustervertrag haben wir so überarbeitet, dass er der im Februar 2010 durch die Europäische Kommission beschlossenen Änderung der einschlägigen Standardvertragsklauseln Rechnung trägt. Beide Dokumente befinden sich unter Themen – Datenschutz – Übermittlungen ins Ausland (siehe auch Ziff. 1.8.2 des vorliegenden Tätigkeitsberichts).

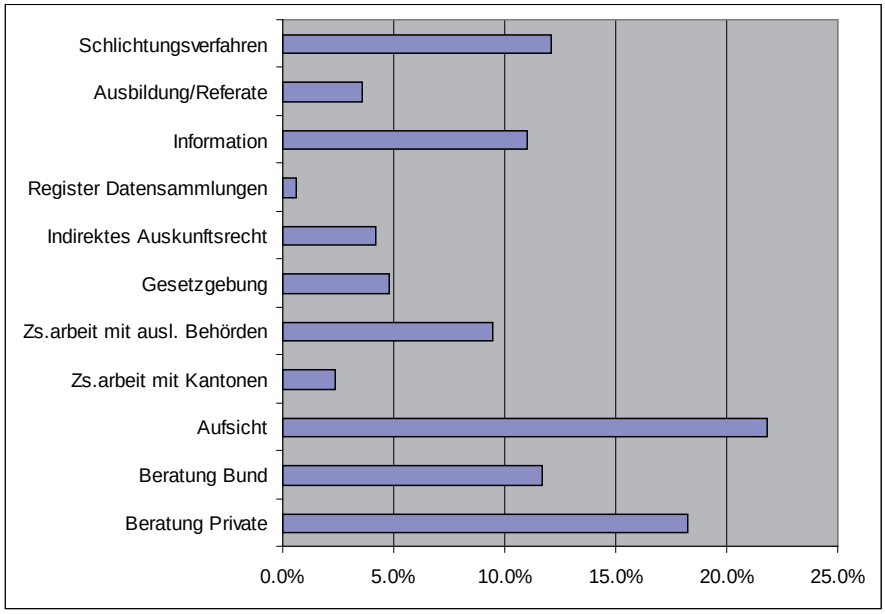
Um die Sicherheit und das Vertrauen der Bevölkerung im Umgang mit den Informations- und Kommunikationstechnologien (IKT) zu stärken, haben Stellen aus Bund und Kantonen, darunter auch der EDÖB, die Broschüre «Geschichten aus dem Internet, die man selber nicht erleben möchte» publiziert. Sie enthält Comics, die gefährliche Situationen im Web aufzeigen und Tipps zu ihrer Vermeidung geben, so zum Beispiel, dass es sich lohnt, den Zugang zum eigenen Computer, zum Wireless Network und zu persönlichen Anwendungen angemessen zu schützen. Oder dass unbedarft ins Netz gestellte Bilder und Mitteilungen unangenehme Folgen haben können, etwa im Rahmen einer Stellenbewerbung. Im Anschluss an die einzelnen Geschichten befinden sich Links zu

weiterführenden Informationen der zuständigen Fachstellen. Die Broschüre kann in allen vier Landessprachen sowie in Englisch unter www.derbeauftragte.ch, Themen – Datenschutz – Internet oder auf www.geschichtenausdeminternet.ch in Papierform kostenlos bezogen werden.

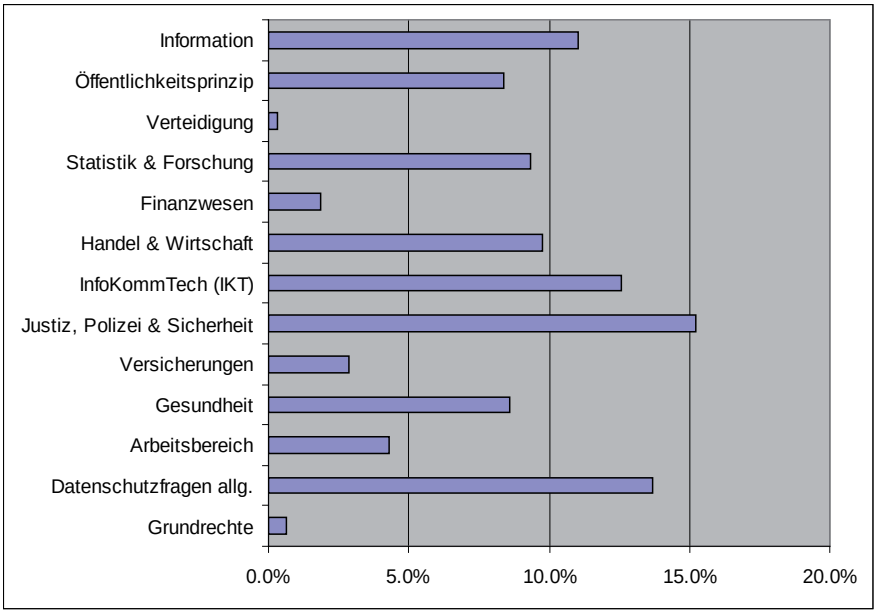
Ebenfalls haben wir ein Datenschutz-Lehrmittel für Jugendliche zwischen 15 und 19 Jahren verfasst, mit dem Lehrer und Lehrerinnen den Umgang mit persönlichen Daten im Unterricht thematisieren können. Besonderes Gewicht legen die Lektionen auf die digitalen Medien (siehe auch Ziff. 3.4 des vorliegenden Tätigkeitsberichts; das Lehrmittel befindet sich unter www.derbeauftragte.ch Themen – Datenschutz – Internet – Kinder und Jugendliche).

3.6 Statistik über die Tätigkeit des EDÖB vom 01. April 2010 bis 31. März 2011

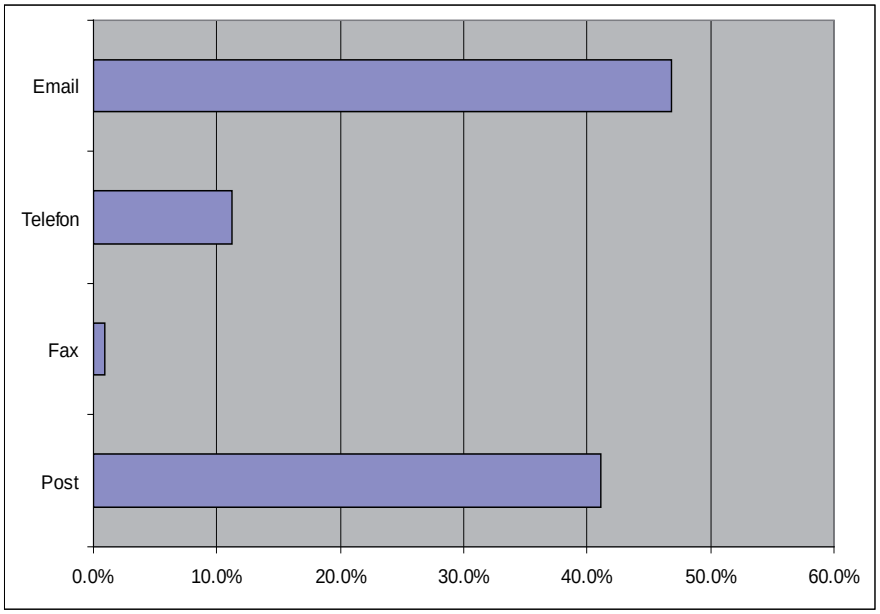
Aufwand nach Aufgabengebiet



Aufwand nach Sachgebiet



Herkunft der Anfragen



3.7 Statistik über die bei den Departementen eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2010 bis 31. Dezember 2010)

Dep.	Anzahl Gesuche	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
BK	15	11	2	2	0
EDA	39	18	6	15	0
EDI	54	18	16	17	3
EJPD	23	10	10	3	0
VBS	8	5	2	0	1
EFD	17	6	4	5	2
EVD	31	13	10	7	1
UVEK	52	25	12	14	1
Total 2010 (in %)	239 (100%)	106 (45%)	62 (26%)	63 (26%)	8 (3%)
Total 2009 (in %)	232 (100%)	124 (54%)	68 (29%)	40 (17%)	-
Total 2008 (in %)	221 (100%)	115 (52%)	71 (32%)	35 (16%)	-
Total 2007 (in %)	249 (100%)	147 (59%)	82 (33%)	20 (8%)	-
Total 2006 (in %)	95 (100%)	51 (54%)	41 (43%)	3 (3%)	-

Schweizerische Bundeskanzlei BK

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
BK	5	2	2	1	0
EDÖB	10	9	0	1	0
TOTAL	**15**	**11**	**2**	**2**	**0**

Eidg. Departement für auswärtige Angelegenheiten EDA

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
EDA	39	18	6	15	0
TOTAL	**39**	**18**	**6**	**15**	**0**

Eidg. Departement des Innern EDI

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS EDI	4	1	2	1	0
EBG	0	0	0	0	0
BAK	3	0	3	0	0
BAR	2	2	0	0	0
METEO CH	0	0	0	0	0
BAG	32	9	6	14	3
BFS	1	1	0	0	0
BSV	7	2	3	2	0
SBF	0	0	0	0	0
ETH Rat	1	0	1	0	0
SWISS MEDIC	3	2	1	0	0
SNF	1	1	0	0	0
SUVA	0	0	0	0	0
TOTAL	**54**	**18**	**16**	**17**	**3**

Eidg. Justiz- und Polizeidepartement EJPD

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS EJPD	0	0	0	0	0
BJ	3	1	2	0	0
FEDPOL	3	2	1	0	0
METAS	0	0	0	0	0
BFM	8	4	3	1	0
BA	3	0	3	0	0
SIR	0	0	0	0	0
IGE	2	2	0	0	0
ESBK	3	1	0	2	0
ESchK	1	0	1	0	0
RAB	0	0	0	0	0
ISC	0	0	0	0	0
NKVF	0	0	0	0	0
TOTAL	**23**	**10**	**10**	**3**	**0**

Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS VBS	7	5	1	0	1
Verteidig./ Armee	1	0	1	0	0
armasuisse	0	0	0	0	0
BABS	0	0	0	0	0
BASPO	0	0	0	0	0
TOTAL	**8**	**5**	**2**	**0**	**1**

Eidg. Finanzdepartement EFD

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS	2	1	0	1	0
EFV	1	1	0	0	0
EPA	1	0	1	0	0
ESTV	5	2	2	1	0
EZV	0	0	0	0	0
EAV/RFA	0	0	0	0	0
BBL	1	0	0	1	0
BIT	1	0	0	1	0
EFK	6	2	1	1	2
SIF	0	0	0	0	0
PUBLICA	0	0	0	0	0
ZAS	0	0	0	0	0
TOTAL	**17**	**6**	**4**	**5**	**2**

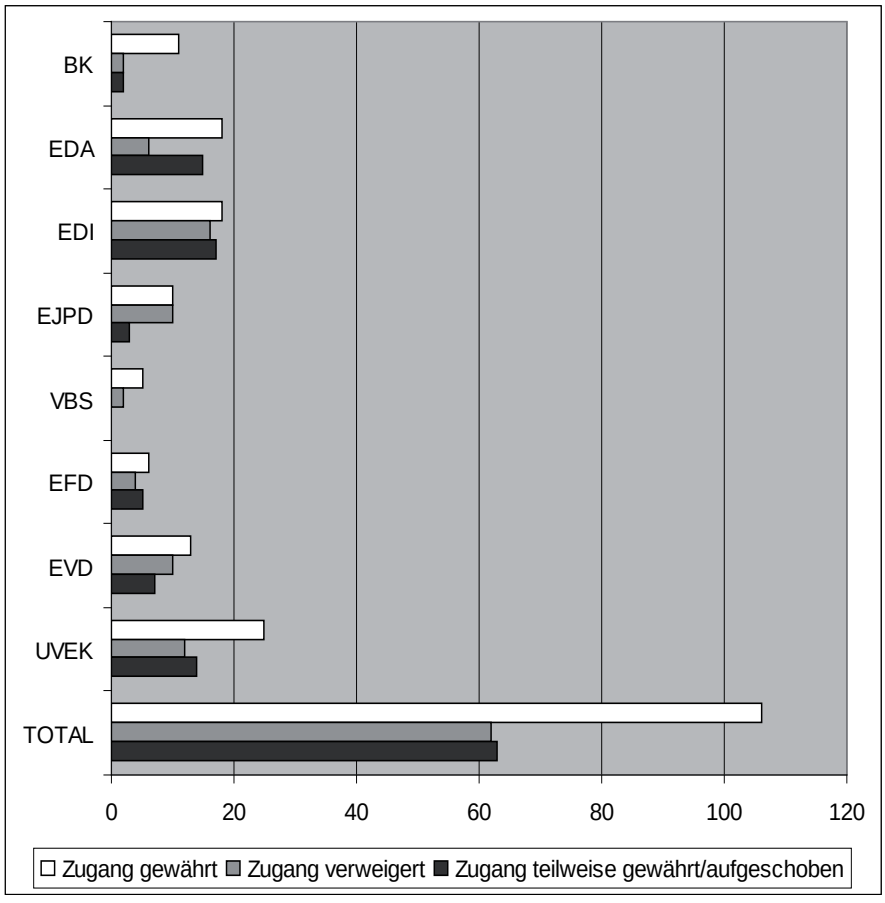
Eidg. Volkswirtschaftsdepartement EVD

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS	1	1	0	0	0
SECO	7	2	2	2	1
BBT	2	2	0	0	0
BLW	14	4	5	5	0
BVET	3	2	1	0	0
BWL	0	0	0	0	0
BWO	0	0	0	0	0
PUE	1	0	1	0	0
WEKO	2	1	1	0	0
ZIVI	0	0	0	0	0
BFK	1	1	0	0	0
TOTAL	**31**	**13**	**10**	**7**	**1**

Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
GS	0	0	0	0	0
BAV	5	3	1	0	1
BAZL	10	2	6	2	0
BFE	4	0	1	3	0
ASTRA	3	3	0	0	0
BAKOM	6	2	1	3	0
BAFU	9	4	2	3	0
ARE	1	0	1	0	0
COMCOM	1	1	0	0	0
ENSI	6	4	0	2	0
PostReg	1	0	0	1	0
UBI	6	6	0	0	0
TOTAL	**52**	**25**	**12**	**14**	**1**

Behandlung der Zugangsgesuche



3.8 Statistik über die bei den Parlamentsdiensten eingereichten Zugangsgesuche nach Art. 6 des Öffentlichkeitsgesetzes (Zeitraum: 1. Januar 2010 bis 31. Dezember 2010)

Parlamentsdienste PD

Betroffener Fachbereich	Anzahl	Zugang vollständig gewährt	Zugang vollständig verweigert	Zugang teilweise gewährt/auf-geschoben	hängig
PD	0	0	0	0	0
TOTAL	**0**	**0**	**0**	**0**	**0**

3.9 Anzahl Schlichtungsgesuche nach Kategorien der Antragsteller (Zeitraum: 1. Januar 2010 bis 31. Dezember 2010)

Kategorie Antragsteller	2010
Medien	17
Privatpersonen (bzw. keine genaue Zuordnung möglich)	5
Interessenvertreter (Verbände, Organisationen, Vereine usw.)	6
Unternehmen	1
Rechtsanwälte	3
Universitäten	0
Total	**32**

3.10 Das Sekretariat des EDÖB

Eidgenössischer Datenschutz-und Öffentlichkeitsbeauftragter:

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

Sekretariat:

Leiter:	Walter Jean-Philippe, Dr. iur.
Stellvertreter:	Buntschu Marc, lic. iur.
Einheit 1:	10 Personen
Einheit 2:	12 Personen
Einheit 3:	2 Personen
Kanzlei:	3 Personen

4. Anhänge

4.1 Datenschutz

4.1.1 Erläuterungen zum Einsatz von digitalen Stromzählern

Mit dem neuen Stromversorgungsgesetz wird der Elektrizitätsmarkt seit 1.1.2008 schrittweise dereguliert. Zusammen mit den verschiedenen alternativen Energieträgern macht das eine neue Verbrauchserfassung notwendig. Digitale Zähler, so genannte «Smart Meter», können sehr viele Daten speichern, was aus Sicht des Datenschutzes Risiken für die Privatsphäre birgt.

Diese Erläuterungen zeigen die wesentlichen Datenschutzrisiken beim Einsatz von elektronischen Energiezählern, auch «Smart Meter» genannt, auf und geben Empfehlungen aus der Sicht des Datenschutzes.

Liberalisierung des Strommarktes und erneuerbare Energien

Am 1. Januar 2008 trat das Stromversorgungsgesetz in Kraft. Es legt fest, dass der staatlich regulierte Markt etappenweise geöffnet wird. In einem ersten Schritt konnten Grossverbraucher mit einem jährlichen Stromverbrauch von über 100 Megawattstunden in den freien Markt eintreten. Rund 50'000 Unternehmen haben seit 2009 die Möglichkeit, ihren Stromlieferanten frei zu wählen. Dies bedeutet nicht zuletzt eine grosse Umstellung für die rund 900 Elektrizitätsversorgungsunternehmen in der Schweiz. In einem weiteren Schritt sollen ab 2014 auch kleine Firmen und Haushalte den Zutritt zum freien Markt erhalten. Somit können die Stromkunden in der Schweiz zukünftig frei entscheiden, woher sie ihren Strom beziehen möchten. Allerdings untersteht diese zweite Öffnungsetappe, wie bereits die erste, auch dem fakultativen Referendum.

Mit dieser Öffnung verbunden ist die Trennung von Netz und Energie. Das bedeutet, dass der Stromkunde in Zukunft einen Netzbetreiber und einen Stromanbieter hat; ersteren kann er nicht wählen, letzteren kann er selber bestimmen.

Weiter schafft der wachsende Anteil von Strom aus alternativen Energieträgern (Sonnen- und Windenergie) im Stromnetz einen erhöhten Steuerungsbedarf bezüglich Einspeisung und Verbrauch von Energie. Im Gegensatz zur Stromgewinnung aus Sonnen- und Windenergie lässt sich die Stromproduktion mit herkömmlichen Kraftwerken (Kernenergie, Kohle, Öl, Gas) relativ einfach steuern. Der Ausgleich der Lastschwankungen erfolgt durch die Regulierung der Leistung herkömmlicher Kraftwerke, durch den Einsatz von Wasserkraftwerken (Pumpspeicherkraftwerke) sowie durch den Stromhandel.

Zur Planung der Energiebereitstellung und des Angebots von kostengünstigen Tarifen bedarf es einer genauen Verbrauchsprognose, da kurzfristig auftretende Über- und Unterkapazitäten für die Stromlieferanten teuer sind. Dazu benötigen die Energielieferanten detaillierte Informationen über den Energieverbrauch der Haushalte. Im Interesse einer gleichmässigeren und effizienteren Auslastung des Stromnetzes ist in Zukunft sogar denkbar, leistungsstarke Haushaltsgeräte abhängig von der Netzauslastung zu steuern. So könnten bspw. die Kühlintervalle von Gefrier- und Kühlschränken oder das Aufladen von Energiespeichern in Fahrzeugen auf Perioden mit geringer Netzauslastung verschoben werden.

Bisherige Energieverbrauchserfassung und technische Anforderungen an neue Energiezähler

Bislang wurde der Stromverbrauch mit elektromechanischen Stromzählern gemessen, welche in Eintarif- und Doppeltarifzähler unterschieden werden. Der Eintarifzähler hat ein einziges Zählwerk und summiert den gesamten verbrauchten Strom auf. Liefert das Elektrizitätswerk Strom zu Hoch- und Niedertarifen, werden Doppeltarifzähler verwendet, welche den Verbrauch im Hochtarif (vorwiegend tagsüber) und im Niedertarif separat erfassen. Die Auslesung erfolgt halbjährlich oder jährlich direkt vor Ort.

Mit der Trennung von Netzbetreiber und Energielieferant müssen die Energiezähler individuell umgeschaltet werden können, da die verschiedenen Lieferanten ihre Tarife nach Angebot und Nachfrage ausrichten. Dazu werden digitale Zähler benötigt, welche den Energieverbrauch in verschiedenen Intervallen erheben können. Weiter bieten die digitalen Energiezähler die Möglichkeit der Fernauslesung, d.h. zukünftig können Energiezähler zu jedem beliebigen Zeitpunkt ausgelesen werden, ohne dass jemand physisch vor Ort sein muss. Dies ermöglicht eine flexible und kostengünstigere Auslesung.

Neben diesen Anforderungen wird den Kunden, je nach Netzbetreiber und Energielieferant, zusätzlich via Internet oder Wohnungsterminal Zugriff auf seine aktuellen und vergangenen Verbrauchsdaten angeboten. Dies soll den Energieverbrauch aufzeigen und zu dessen Reduktion führen.

Risiken aus der Sicht des Datenschutzes

Die intelligenten Energiezähler können den gesamten und den aktuellen Energieverbrauch sowie die Nutzungszeit anzeigen. Je nach Konfiguration des Gerätes werden die Lastprofile eines Haushaltes mehr oder weniger detailliert ausfallen. Ein solches Lastprofil entsteht durch die viertelstündliche Aufzeichnung des Energieverbrauches (35'000 Messpunkte pro Jahr) und wird bis zur Auslesung oder Überschreibung im Gerät gespeichert.

Aufgrund der technischen Ausgestaltung der digitalen Energiezähler ist es grundsätzlich möglich, neben den abrechnungsrelevanten Daten auch ein Energienutzungsprofil des Haushaltes bzw. des Unternehmens zu erheben. Diese detaillierteren Daten können für den Kunden wichtige Informationen über den Energieverbrauch und die damit zusammenhängenden Einsparungsmöglichkeiten enthalten, jedoch auch Informationen über Geschäftstätigkeiten, Produktionsprozesse, persönliche Aktivitäten, Tagesablauf, Krankheiten etc. Eine automatische Weitergabe dieser detaillierten Informationen an den Energielieferanten bzw. den Netzbetreiber ist jedoch aus der Sicht des Eidgenössischen Datenschutzbeauftragten nicht notwendig. Bedarfsprognosen können auch auf der Basis von anonymisierten Daten erstellt werden, die über mehrere Haushalte zusammengefasst werden.

Massnahmen

Grundsätzlich müssen bei der Sammlung von nicht abrechnungsrelevanten Nutzungsdaten, also bei der Erstellung des detaillierten Lastprofils eines Haushaltes, die Datenschutzgrundsätze beachtet werden. Das bedeutet, dass sowohl bei der Information der Betroffenen als auch bei der Ausgestaltung des Systems insbesondere auf Verhältnismässigkeit, Datensicherheit, Erkennbarkeit der Bearbeitung und des Zweckes geachtet wird. Im Zusammenhang mit Smart Grid bedeutet das folgendes:

Die Verhältnismässigkeit verlangt, dass nicht mehr Personendaten erhoben werden, als für den Bearbeitungszweck notwendig sind. Der Bearbeitungszweck muss bei der Beschaffung der Daten, bspw. in den Allgemeinen Geschäftsbedingungen, angegeben werden, darf jedoch nicht derart allgemein formuliert sein, dass im Prinzip jede Art der Bearbeitung darunter verstanden werden könnte. Es gilt also, von vornherein festzulegen, zu welchem Zweck die Daten verwendet werden, und eine entsprechende Selektion der dazu unbedingt notwendigen Daten vorzunehmen. Damit wird vermieden, dass alle möglichen Informationen auf Vorrat gesammelt werden.

Die Datensicherheit muss den ganzen Datenlebenszyklus von der Generierung im Smart Meter bis zur Löschung beim Energielieferanten respektive Netzbetreiber umfassen. Dabei sind nicht nur die ordentliche Erhebung der verbrauchten Energie und die Datenspeicherung gemeint, sondern auch die verschiedenen Übertragungsmöglichkeiten (Terminal in der Wohnung, Übertragung an den Netzbetreiber/Energielieferanten).

Bei einem Outsourcing der Datenbearbeitung an Dritte müssen überdies die allgemeinen Vorschriften gemäss Art. 10a DSG beachtet werden.

Empfehlungen des EDÖB

- Umfassende und verständliche Information der betroffenen Personen über die Datenbearbeitung (insb. Zweck der Bearbeitung, aber auch allfällige Weitergabe an Dritte), beispielsweise in den AGB.
- Zur Erstellung von Bedarfsprognosen Erhebung von über mehrere Haushalte zusammengefassten oder anonymisierten Daten anstelle von detaillierten Lastprofilen, die den einzelnen Haushalten zugeordnet werden können.
- Kein Zugriff auf Echtzeitdaten durch den Netzbetreiber bzw. den Energielieferanten.
- Zugriffskontrolle und Protokollierung der Auslesung des Energieverbrauchs/ Lastprofils aus den Energiezählern.
- Zugriffskontrolle und Protokollierung im Falle der Speicherung von Lastprofilen bei Energielieferanten bzw. Netzbetreiber.
- Verschlüsselte Übertragung sowohl im Haus als auch an den Energielieferanten bzw. Netzbetreiber.
- Schutz vor Verlust, Diebstahl, unerlaubtem Zugriff, Bekanntgabe, Verwendung oder Modifizierung der Daten.
- Zustimmung der Betroffenen zur Weitergabe oder Auswertung von haushaltsbezogenen Lastprofilen.

Weitere Informationen

Smart Meter und Smart Grid – Intelligente Energiemessung, ULD (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)

https://www.datenschutzzentrum.de/smartmeter/

The Smart Grid and Privacy, Electronic Privacy Information Center

http://epic.org/privacy/smartgrid/smartgrid.html

4.1.2 Empfehlung betreffend die «Verwendung biometrischer Daten für das Reservationssystem des Tennisclub XX»

Verwendung biometrischer Daten

für das Reservationssystem

des Tennisclub XX

Schlussbericht

vom 13. Septembre 2010

der Kontrolle
des Eidgenössischen Datenschutz- und
Öffentlichkeitsbeauftragten (EDÖB)
nach Art. 29 des

Bundesgesetzes über den Datenschutz (DSG)

1. Ausgangslage

Im Sommer 2009 hat der TC XX ein neues System für die Reservation der Tennisplätze eingeführt. Neu werden die Fingerabdrücke der Mitglieder erfasst und in Form von Templates gespeichert. Jede Reservation eines Tennisplatzes muss nun mit der Mitgliedernummer und mit Einsatz des Fingerabdruckes bestätigt werden, damit der Platz bespielt werden darf.

Das neue Reservationssystem soll sicherstellen, dass nur Berechtigte die Plätze des TC XX nutzen.

2. Umfang der Kontrolle

Die Datenschutzkontrolle bezog sich auf die Datenabläufe im Zusammenhang mit dem neuen Reservationssystem. Der Schwerpunkt lag dabei bei der Bearbeitung der erhobenen biometrischen Daten sowie der im Zusammenhang mit der Online-Reservation veröffentlichten Personendaten.

3. Chronologie der Kontrolle

Anfang Oktober 2009	Der EDÖB erfährt aufgrund von Anfragen von Clubmitgliedern des TC XX vom biometrischen Reservationssystem des Clubs. Nachdem sich innerhalb des Clubs Widerstand formiert hat und mehr als 1000 Personen von diesem Reservationssystem betroffen sind, beschliesst der EDÖB, eine Sachverhaltsabklärung durchzuführen.
15.10.2009	Der EDÖB informiert den TC XX schriftlich über die geplante Datenschutzkontrolle betreffend das Reservationssystem sowie über die geplante Sachverhaltsabklärung vor Ort. Zusätzlich bittet der EDÖB um Dokumentation über das neue System und um Beantwortung eines beigelegten Fragebogens.
30.10.2009	Der TC XX beantwortet den Fragekatalog des EDÖB und schickt Unterlagen.
03.12.2009	Der EDÖB stellt Rückfragen.
14.12.2009	Der TC XX beantwortet die Rückfragen und schickt weitere Unterlagen.
14.01.2010	Der EDÖB macht Terminvorschläge und bittet und Nennung der anwesenden Personen.
27.01.2010	Der Termin wird auf den 11.02.2010 festgelegt.
11.02.2010	Sachverhaltsabklärung mit den verantwortlichen Personen.
2. Hälfte Februar 2010	Mailverkehr zwischen dem EDÖB und dem TC XX betreffend Ergänzungsfragen
05.03.2010	Der EDÖB schickt dem TC XX ein Factsheet mit der Bitte um materielle Bereinigung des Textes und Beantwortung der Ergänzungsfragen.
22.03.2010	Der TC XX bestätigt schriftlich den Inhalt des Factsheets
April 2010	Analyse und Auswertung aller Unterlagen und Sachverhalte sowie Ausarbeitung des Schlussberichtes durch den EDÖB.
13. September 2010	Verabschiedung des Schlussberichtes durch den EDÖB.

4. Sachverhaltsabklärung vom 11. Februar 2010

4.1 Anwesende Personen :

- Präsident des TC XX
- Rechtsvertreter des TC XX
- Systemverantwortlicher des TC XX
- 2 Vertreter des Systemlieferanten
- 2 Mitarbeiter des EDÖB

4.2 Enrolement:

Das Enrolement wird durch das Mitglied selbständig durchgeführt. Die Personalien sowie die Mitgliedernummer bestehen bereits auf der Mitgliederdatenbank des Clubs. Das Mitglied gibt seine Mitgliedernummer in das System ein und liest seinen Fingerabdruck über einen Scanner ein. Aus dem Scan wird ein Template mit 12 Minutien extrahiert und unter der Mitgliedernummer auf dem Server «Biometrie» im vom Lesegerät generierten Format (ASN.1 DER) gespeichert. Wir gehen davon aus, dass die Templates nur codiert und nicht verschlüsselt gespeichert werden. Der EDÖB verfügen jedenfalls trotz wiederholtem Nachfragen über keinerlei Informationen, welche eine allfällige Verschlüsselung belegen würden (Algorithmus, Schlüssel, Länge des Schlüssels).

Das Reservationssystem funktioniert ohne Karten, so dass sämtliche Daten zentral gespeichert werden. Die Templates befinden sich aber nicht auf demselben Rechner wie die übrigen Mitgliederdaten. Jene sind auf einem PC im Sekretariat (Mitgliederdatenbank) und auf einem Webserver (Reservationssystem) gespeichert. Der PC «Biometrie» ist dabei durch ein drahtloses Netzwerk (WLAN/WPA) mit dem Sekretariats-PC verbunden, welcher seinerseits via ADSL mit dem Internet verbunden ist. Es werden keine Rohdaten des Fingerabdrucks gespeichert. Gemäss Aussage des Herstellers des Lesegeräts können aus den gespeicherten Templates keine Rohdaten rekonstruiert werden.

4.3 Reservation eines Tennisplatzes

Bevor auf einem Platz gespielt werden darf, muss dieser zwingend reserviert werden. Dies kann entweder vor Ort oder via Internet geschehen. Diese Reservation muss anschliessend bis spätestens 10 Minuten nach Spielbeginn mittels Fingerabdruck bestätigt werden. Es müssen sämtliche Spieler, mit Ausnahme eingeladener Gäste, ihre Anwesenheit mittels Fingerabdruck bestätigen.

Hierzu gibt das Mitglied seine Mitgliedernummer ein. Es folgt die Aufforderung, seinen Finger auf den Scanner zu legen. Durch die Mitgliedernummer wird automatisch das dazugehörende Template (Referenzdatum) aufgerufen und mit dem Fingerabdruck des anwesenden Mitglieds verglichen. Es findet also kein 1:n-Verlgeich (Identifikation) mit der ganzen Datenbank statt, sondern ein 1:1 Vergleich (Verifikation) über die Mitgliedernummer. Ist die Verifikation aller für die Reservation eingeschriebenen Mitglieder gelungen, wird die Reservation bestätigt. Gelingt die Verifikation nicht oder wird die Reservation nicht (vollständig) bestätigt, wird die Reservation 10 Minuten nach Beginn der Reservationszeit gelöscht. Der Platz erscheint im System als «frei» und darf nicht benützt werden. Wird auf einem Platz ohne Reservation gespielt, können die Spieler vom Platz gewiesen werden.

Über die Reservationen werden im Reservationssystem (Webserver) Logfiles erstellt, und auch die Reservationsdaten selbst werden gespeichert. So ist es möglich, für ca. 1 Jahr rückwirkend die Reservationen und damit die Platznutzung der Mitglieder einzusehen.

4.4 Löschung der Daten

Es werden an drei verschiedenen Orten Personendaten der Mitglieder gespeichert: In der Mitgliederdatenbank (Sekretariats-PC), im Reservationssystem (Webserver) und in der Template-Datenbank (Biometrie). Gemäss Aussage der Informatiker können alle Daten grundsätzlich jederzeit gelöscht werden. Es seien zurzeit jedoch keine Speicherfristen geregelt, dies läge im Verantwortungsbereich des TC XX. Wenn ein Mitglied austritt, kann das Template einfach gelöscht werden. Im Reservationssystem werden die Daten alle 2 bis 3 Jahre durch die Informatiker gelöscht, Logfiles nach ca. 1 Jahr, um Platz zu schaffen. Der TC XX selbst führt keine regelmässigen Datenlöschungen durch.

Der EDÖB macht vor Ort darauf aufmerksam, dass der Grundsatz der Verhältnismässigkeit der Datenbearbeitung eine frühest mögliche Löschung von Daten verlange und regt an, dass der TC XX Regeln für eine sinnvolle Löschung der Daten einführen soll.

4.5 Aufklärungs- und Auskunftsrecht

Die Mitglieder wurden im Rahmen der entsprechenden Abstimmung der GV vorgängig über das geplante System informiert. Anlässlich der GV fand eine Diskussion statt, in welcher ebenfalls Informationen ausgetauscht wurden. Nachdem der Beschluss zur Einführung des Systems gefasst worden ist, wurden sämtliche Mitglieder per Post oder Mail sowie im Clubmagazin über das System informiert. Eine standardisierte Information von Neumitgliedern besteht nicht. Auf Anregung des EDÖB wird der Präsident die Information der Mitglieder verbessern.

Die Mitglieder können sich jederzeit an den Clubpräsidenten wenden und Einsicht in die Templatedatenbank nehmen. Auf Anregung des EDÖB wird der Präsident dieses Auskunftsrecht auch auf die Mitgliederdatenbank und das Reservationssystem ausdehnen.

4.6 Alternativen zur biometrischen Erfassung

Das System erlaubt es, dass die Reservation mit einem PIN anstelle des Fingerabdrucks bestätigt werden kann. Diejenigen Personen, welche das biometrische System nicht nutzen können oder wollen, können auf dieses System ausweichen. Diese Alternative wird zurzeit von ca. 10 Personen genutzt.

Auf Anregung des EDÖB hat der Präsident eingewilligt, die Mitglieder zukünftig transparent über diese Alternative zu informieren.

4.7 Vorteile des biometrischen Erfassungssystems

Die Anlage des TC XX besteht hauptsächlich aus den Tennisplätzen und dem Clubhaus mit Garderoben und Restaurant. Eine Reception oder dergleichen existiert nicht. Aus diesem Grund muss die Kontrolle, dass nur Berechtigte die Anlage nutzen, automatisiert erfolgen.

Bisher wurde dies mit einem Reservationssystem mit PIN gemacht. Das Problem hierbei war, dass die PINs teilweise weitergegeben und von mehreren Personen (Nichtmitglieder) benutzt wurden. Das System musste daher so abgeändert werden, dass eine eindeutige Verifizierung mit möglichst geringem Aufwand (die finanziellen Mittel des Clubs seien gemäss Aussage des Präsidenten gering) möglich ist. Die Verifizierung mittels Fingerabdruck bietet diese Möglichkeiten und wurde daher ausgewählt. Der Club hat seither einen deutlichen Mitgliederzuwachs erlebt, und trotzdem sind die Plätze weniger ausgebucht als früher. Dies legt den Schluss nahe, dass der Missbrauch des früheren Systems bedeutend war.

Man hat sich bewusst gegen ein System mit Karten entschieden. Die Karten können leicht vergessen oder verloren gehen, was einerseits die Missbrauchsgefahr wieder erhöht und andererseits dem Mitglied einen Zusatzaufwand gibt. Die Mitglieder begrüssen mit grosser Mehrheit die Lösung ohne Karte, weil diese viel bequemer sei («die Finger hat man immer mit dabei…»). Das System sei bei einer grossen Mehrheit der Mitglieder akzeptiert und man sei sehr zufrieden mit dieser Lösung.

4.8 Weiterleitung von Daten an aussenstehende Dritte

Es werden keine biometrischen Daten an Dritte weitergeleitet. Es findet auch kein Transfer solcher Daten an den Hersteller statt, das System ist nicht mit dem Hersteller verbunden.

Dagegen ist das Reservationssystem (ohne biometrische Daten) ohne Passwortschutz oder dergleichen auf der Website des Clubs abrufbar. Jeder Internetnutzer kann damit sehen, wer zu welcher Zeit welchen Platz reserviert hat. Dies ist auch rückwirkend für 2-3 Jahre möglich. Jedes Clubmitglied kann beim Einrichten seines Benutzerkontos zwar den Benutzernamen abändern und so ein Pseudonym anzeigen lassen. Die Default-Einstellung entspricht jedoch dem ersten Buchstaben des Vornamens, gefolgt von max. den ersten 20 Buchstaben des Nachnamens.

4.9 Serverraum und Server, Datensicherheit

Die Templates sind auf einem PC «Biometrie» gespeichert, welcher sich in einem Vorraum zum Clubhaus befindet. Der Raum ist mit einer normalen Türe mit einfachem Schloss gesichert. Zutritt zu diesem Raum haben der Clubpräsident, der Verwalter, der Informatiker sowie 2 bis 3 weitere Personen. Auf einem Tablar ausserhalb des Gebäudes befinden sich folgende zum PC «Biomentrie» gehörenden Peripherie-Geräte: Eine numerische Tastatur zur Eingabe der Mitgliedernummer, ein Fingerabdrucklesegerät und eine Maus, mit der auf dem Bildschirm navigiert werden kann.

Die Mitgliederdaten befinden sich auf einem PC im Clubsekretariat, welches sich im 1. Stock des Clubhauses, von aussen zugänglich über eine Galerie, befindet. Das Sekretariat ist ebenfalls mit einer normalen Tür mit einfachem Schloss gesichert und kann während der Öffnungszeiten des Sekretariats von Jedermann betreten werden. Ausserhalb der Öffnungszeiten haben der Präsident, der Verwalter, der Informatiker, 4 Vorstandsmitglieder sowie 4 Angestellte Zutritt zum Sekretariat. Der Zugang zum Sekretariats-PC ist mit einem Passwort gesichert. Hier muss beachtet werden, dass auch vom Sekretariats-PC aus via eine versteckte Partition auf dem PC «Biometrie» auf die Templates zugegriffen werden kann. Um die Sicherheit dieses Zugangs zu erhöhen, wurde dem EDÖB vorgeschlagen, hierfür ein separates Administratorenprofil zu erstellen.

Das Reservationssystem befindet sich auf einem Webserver. Der Zugang zu den Personendaten wird durch ein Passwort für den Administrator des Reservationssystems geschützt. Wir kennen die Vertragsbedingungen betreffend Datenschutz mit dem Serverbetreiber nicht.

Die beiden PCs sind mit dem Internet und untereinander via WIFI verbunden. Das WIFI wird zurzeit durch das Protokoll WPA geschützt (ab März 2010 durch das Protokoll WPA2) und kann gemäss Website auch von Mitgliedern für den Zugang zum Internet benutzt werden. Diese erhalten auf Anfrage das Zugangspasswort.

Die nicht biometrischen Personendaten der Mitglieder werden in Klartext gespeichert, während die Templates angeblich verschlüsselt gespeichert werden. Der EDÖB geht aber davon aus, dass es sich eher um eine Codierung (ASN.1 DER) als um eine Verschlüsselung handelt, insbesondere da er keinerlei Informationen betreffend die behauptete Verschlüsselung erhalten hat (Algorithmus, Schlüssel, Länge des Schlüssels).

4.10 Systemwartung

Die Systemwartung erfolgt durch die Informatiker des TC XX. Die Templates können aufgrund der Codierung/Verschlüsselung im Rahmen von Wartungsarbeiten nicht gelesen werden, die übrigen, unverschlüsselt gespeicherten Daten dagegen schon.

5. Datenschutzrechtliche Beurteilung

5.1 Biometrische Daten als Personendaten

5.1.1 Ausgangslage

Das Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1) findet dort Anwendung, wo mit Personendaten im Sinne des Art. 3 lit. a DSG operiert wird. Im vorliegenden Fall werden für die Reservation eines Tennisplatzes biometrische Daten bearbeitet (Templates von Fingerabdrücken).

5.1.2 Beurteilung aus Sicht des EDÖB

Biometrische Daten der Fingerabdrücke in Form von Templates (=Referenzdatum) machen eine Person durch Abgleich mit einem aktuell präsentierten Fingerabdruck bestimmbar. Somit können die biometrischen Daten der Verifizierung (resp. Identifizierung) einer Person dienen. Die Bestimmbarkeit ergibt sich nicht nur aus dieser Abgleichsmöglichkeit, sondern auch dadurch, dass eine Verbindung zwischen der Template-Datenbank und dem Sekretariats-PC mit den Mitgliederdaten besteht. Die biometrischen Daten in Form von Templates können in Verbindung mit diesen weiteren Daten klar einer Person zugeordnet werden und machen diese bestimmbar (Art. 3 lit. a DSG).

Im Falle des TC XX werden 12 Minutien, die aus einem Fingerabdruck entnommen werden, abgespeichert. Die Minutien-Daten werden mittels eines mathematischen Algorithmus codiert und komprimiert. Die Algorithmen für die Template-Extrahierung von biometrischen Rohdaten sind heutzutage weder standardisiert noch transparent,

weswegen es derzeit schwierig ist, die Sensibilität (Elemente über Gesundheit/Rasse) eines Templates formell abschliessend einschätzen zu können. Zudem machen biometrische Daten in Form von Rohdaten oder Templates eine Person identifizierbar resp. bestimmbar, und ihre Erhebung hinterlässt in der Regel – insbesondere bei der Erhebung von Fingerabdrücken – (Daten-) Spuren. Die Erhebung von Rohdaten oder Templates ist somit geeignet, ein Bewegungsprofil der betroffenen Person zu erstellen. Gestützt auf diese Tatsache besteht bei der Erhebung biometrischer Daten für die betroffene Person ein hohes Gefährdungspotenzial für ihre Persönlichkeitsrechte. Ferner ist festzuhalten, dass auch der Europarat und die Art. 29-Datenschutzgruppe der EU (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) aus gleichen Gründen die hohe Sensibilität biometrischer Daten anerkennt.

5.2 Zweck der Datenbearbeitung

5.2.1 Ausgangslage

Jede Bearbeitung von Personendaten stelle einen Eingriff in das Recht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101) dar. Daher bedarf die Bearbeitung einer besonderen Rechtfertigung. Praktikabilitätserwägungen oder allgemeine Kundenfreundlichkeit stellen grundsätzlich keine ausreichende Rechtfertigung für die Bearbeitung biometrischer Daten dar.

Gemäss Angaben des TC XX geht es beim Erfassen biometrischer Daten ausschliesslich darum, den Missbrauch der Tennisplätze durch Unberechtigte zu verhindern. Vor Einführung des biometrischen Reservationssystems wurden die Plätze mit einem PIN reserviert, was sich als missbrauchsanfällig erwiesen hat. Die Nummern wurden teilweise weitergeben und durch mehrere Personen (Nichtmitglieder) verwendet. Dies ist mit dem neuen, biometrischen System nicht mehr möglich. Der TC XX hat denn auch seit Einführung des neuen Systems einen deutlichen Mitgliederzuwachs erfahren, während die Plätze aber weniger frequentiert werden.

Auf den Einsatz von Kartensystemen wurde bewusst verzichtet, da hier die Gefahr besteht, dass die Karten verloren oder vergessen gehen und die Mitglieder ein kartenloses System aus Komfortgründen bevorzugen.

5.2.2 Beurteilung aus Sicht des EDÖB

Das neue Reservationssystem und die damit verbundene Erhebung biometrischer Daten verfolgt nachvollziehbare Zwecke. Für den EDÖB stellt sich jedoch ernsthaft die Frage, ob es nicht Alternativen zur Missbrauchsvermeidung gäbe, welche weniger stark in die Persönlichkeitsrechte der Betroffenen eingreifen würden (vgl. dazu auch die grundsätzlichen Bemerkungen zur Verhältnismässigkeit unter Ziff. 5.5).

5.3 Rechtmässigkeit der Datenbeschaffung / Einwilligung der Betroffenen

5.3.1 Ausgangslage

Biometrische Daten sind Personendaten im Sinne des Datenschutzgesetzes, für deren Bearbeitung ein Rechtfertigungsgrund (Art. 12 und 13 DSG) benötigt wird. Als Rechtfertigung der Datenbearbeitung kommt im vorliegenden Fall die Einwilligung der Betroffenen in Frage.

Gemäss Auskunft des TC XX wurde das geplante System an der Generalversammlung in grundsätzlicher Hinsicht besprochen. Bei der anschliessend durchgeführten Abstimmung har sich die Mehrheit der Mitglieder für die Einführung eines solchen Systems ausgesprochen. Das System wurde in der Folge eingeführt und auf der Website resp. auf dem «Borne» eine Gebrauchsanweisung aufgeschaltet, welche über das Reservationssystem Auskunft gibt. Gemäss Auskunft des TC XX werden Neumitglieder zudem vom Präsidenten mündlich über das Reservationssystem informiert.

Offenbar existieren keine schriftlichen Aufzeichnungen darüber, welche Informationen den Mitgliedern anlässlich der GV gegeben wurden. Es muss jedoch davon ausgegangen werden, dass die Informationen nur grundsätzlicher Natur waren und insbesondere nicht über die Bearbeitungsmodalitäten im Rahmen des biometrischen Reservationssystems (z.B. Speicherort, Speicherdauer, Zugriffsberechtigungen u.V.m.) Auskunft gaben.

Die Gebrauchsanweisung für das Reservationssystem äussert sich nur grob über die Bearbeitungsmodalitäten des Systems. Sie gibt hauptsächlich Auskunft über das Vorgehen beim Enrolement und bei der Reservation.

Die mündliche Auskunft durch den Präsidenten erfolgt jeweils individuell und ist nicht standardisiert. Es ist auch hier davon auszugehen, dass der Präsident nicht über die Bearbeitungsmodalitäten informiert.

Weiteres Informationsmaterial existiert zurzeit nicht, soll aber gemäss Auskunft des TC XX erstellt und an die Mitglieder abgegeben werden.

Diejenigen Personen, welche das biometrische Reservationssystem nicht benützten können oder wollen, können die Reservation, wie bis anhin, mit einem PIN vornehmen. Zurzeit machen ca. 10 Personen von dieser Möglichkeit Gebrauch. Die Mitglieder werden nicht vorgängig über diese Alternative informiert. Erst, wenn sich jemand weigert, seine biometrischen Daten zu erfassen, oder wenn sich herausstellt, dass das biometrische System nicht benutzt werden kann, wird auf die Alternative hingewiesen.

5.3.2 Beurteilung aus Sicht des EDÖB

Aus Sicht des EDÖB müssen für die Einwilligung der Betroffenen – gerade in so einem sensiblen Bereich wie bei der Bearbeitung von Fingerabdrücken – strenge Anforderungen an die Aufklärung der betroffenen Personen gestellt werden. Es ist daher zu fordern, dass die Mitglieder konkreter über die Bearbeitungsmodalitäten informiert werden, damit sie sich über die Tragweite ihrer Einwilligung im Klaren sind. Es sind den Betroffenen daher die Hauptpunkte der Datenbearbeitung mitzuteilen, wie z.B. wo und für wie lange die Daten gespeichert werden, was mit den Templates und den Transaktionsdaten geschieht, wer Zugriff auf die Daten hat und an wen sie, wenn überhaupt, weitergegeben werden. Dies sollte mittels standardisiertem Informationsblatt geschehen, welches sämtlichen bestehenden und neu eintretenden Mitgliedern abzugeben ist. Das Informationsblatt muss vom Vorstand des TC XX unterschrieben und mit einer Versionenkontrolle versehen werden. Zudem müssen die Mitglieder über die Alternative (vorliegend: Reservation mittels PIN) informiert werden, damit die Einwilligung freiwillig erfolgt und nicht unter der vermeintlichen Annahme, man habe keine Wahl.

Die Mitglieder verfügten im Zeitpunkt der GV-Abstimmung nicht über die notwendigen Kenntnisse der Sachlage, um eine rechtsgenügliche Einwilligung abzugeben. Zudem muss an dieser Stelle darauf hingewiesen werden, dass nur die Einwilligung jedes einzelnen Betroffenen die Verletzung der Persönlichkeitsrechte zu rechtfertigen vermag. Ein Mehrheitsbeschluss an einer GV erfüllt diese Voraussetzung nicht.

Auch im jetzigen Zeitpunkt muss davon ausgegangen werden, dass die Mitglieder nicht genügend über die Bearbeitungsmodalitäten informiert sind, um rechtsgültig in die Datenbearbeitung einzuwilligen. Erst, wenn die oben aufgeführten Voraussetzungen erfüllt sind und sich die Mitglieder in Kenntnis dieser Informationen für das biometrische Reservationssystem entscheiden, kann eine rechtsgültige Einwilligung geprüft werden.

5.4 Bearbeitung nach Treu und Glauben / Transparenz

5.4.1 Ausgangslage

Die Bearbeitung von Personendaten muss nach Treu und Glauben erfolgen (Art. 4 Abs. 1 DSG). Die bedeutet zum einen, dass die Datenbearbeitung für die betroffenen Personen transparent erfolgen muss. Zum anderen muss eine Datenbeschaffung und jede weitere Datenbearbeitung grundsätzlich für die Betroffenen erkennbar sein.

Wie bereits unter Ziffer 5.3 ausgeführt, wurden die Mitglieder anlässlich der GV, durch die Gebrauchsanweisung für das Reservationssystem sowie mündlich durch den Vereinspräsidenten über die Erhebung biometrischer Daten informiert. Ein standardisiertes Infoblatt besteht indessen nicht. Das Enrolement erfolgt durch das Mitglied selbst. Dieses muss also aktiv tätig werden, damit seine biometrischen Daten erfasst werden können (Abrollen des Fingers auf dem Sensor beim «Borne» beim Clubeingang). Ohne sein Zutun können keine biometrischen Daten erhoben werden.

5.4.2 Beurteilung aus Sicht des EDÖB

Da die biometrischen Daten nicht ohne Zutun der Betroffenen erhoben werden können, erfolgt die Datenbearbeitung für diese auf klar erkennbare Weise. Für eine möglichst transparente Datenbearbeitung sollte neben den zurzeit den Mitgliedern gegebenen Informationen noch ein standardisiertes Informationsblatt abgegeben werden, auf dem beschrieben wird, was mit den Personendaten geschieht. Es kann auf das unter Ziffer 5.3 Geschriebene verwiesen werden.

5.5 Verhältnismässigkeit der Datenbearbeitung

Die Bearbeitung von Personendaten hat sich am Grundsatz der Verhältnismässigkeit auszurichten (Art. 4 Abs. 2 DSG). Dies bedeutet, dass ein Datenbearbeiter nur diejenigen Daten bearbeiten darf, die er für einen bestimmten Zweck objektiv tatsächlich benötigt und die im Hinblick auf den Bearbeitungszweck und die Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis stehen.

5.5.1 Verhältnismässigkeit in inhaltlicher Hinsicht – Ausgangslage

Eine Datenbearbeitung ist dann verhältnismässig, wenn sie sich inhaltlich auf das absolut Notwendige beschränkt, um ein bestimmtes Ziel zu erreichen. Die inhaltliche Verhältnismässigkeit fordert einen möglichst schonenden Umgang mit Personendaten. Dies bedingt auch, dass keine für den verfolgten Zweck nicht benötigten Überschussinformationen anfallen. Ebenso ist es unzulässig, Personendaten auf Vorrat zu erheben, sofern der damit verfolgte Zweck dies nicht unabdingbar erfordert.

Mit der Einführung des neuen Reservationssystems werden aus den Fingerabdrücken der Mitglieder Templates generiert und diese zentral in einer Datenbank abgelegt. Rohdaten (d.h. das Originalbild des Fingerabdrucks) werden keine erhoben. Das System funktioniert ohne Karten. Eine zuvor über das Reservationssystem online oder auf dem «Borne» getätigte Platzreservation wird bestätigt, indem die Mitgliedernummer eingegeben und anschliessend der Finger auf das Lesegerät gehalten wird. Das aktuell erstellte Template wird nun mit dem durch die Mitgliedernummer ermittelten Referenzdatum verglichen. Stimmen die beiden Templates überein, wird die Reservation bestätigt und die Reservation bleibt für die nächsten zwei bis drei Jahre im Reservationssystem gespeichert und abrufbar. Stimmen die Templates nicht überein, wird die Reservation nicht bestätigt und 10 Minuten nach Beginn der Reservationszeit gelöscht.

Nebst den Templates werden im Sekretariats-PC weitere Daten der Mitglieder (Personalien, Spielerdaten etc.) und im Reservationssystem die Reservationsdaten gespeichert. Die Reservationsdaten sind ohne Passwortschutz durch sämtliche Internetnutzer über das Internet abrufbar. Hierbei werden der Benutzername (im Defaultzustand erster Buchstabe des Vornamens sowie max. die ersten 12 Buchstaben des Nachnamens) sowie die Reservationszeiten für die vergangenen zwei bis drei Jahre angezeigt. Um eine Reservation zu tätigen, muss sich das Mitglied mit seinem Benutzernamen und einem Passwort einloggen. Der angezeigte Name kann durch das Mitglied selbständig geändert werden.

5.5.2 Beurteilung der inhaltlichen Verhältnismässigkeit aus Sicht des EDÖB

5.5.2.1 Zentrale Speicherung biometrischer Daten

Der Einsatz biometrischer Verfahren im Privatbereich stellt je nach Ausgestaltung im konkreten Einzelfall einen mehr oder weniger intensiven Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Grundsätzlich sind daher vor dem Einsatz biometrischer Verfahren immer auch andere geeignete Massnahmen zu prüfen, welche weniger in die Grundrechte der Betroffenen eingreifen und mit denen der angestrebte Zweck ebenfalls erreicht werden kann. Des Weiteren muss schon bei der Auswahl und Ausgestaltung des biometrischen Verfahrens darauf geachtet werden, ein möglichst datensparsames System auszuwählen, das in einem vernünftigen Verhältnis zum angestrebten Zweck steht. Wie die Art. 29-Datenschutzgruppe der EU in ihrer Stellungnahme zum Einsatz von Biometrie festhält, sind bei der Beurteilung der Verhältnismässigkeit «auch die Risiken für den Schutz der Grundrechte und -freiheiten des Einzelnen zu berücksichtigen, vor allem die Frage, ob der beabsichtigte Zweck nicht auch auf eine weniger in die Rechte der Betroffenen eingreifende Weise zu erreichen ist». Wie die Art. 29-Datenschutzgruppe weiter festhält, «sind biometrische Systeme, die zur

Zugangskontrolle (Verifikation) eingesetzt werden, mit geringeren Gefahren für den Schutz der Grundrechte und -freiheiten des Einzelnen verbunden, wenn sie entweder auf Körpermerkmalen basieren, die keine Spuren hinterlassen (z.B. in Form der Hand, aber keine Fingerabdrücke), oder wenn sie zwar Körpermerkmale verwendet, die Spuren hinterlassen, die Daten jedoch auf einem Medium gespeichert werden, das sich im Besitz der betroffenen Person befindet (mit anderen Worten, wenn die Daten nicht im Gerät, das den Zugang kontrolliert oder in einer zentrales Datenbank gespeichert werden (Art. 29-Datenschutzgruppe, Arbeitspapier über Biometrie, angenommen am 1. August 2003, 12168/08/DE WP 80)).

Im vorliegenden Fall geht es um ein Reservationssystem für eine Freizeitanlage. Die Biometrie wird zur Verifizierung der Clubmitglieder eingesetzt. Datensparsamkeit erreicht man, indem nur die unbedingt zur Verifizierung notwendigen biometrischen Daten erhoben werden. Zur Verifizierung werden keine Rohdaten benötigt. Der Vergleich mit Templates reicht aus, um die berechtigte Person bei der Bestätigung der Reservation zu verifizieren. Die Beschränkung der Speicherung biometrischer Daten auf Templates, wie dies vom TC XX vollzogen wird, ist unter dem Gesichtspunkt der Datensparsamkeit verhältnismässig.

Biometrische Daten sind dauerhaft personengebunden. Aus diesem Grund sollten die biometrischen Daten – gerade wenn es um so heikle Bereiche wie Fingerabdrücke geht – im Einflussbereich der betroffenen Person, d.h. des Mitglieds, gespeichert werden und dort verbleiben.

Aus dem bisher Gesagten folgt, dass für eine datenschutzkonforme Umsetzung biometrischer Verifizierungssystemen im Freizeitbereich die nachfolgend beschriebenen drei Varianten in Frage kommen. Für den Einsatz biometrischer Charakteristika, die (physische oder digitale) Spuren hinterlassen (z.B. Fingerabdrücke oder Gesichtsfotografien), können nur die Varianten a) und b) durch den Einsatz von individuellen Karten ein genügendes Sicherheitsniveau garantieren. Die Variante c) ohne Karten kann dagegen nur dann eingesetzt werden, wenn biometrische Charakteristika verwendet werden, die keine Spuren hinterlassen (z.B. Fingervenen oder Handumriss).

a) Dezentralisierung (auf Karten)

Wie der EDÖB in seinem Leitfaden zu biometrischen Erkennungssystemen vom September 2009 festhält, wird beim Einsatz von Biometrie im Privatbereich der Persönlichkeitsschutz der Betroffenen am ehesten gewahrt, indem

1. die biometrischen Daten auf einem Sicherheitsmedium, da sich in der alleinigen Kontrolle der betroffenen Person befindet, auslesesicher gespeichert werden;

2. die betroffene Person jeden Zugriff auf die Daten explizit und bewusst freigeben muss; und

3. die Verifizierung der Identität ausschliesslich auf diesem Sicherheitsmedium stattfindet, so dass die biometrischen Daten zu keinem Zeitpunkt die gesicherte Umgebung des Mediums und die Kontrolle der betroffenen Person verlassen (biometrischer Vergleich auf Karte, vgl. Leitfaden S. 13).

b) Pseudodezentralisierung (mit Karten)

Ein annähernd gleich hohes Niveau betreffend den Persönlichkeitsschutz kann mit der Pseudodezentralisierung erreicht werden. Diese Lösung wurde denn auch vom Bundesverwaltungsgericht in seinem Urteil vom 4 August 2009 in Sachen KSS (A-3908/2008) skizziert. Im Unterscheid zur richtigen Dezentralisierung werden die biometrischen Daten zentral gespeichert, der logische Zugang zu diesen Daten ist aber einzig durch den Einsatz eines Zuordnungscodes möglich, der auf einer Karte gespeichert wird, die sich ausschliesslich im Besitz der betroffenen Person befindet. Im Einzelnen bedeutet dies Folgendes:

1. Die biometrischen Daten werden als verschlüsselte Templates zentral gespeichert (und nicht als Rohdaten, z.B. als Fingerabdruckbild oder als Fotografie);

2. die Templates sind so gespeichert, dass der Inhaber der Datensammlung keinen Bezug zu einer bestimmten oder bestimmbaren Person herstellen kann. Statistische Daten oder weitere Angaben (z.B. Zeitstempel) können in Verbindung mit den biometrischen Daten so lange gespeichert werden, wie durch sie keine Identifizierung der fraglichen Person möglich wird;

3. die Verbindung zwischen dem Template und der betroffenen Person kann einzig durch eine explizite und bewusste Freigabe durch die Verwendung der persönlichen Karte hergestellt werden.

c) Zentralisierung (ohne Karten)

Wird ein Verifizierungssystem ohne die Verwendung persönlicher Karten im Freizeitbereich gewünscht, so ist dies nur mit einer Zentralisierung der biometrischen Daten möglich. Da die zentrale Speicherung biometrischer Daten für den Verifzierungsprozess normalerweise nicht notwendig wäre, muss das System angepasst werden, damit es nicht gegen den Grundsatz der Verhältnismässigkeit verstösst:

1. Es dürfen nur biometrische Charakteristika verwendet werden, die keine (physischen oder digitalen) Spuren hinterlassen;

2. die biometrischen Daten werden als verschlüsselte Templates zentral gespeichert (und nicht als Rohdaten, z.B. als Fotografie);

3. die Templates sind so gespeichert, dass der Inhaber der Datensammlung keinen Bezug zu einer bestimmten oder bestimmbaren Person herstellen kann. Statistische Daten oder weitere Angaben (z.B. Zeitstempel) können in Verbindung mit den biometrischen Daten so lange gespeichert werden, wie durch sie keine Identifizierung der fraglichen Person möglich wird;

4. die Verbindung zwischen dem Template und der betroffenen Person wird einzig in flüchtiger Weise durch das Erkennungssystem hergestellt, mit dem Ziel, die Zugehörigkeit einer Person zum Kreis der Berechtigten festzustellen. Alle weiteren Operationen (Identifizierung der Person, Bestätigung der Reservation…) werden davon getrennt und ohne Verwendung biometrischer Charakteristika durchgeführt.

Daraus folgt, dass der TC XX in Zukunft eine der vorgeschlagenen Varianten wählt, wenn an der Verwendung biometrischer Erkennungssysteme festgehalten wird. Die gilt auch für die bereits zentral gespeicherten biometrischen Daten. Eine zentrale Speicherung, wie sie zurzeit praktiziert wird, ist unter dem Blickwinkel des Grundsatzes der Datensparsamkeit und des Grundsatzes der möglichst schonenden Bearbeitung von Personendaten, im vorliegenden Fall der Reservation von Tennisplätzen des TC XX, unverhältnismässig.

5.5.2.2 Veröffentlichung der Reservationsdaten im Internet

Das Reservationssystem ermöglicht es den Mitgliedern, die Platzreservation via Internet vorzunehmen und die so getätigte Reservation anschliessend vor Ort mit dem Fingerabdruck zu bestätigen. Zu diesem Zweck ist das System auf der Website des TC XX aufgeschaltet. Der EDÖB anerkennt, dass die Online-Reservation den Mitgliedern einen grossen Nutzen bringt und daneben auch die Möglichkeit eröffnet, Spielpartner zu suchen und zu finden. Zur Erfüllung dieses Zwecks erscheint es auch verhältnismässig, den Mitgliedern einen Online-Zugang zum Reservationssystem zu gewähren.

Nach Ansicht des EDÖB besteht dagegen kein Grund dafür, den Zugang zu den Reservationsdaten ohne Beschränkung zuzulassen und damit auch Nichtmitgliedern Einsicht zu gewähren. Dies geht weit über das für die Zweckerreichung Notwendigen hinaus. Nach Ansicht des EDÖB ist der Online-Zugang zum Reservationssystem daher auf die Clubmitglieder zu beschränken. Dies kann beispielsweise durch einen Passwortschutz geschehen. Nachdem die Online-Reservation ohnehin ein Login erfordert, bedarf es für diese Beschränkung nur einer geringfügigen Änderung des Systems. So könnte man beispielsweise bereits für die Einsicht in die Reservationsdaten ein Login verlangen.

Der EDÖB regt zudem an, dass bei Erstellung eines Benutzerkontos automatisch darauf hingewiesen wird, dass bei unveränderten Grundeinstellungen im Online-Reservationssystem der richtige Nachname angezeigt wird, dass explizit danach gefragt wird, ob die betroffene Person damit einverstanden ist und auf die Möglichkeit der Pseudonymisierung des angezeigten Namens verwiesen wird.

Zusammenfassend kann festgehalten werden, dass die jetzige Veröffentlichung der Reservationsdaten im Internet weit über das zur Zweckverfolgung Notwendige hinausgeht. Sie ist damit unter dem Grundsatz der möglichst schonenden Bearbeitung von Personendaten unverhältnismässig.

5.5.3 Verhältnismässigkeit in zeitlicher Hinsicht – Ausgangslage

Das Erfordernis der Verhältnismässigkeit begrenzt die Datenbearbeitung auch in zeitlicher Hinsicht. Sofern personenbezogene Daten für den verfolgten Zweck nicht mehr gebraucht werden, sind sie zu vernichten oder zu anonymisieren. Dabei ist eine frühest mögliche Löschung/Anonymisierung vorzusehen.

Vorliegend werden an drei Orten Personendaten gespeichert: Auf dem PC «Biometrie», auf dem Sekretariats-PC und auf dem Webserver für das Reservationssystem. Für keinen dieser Speicherorte besteht eine Regelung für die Speicherdauer oder die Zuständigkeit für die Löschung. Bis jetzt werden auf dem PC «Biometrie» und auf dem Sekretariats-PC keine regelmässigen Datenlöschungen durchgeführt, im Reservationssystem werden die Reservationsdaten aus Platzgründen alle 2 bis 3 Jahre, die Logdaten nach ca. 1 Jahr, gelöscht.

5.5.4 Beurteilung der zeitlichen Verhältnismässigkeit aus Sicht des EDÖB

Der EDÖB hat bereits bei der Besichtigung der Anlage vor Ort darauf aufmerksam gemacht, dass bei der Bearbeitung von sensiblen Personendaten die Speicherdauer der Daten sowie die Zuständigkeit für die Löschung nicht mehr benötigter Daten geregelt und in einem Reglement festgehalten werden sollte, da für die Betroffenen sonst nicht einschätzbar ist, wie lange die Daten gespeichert werden. Zudem besteht tatsächlich die Gefahr, dass der Löschung der Daten zu wenig Beachtung geschenkt wird und diese daher dauerhaft aufbewahrt würden.

Die Templates auf dem PC «Biometrie» sowie die auf dem Sekretariats-PC gespeicherten Mitgliederdaten sind zu löschen, sobald sie nicht mehr benötigt werden. Dies ist spätestens dann der Fall, wenn ein Mitglied den Austritt gibt. Die Löschung der Daten beim Austritt muss daher einerseits im Reglement festgehalten und in den Standardprozess für solche Fälle aufgenommen werden. Für den EDÖB sind keinerlei Gründe ersichtlich, welche die Speicherdauer von 2 bis 3 Jahren für die Reservationsdaten und die von einem Jahr für die Logdaten im Reservationssystem rechtfertigen würden.

Es wird daher davon ausgegangen, dass die Speicherdauern unverhältnismässig lange sind und auf ein angemessenes Mass reduziert werden müssen. Der TC XX hat dem EDÖB daher einen Vorschlag zu unterbreiten, wie die Löschfristen festgelegt werden sollen und diese Fristen anschliessend (technisch) umzusetzen. Dabei muss nebst der Löschung der oberwähnten Daten auch diejenige von diesen Daten gemachten Backups und dergleichen geregelt werden.

5.6 Zweckbindung der Datenbearbeitung

5.6.1 Ausgangslage

Personendaten dürfen nur für den Zweck bearbeitet werden, welcher bei der Beschaffung angegeben worden ist oder der aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG). Da eine Änderung des Bearbeitungszwecks von den Betroffenen durch die zentrale Speicherung der biometrischen Daten nicht kontrollierbar ist, sind technische Lösungen vorzuziehen, welche die Zweckbindung ausreichend gewährleisten.

5.6.2 Beurteilung aus Sicht des EDÖB

Durch die zentrale Speicherung der Templates in der Datenbank ist eine Zweckentfremdung in der Bearbeitung dieser Daten nicht gänzlich ausgeschlossen. Dies unter anderem auch deshalb, weil die Daten sich nicht in der Nutzersphäre der Betroffenen befinden. Eine Zweckentfremdung im Sinne einer Verknüpfung mit anderen Datensammlungen oder eine Weitergabe an aussen stehende Dritte wäre möglich. Auch wenn die Tatsache berücksichtigt wird, dass keine Rohdaten, sondern Templates in der Datenbank abgelegt werden, ist auch aus Gründen der Zweckbindung der Datenbearbeitung auf eine zentrale Speicherung der biometrischen Daten, wie sie zurzeit praktiziert wird, zu verzichten und auf einer der unter Ziffer 5.5.2.1 aufgeführten Varianten umzustellen.

5.7 Datenrichtigkeit (Zuverlässigkeit, Anwendbarkeit)

5.7.1 Ausgangslage

Das Vergleichsverfahren zwischen Referenz- und aktuell präsentieren Daten (hier Templates der Fingerabdrücke) basiert auf Wahrscheinlichkeitsberechnungen und ergibt einen Übereinstimmungswert, der grösser als eine vordefinierte Schwelle sein muss, um die Person zu erkennen. Von dieser einzigen Schwelle sind die beiden Werte «Fals Rejection Rate (FFR)» und «False Acceptance Rate (FAR)» umgekehrt abhängig. Aus

Gründen des Persönlichkeitsschutzes sollte von allem die FAR vermindert werden, ohne aber die FRR zu stark zu beeinträchtigen. Die Wahl eines optimalen Schwellenwertes für eine ausreichende Zuverlässigkeit des gesamten biometrischen Systems ist aus diesem Grunde nicht einfach zu treffen.

Nicht ausser Acht gelassen werden darf auch die Tatsache, dass gewisse Anwender (aufgrund fehlender Gliedmassen, Verletzungen, Narben oder aufgrund des Alters, wie z.B. Kinder oder ältere Personen) keine oder zu wenig gute biometrische Merkmale vorweisen und ihre Verifizierung misslingen kann. Für diese Personen ist ein Alternativszenario vorzusehen, welches nicht zu einer Diskriminierung der Betroffenen führen darf.

5.7.2 Beurteilung aus Sicht des EDÖB

Aus Datenschutzgründen sollte die FAR vermindert werden, ohne aber die FRR zu stark zu beeinträchtigen. Zudem sollte ein optimaler Schwellenwert gewählt werden. Jedes biometrische System weist einen gewissen Prozentsatz an FAR auf. Die Verifizierung kann infolgedessen nicht zu 100 % zuverlässig erfolgen. Das System des TC XX extrahiert 12 Minutien pro Template. Dies ist aus heutiger Sicht knapp ausreichend. Tests vor Ort haben denn auch ergeben, dass das System funktioniert.

Probleme ergeben sich weiter auch bei Personen, denen gewisse biometrische Merkmale fehlen oder nur schlecht lesbar vorhanden sind (Enrolement). Für solche Ausnahmen muss eine äquivalente Anwendbarkeit des Erkennungssystems geplant und eingesetzt werden. Eine solche Alternative besteht vorliegend. Anstelle einer Verifizierung mittels Fingerabdrücken wird eine PIN eingesetzt. Diese Alternative ist für die Betroffenen sowohl kostenneutral als auch von der Handhabung her äquivalent. Es gibt offenbar bereits Mitglieder, welche das Fingerabdrucksystem aus gesundheitlichen Gründen nicht nutzen können und ihre Reservationen daher mittels PIN bestätigen. Dies funktioniert problemlos.

Die Datenrichtigkeit ist damit beim Reservationssystem des TC XX gewährleistet. Der EDÖB hat hier keine weiteren Bemerkungen.

5.8 Datensicherheit

5.8.1 Ausgangslage

Gemäss Art. 7 DSG müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten gesichert werden. Zu gewährleisten sind insbesondere die Vertraulichkeit, die Verfügbarkeit sowie die Integrität der Personendaten. Diese Anforderungen sind dann nicht mehr gewährleistet, wenn

Unbefugte leichten Zugriff auf die Daten haben oder ein fremdes «Drittgerät» die Daten abhören oder manipulieren könnte. Die Datensicherheit liegt in der Verantwortung derjenigen Stelle, welche die Datenherrschaft über die Personendaten inne hat (Art. 8 Abs. 1 der Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG; SR 235.11).

Wie bereits ausgeführt wurde, befinden sich sowohl der PC «Biometrie» als auch der Sekretariats-PC in von aussen zugänglichen und nur durch ein einfaches Schloss gesicherten Räumen des Clubhauses. Zum PC «Biometrie» haben 5 bis 6 Personen Zutritt, wobei 2 bis 3 davon vom TC XX nicht näher benannt werden konnten. Zum Sekretariats-PC haben ausserhalb der Öffnungszeiten 11 Personen Zutritt, während der Öffnungszeiten kann der Raum von jedermann betreten werden, wobei der PC dann i.d.R. nicht unbeaufsichtigt ist und der Zugang auf die dort gespeicherten Daten passwortgeschützt ist.

Der PC «Biometrie» und der Sekretariats-PC sind via WIFI miteinander und mit dem Internet verbunden. Das WIFI ist durch das Protokoll WPA (seit März 2010 WPA2) gesichert. Den Mitgliedern wird auf Wunsch das WIFI-Passwort bekannt gegeben, damit diese während ihres Aufenthalts auf dem Clubgelände via WIFI aufs Internet zugreifen können.

Vom Sekretariats-PC aus kann via eine versteckte Partition auf dem PC «Biometrie» auf die dort gespeicherten Templates zugegriffen werden.

5.8.2 Beurteilung aus Sicht des EDÖB

Der EDÖB beurteilt die physische Sicherung des PC «Biometrie» und des Sekretariats-PC als ungenügend. Die Türen samt Schlössern können ohne grösseren Aufwand aufgebrochen werden. Damit sind die beiden PCs nicht in dem Masse physisch gesichert, wie dies vorliegend angezeigt wäre, und ein «Datendiebstahl» oder gar die Entwendung der ganzen PCs wäre leicht möglich. Dies muss aus Sicht des EDÖB dringend verbessert werden, insbesondere in Anbetracht der Sensibilität der auf den PCs gespeicherten Daten.

Der Zugang zu den PCs «Biometrie» und dem Sekretariats-PC ist zuwenig klar geregelt. Es muss daher für beide Rechner sowie eine Liste erstellt werden, in der die Zutrittsberechtigten klar definiert werden, wobei die Anzahl der Berechtigten auf ein Minimum reduziert werden muss. Dasselbe gilt für die Zugangsberechtigten für die genannten Rechner (Benutzerkonten) und den Zutritt und den Zugang zu Backups und dergleichen.

Der EDÖB erachtet es zudem als problematisch, dass die Übertragung (biometrischer) Persondaten via WIFI erfolgt, welches nicht denselben Sicherheitsstandard bieten kann wie eine Übermittlung via Kabel, und dieses WIFI auch von den Mitgliedern für den

Zugang zum Internet genutzt werden kann. Er schlägt daher vor, dass die Verbindung zwischen dem PC «Biometrie» und dem Sekretariats-PC sowie die Verbindungen zum Router/Modem mittels Kabel erfolgen und das WIFI nur noch für den Internetzugang der Mitglieder genutzt wird. Damit erfolgt die Übertragung der (biometrischen) Personendaten sicherer und getrennt vom Internetverkehr der Mitglieder.

5.9 Auskunftsrecht

5.9.1 Ausgangslage

Gemäss Art. 8 DSG kann jede Person vom Inhaber der Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden.

Beim TC XX können die Mitglieder sich jederzeit an den Präsidenten wenden, um Einsicht in die Template-Datenbank zu erhalten. Der Präsident will dieses Auskunftsrecht auf sämtliche Mitgliederdaten ausweiten.

5.9.2 Beurteilung aus Sicht des EDÖB

Mit der Ausweitung des Auskunftsrechts auf sämtliche Mitgliederdaten sind die diesbezüglichen Rechte der Mitglieder gewahrt. Der EDÖB hat dazu keine weiteren Bemerkungen.

6. Ergebnisse

Aufgrund der Auswertung der eingereichten Unterlagen und Dokumente sowie gestützt auf die durchgeführte Kontrolle vom 11. Februar 2010 gemäss Art. 29 DSG gelangt der EDÖB zu einer kritischen Gesamtbeurteilung des biometrischen Reservationssystems. Die Datenschutzkontrolle hat gezeigt, dass die seit der Einführung des biometrischen Reservationssystems erfolgte Bearbeitung von Personendaten durch den TC XX nicht in allen Aspekten datenschutzkonform verläuft. Der EDÖB ist in seiner Kontrolle auf Sachverhalte gestossen, welche aus datenschutzrechtlicher Sicht einer Verbesserung resp. Änderung bedürfen.

Ausgehend von diesem Gesamtbild erlässt der EDÖB zuhanden des TC XX seine Gesamtbeurteilung in folgender Form:

- Feststellungen und/oder
- Empfehlungen im Sinne des Art. 29 Abs. 3 DSG.

6.1 Biometrische Daten als Personendaten

Bei biometrischen Daten der Fingerabdrücke handelt es sich um Personendaten gemäss Art- 3 lit. a DSG. Biometrische Daten in Form von Rohdaten oder Templates machen eine Person identifizierbar resp. bestimmbar. Ihre Erhebung hinterlässt in der Regel – insbesondere bei der Erhebung von Fingerabdrücken – (Daten-)Spuren. Die Erhebung von Rohdaten oder Templates ist somit geeignet, ein Bewegungsprofil der betroffenen Person zu erstellen. Gestützt auf diese Tatsache besteht bei der Erhebung biometrischer Daten für die betroffene Person ein hohes Potenzial für Persönlichkeitsverletzungen.

6.2 Zweck der Datenbearbeitung

Jede Bearbeitung von Personendaten stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 des Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101) dar. Daher bedarf die Bearbeitung einer besonderen Rechtfertigung. Praktikabilitätserwägungen oder allgemeine Bedienerfreundlichkeit stellen grundsätzlich keine ausreichende Rechtfertigung für die Bearbeitung biometrischer Daten dar.

Gemäss Auskunft des TC XX geht es bei der Erfassung der biometrischen Daten ausschliesslich um die automatisierte Missbrauchsbekämpfung bei der Reservation und der Nutzung von Tennisplätzen. Der Vorteil für den TC XX läge darin, dass keine persönliche Prüfung der Identität der Spieler bei der Reservation und der Platznutzung (z.B. durch den Betrieb einer Reception) vorgenommen werden müsse. Das neue biometrische Reservationssystem ersetzt das veraltete Reservationssystem mittels PIN, bei dem es zu zahlreichen Missbräuchen gekommen sei. Gemäss Angaben des TC XX hat sich die Zahl der Mitglieder seit Einführung des neuen Systems stark erhöht, während die Plätze in derselben Zeit weniger genutzt wurden, was mit der fehlenden Missbrauchsmöglichkeit in Zusammenhang stehe. Der Vorteil für die Mitglieder besteht darin, dass sie keine Mitgliederkarte oder dergleichen mit sich führen müssen. Zudem sind, wie unter dem bisherigen System, Reservationen via Internet möglich.

Das neue biometrische Reservationssystem des TC XX verfolgt nachvollziehbare Zwecke. Dennoch möchte der EDÖB seine ernsthaften Bedenken bezüglich der Frage äussern, ob es nicht andere Alternativen zur Missbrauchsvermeidung geben würde, welche weniger stark in die Persönlichkeitsrechte der Betroffenen eingreifen würden (vgl. dazu auch das Ergebnis des Verhältnismässigkeitsprüfung unter Ziffer 6.5.1.1, Empfehlung Nr. 2).

6.3 Rechtmässigkeit der Datenbeschaffung / Einwilligung der Betroffenen

Die Bearbeitung biometrischer Daten bedarf eines Rechtfertigungsgrundes (Art. 12 und 13 DSG). Als Rechtfertigungsgrund kommt im vorliegenden Fall die Einwilligung der Betroffenen in Frage. Das biometrische Reservationssystem wurde nach einem entsprechenden GV-Beschluss eingeführt. Denjenigen Mitgliedern, die mit dem System nicht einverstanden waren, wurde eine valable Alternative geboten, so dass davon ausgegangen werden kann, dass diejenigen Mitglieder, welche das biometrische System nutzen, ihre Einwilligung geben. Aus Sicht des EDÖB fehlen jedoch wichtige Informationen, wie insbesondere die Bearbeitungsmodalitäten und der explizite Hinweis auf die Alternative ohne Einsatz biometrischer Daten.

Aus Sicht des EDÖB fehlen vorliegend wichtige Informationen, insbesondere über die Bearbeitungsmodalitäten, die explizite Erwähnung des Bestehens einer Alternative ohne Verwendung biometrischer Daten und die Tatsache, dass der Familienname im Reservationssystem angezeigt wird (vgl. Ziffer 6.5.1.2 nachstehend).

Empfehlung Nr. 1:

a) Der TC XX erarbeitet bis zum 31.12.2010 ein Informationenblatt, welches die Modalitäten der Bearbeitung der biometrischen Daten, die Möglichkeit einer Alternative ohne Verwendung biometrischer Daten, wie auch die Tatsache, dass der Familienna-men der Mitglieder im Reservationssystem angezeigt wird, wenn nicht von der Möglichkeit der Pseudonymisierung Gebrauch gemacht wird, Auskunft gibt. Aufgeführt werden müssen die Hauptpunkte der Datenbearbeitung, wie z.B. die Einzelheiten Datenbe-arbeitung, wo und wie lange die Daten gespeichert werden, insbesondere, was mit den Templates und den Transaktionsdaten geschieht, wer Zugriff auf die Daten hat und an wen sie, wenn überhaupt, weitergegeben werden etc.

b) Dieses Informationsblatt muss von einem Mitglied des Vorstands unterzeichnet und mit einer Versionenkontrolle versehen werden.

c) Dieses Informationsblatt ist umgehend allen bestehenden Mitgliedern auszuhändigen und jedem Neumitglied vor dem Enrolement abzugeben. Dem Neumitglied ist genügend Zeit zu Verfügung zu stellen, das Informationsblatt vor dem Enrolement durchzulesen.

6.4 Bearbeitung nach Treu und Glauben / Transparenz

Das Enrolement erfolgt ausschliesslich unter Mitwirkung des Mitglieds. Ohne sein Zutun können beim TC XX keine biometrischen Daten erhoben werden. Die Datenbearbeitung erfolgt in diesem Punkt transparent und ist für die Betroffenen erkennbar.

Jedoch muss bemängelt werden, dass die Information der Mitglieder hinsichtlich der Bearbeitungsmodalitäten ungenügend ist. Die Mitglieder wurden zwar anlässlich der GV, durch die Gebrauchsanweisung sowie mündlich durch den Vereinspräsidenten informiert. Für eine möglichst transparente Datenbearbeitung sollte neben den mündlichen Informationen durch den Vereinspräsidenten und der rein über die richtige Handhabung des Systems informierende Gebrauchsanweisung auch ein Infoblatt abgegeben werden, auf dem umschrieben ist, was mit den Personendaten geschieht und dass eine Alternative ohne Erhebung biometrischer Daten besteht (vgl. EmpfehlungNr. 1).

6.5 Verhältnismässigkeit der Datenbearbeitung

6.5.1 Verhältnismässigkeit in inhaltlicher Hinsicht

6.5.1.1 Zentrale Speicherung biometrischer Daten

Der Einsatz biometrischer Verfahren im Privatbereich stellt, je nach Ausgestaltung im konkreten Einzelfall, einen mehr oder weniger intensiven Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Grundsätzlich sind daher vor dem Einsatz biometrischer Verfahren immer auch andere geeignete Massnahmen zu überprüfen, welche weniger in die Grundrechte der Betroffenen eingreifen und mit denen der angestrebte Zweck ebenfalls erreicht werden kann. Des Weitere muss bei der Auswahl und Ausgestaltung des biometrischen Verfahrens darauf geachtet werden, ein möglichst datensparsames System auszuwählen, das in einem vernünftigen Verhältnis zum angestrebten Zweck steht.

Im vorliegenden Fall geht es um ein Reservationssystem für Tennisplätze. Die Biometrie wird hier zur Verifizierung der Mitglieder eingesetzt. Datensparsamkeit erreicht man, indem nur die unbedingt zur Verifizierung notwendigen biometrischen Daten erhoben werden.

Für den Einsatz des neuen Reservationssystems werden aus den Fingerabdrücken der Mitglieder Templates generiert und diese zentral in einer Datenbank abgelegt. Rohdaten (d.h. das Originalbild des Fingerabdrucks) werden keine erhoben. Die Beschränkung der Speicherung biometrischer Daten auf Templates, wie dies vom TC XX vollzogen wird, ist unter dem Gesichtspunkt der Datensparsamkeit verhältnismässig und zu begrüssen.

Biometrische Daten sind dauerhaft personengebunden und geeignet, von der betroffenen Person ein Bewegungsprofil zu erstellen. Aus diesem Grund sollten die biometrischen Daten – gerade wenn es um so heikle Bereiche wie Fingerabdrücke geht – im Einflussbereich der betroffenen Person resp. des Nutzers gespeichert werden. Der Grundsatz der inhaltlichen Verhältnismässigkeit erfordert, dass bei biometrischen Systemen, die auch ohne zentrale Speicherung funktionsfähig sind, die biometrischen Merkmale möglichst nicht in einer zentralen Datenbank gespeichert werden sollten, sondern nur auf einem Medium, das ausschliesslich dem Benutzer zugänglich ist. Insbesondere beim Einsatz der Biometrie für ein Reservationssystem in einer Freizeitanlage muss aus Gründen des Persönlichkeits- und Datenschutzes auf eine zentrale Speicherung verzichtet werden.

Aus dem bisher Gesagten folgt, dass für eine datenschutzkonforme Umsetzung biometrischer Verifizierungssystemen im Freizeitbereich die nachfolgend beschriebenen drei Varianten in Frage kommen. Für den Einsatz biometrischer Charakteristika, die (physische oder digitale) Spuren hinterlassen (z.B. Fingerabdrücke oder Gesichtsfotografien), können nur die Varianten a) und b) durch den Einsatz von individuellen Karten ein genügendes Sicherheitsniveau garantieren. Die Variante c) ohne Karten kann dagegen nur dann eingesetzt werden, wenn biometrische Charakteristika verwendet werden, die keine Spuren hinterlassen (z.B. Fingervenen oder Handumriss).

a) Dezentralisierung (auf Karten)

Wie der EDÖB in seinem Leitfaden zu biometrischen Erkennungssystemen vom September 2009 festhält, wird beim Einsatz von Biometrie im Privatbereich der Persönlichkeitsschutz der Betroffenen am ehesten gewahrt, indem

1. die biometrischen Daten auf einem Sicherheitsmedium, da sich in der alleinigen Kontrolle der betroffenen Person befindet, auslesesicher gespeichert werden;
2. die betroffene Person jeden Zugriff auf die Daten explizit und bewusst freigeben muss; und
3. die Verifizierung der Identität ausschliesslich auf diesem Sicherheitsmedium stattfindet, so dass die biometrischen Daten zu keinem Zeitpunkt die gesicherte Umgebung des Mediums und die Kontrolle der betroffenen Person verlassen (biometrischer Vergleich auf Karte, vgl. Leitfaden S. 13).

b) Pseudodezentralisierung (mit Karten)

Ein annähernd gleich hohes Niveau betreffend den Persönlichkeitsschutz kann mit der Pseudodezentralisierung erreicht werden. Diese Lösung wurde denn auch vom

Bundesverwaltungsgericht in seinem Urteil vom 4 August 2009 in Sachen KSS (A-3908/2008) skizziert. Im Unterscheid zur richtigen Dezentralisierung werden die biometrischen Daten zentral gespeichert, der logische Zugang zu diesen Daten ist aber einzig durch den Einsatz eines Zuordnungscodes möglich, der auf einer Karte gespeichert wird, die sich ausschliesslich im Besitz der betroffenen Person befindet. Im Einzelnen bedeutet dies Folgendes:

1. Die biometrischen Daten werden als verschlüsselte Templates zentral gespeichert (und nicht als Rohdaten, z.B. als Fingerabdruckbild oder als Fotografie);
2. die Templates sind so gespeichert, dass der Inhaber der Datensammlung keinen Bezug zu einer bestimmten oder bestimmbaren Person herstellen kann. Statistische Daten oder weitere Angaben (z.B. Zeitstempel) können in Verbindung mit den biometrischen Daten so lange gespeichert werden, wie durch sie keine Identifizierung der fraglichen Person möglich wird;
3. die Verbindung zwischen dem Template und der betroffenen Person kann einzig durch eine explizite und bewusste Freigabe durch die Verwendung der persönlichen Karte hergestellt werden.

c) Zentralisierung (ohne Karten)

Wird ein Verifizierungssystem ohne die Verwendung persönlicher Karten im Freizeitbereich gewünscht, so ist dies nur mit einer Zentralisierung der biometrischen Daten möglich. Da die zentrale Speicherung biometrischer Daten für den Verifizierungsprozess normalerweise nicht notwendig wäre, muss das System angepasst werden, damit es nicht gegen den Grundsatz der Verhältnismässigkeit verstösst:

1. Es dürfen nur biometrische Charakteristika verwendet werden, die keine (physischen oder digitalen) Spuren hinterlassen;
2. die biometrischen Daten werden als verschlüsselte Templates zentral gespeichert (und nicht als Rohdaten, z.B. als Fotografie);
3. die Templates sind so gespeichert, dass der Inhaber der Datensammlung keinen Bezug zu einer bestimmten oder bestimmbaren Person herstellen kann. Statistische Daten oder weitere Angaben (z.B. Zeitstempel) können in Verbindung mit den biometrischen Daten so lange gespeichert werden, wie durch sie keine Identifizierung der fraglichen Person möglich wird;
4. die Verbindung zwischen dem Template und der betroffenen Person wird einzig in flüchtiger Weise durch das Erkennungssystem hergestellt, mit dem Ziel, die Zugehörigkeit einer Person zum Kreis der Berechtigten festzustellen. Alle weiteren

Operationen (Identifizierung der Person, Bestätigung der Reservation…) werden davon getrennt und ohne Verwendung biometrischer Charakteristika durchgeführt.

Empfehlung Nr. 2:

a) In Zukunft, jedoch spätestens ab 30.06.2011verzichtet der TC XX auf die zentrale Speicherung der biometrischen Daten in der heute praktizierten Form von Templates der Fingerabdrücke.

b) Wenn der TC XX an der Verwendung biometrischer Daten für die Verifizierung seiner Mitglieder im Reservationssystem festhalten will, so

- sind diese biometrischen Daten – auch diejenigen, welche bereits zentral erfasst wurden – auf einem Datenträger, welcher in der Benutzersphäre und unter Kontrolle der betroffenen Personen verbleibt (Minimum biometrischer Vergleich auf Karte, vgl. S. 13 des Leitfadens), zu speichern; oder

- sind diese biometrischen Daten zentralisiert als verschlüsselte Templates zu speichern, ohne jegliche Verbindung zu anderen Personendaten, so dass der Bezug zu einer bestimmten oder bestimmbaren Person einzig durch eine bewusste und explizite Freigabe durch die betroffene Person durch die Verwendung einer persönlichen Karte hergestellt werden kann; oder

- sind nur biometrische Charakteristika zu verwenden, die keinerlei (physische oder digitale) Spuren hinterlasse. Die biometrischen Daten sind dabei als verschlüsselte Templates ohne dauerhaften Bezug zu anderen Personendaten zu speichern.

6.5.1.2 Veröffentlichung der Reservationsdaten im Internet

Eine Veröffentlichung von Personendaten im Internet ist stets mit besonderen Risiken Verbunden. Aus diesem Grund ist der Zweck der Veröffentlichung vorgängig sorgfältig zu prüfen und die Veröffentlichung auf die für den Zweck unbedingt erforderlichen Daten zu beschränken. Wenn immer möglich, ist der Zugang beispielsweise durch einen Passwortschutz auf diejenigen Personen zu beschränken, die den Zugang zur Zweckerreichung benötigen.

Vorliegend dient die Veröffentlichung im Internet dem Zweck, den Clubmitgliedern eine Online-Reservation zu ermöglichen. Dieser Zweck kann ohne Einschränkungen auch erreicht werden, wenn der Zugang auf die Clubmitglieder beschränkt wird. Auch die technische Umsetzung der Zugangsbeschränkung dürfte wenig Probleme bereiten, wird doch für die Tätigung einer Reservation bereits jetzt ein Login benötigt. Die Beschränkung kann mit Benutzeridentifikation und Passwort erreicht werden. Für die

vertrauliche Übertragung stehen heute erprobte Verschlüsselungssysteme, wie beispielsweise das SSL-Protokoll (Secure Socket Layer), zur Verfügung. Die Schlüssellänge sollte dabei mindestens 128 Bit betragen.

Empfehlung Nr. 3:

Der Zugang zum online- Reservationssystem ist bis zum 31.12.2010 auf die Mitglieder zu beschränken und daher mit einem Passwortschutz zu versehen Die Übertragung der Daten hat verschlüsselt (nach aktuellem Stand der Technik) zu erfolgen.

Für die Online-Reservation ist die Namensnennung zudem nicht notwendig. Es genügt, wenn erkennbar ist, ob ein Platz frei oder besetzt ist. Der Mehrwert, durch die Namensnennung Spielpartner finden zu können, muss auf freiwilliger Basis geschehen. Wird in den Grundeinstellungen jedoch der richtige Name angezeigt, besteht die Gefahr, dass viele Mitglieder aus Unwissenheit oder Bequemlichkeit den richtigen Namen stehen lassen, ohne dass sie mit einer Veröffentlichung ihres Namens im Reservationssystem tatsächlich einverstanden sind. Aus diesem Grund müssen die Mitglieder auf diesen Umstand sowie die Möglichkeit der Pseudonymisierung aufmerksam gemacht werden (vgl. Empfehlung Nr. 1a).

6.5.2 Verhältnismässigkeit in zeitlicher Hinsicht

Beim TC XX werden zurzeit keine regelmässigen Datenlöschungen durchgeführt. Die Daten im Reservationssystem werden aus Platzgründen alle 2 bis 3 Jahre gelöscht, die übrigen Daten werden bis jetzt gar nicht gelöscht. Es sind nirgends Löschfristen für die Daten festgehalten. Dies ist in zeitlicher Hinsicht unverhältnismässig.

Empfehlung Nr. 4:

Der TC XX hat für sämtliche Personendaten Löschfristen einzuführen, inkl. für die Backupdaten. Daher hat der TC XX dem EDÖB einen Vorschlag für die Regelung der Löschfristen einzureichen und diese bis zum 31.12.2010 umzusetzen und die technischen Anpassungen vorzunehmen.

6.6 Zweckbindung der Datenbearbeitung

Durch die derzeit praktizierte zentrale Speicherung der Templates kann eine Zweckentfremdung (d.h. eine über die Missbrauchsverhinderung hinausgehende Datenbearbeitung) dieser heiklen Daten nicht gänzlich ausgeschlossen werden. Eine Zweckentfremdung im Sinne einer Verknüpfung mit anderen Datensammlungen oder einer Weitergabe an aussenstehende Dritte wäre möglich. Da eine Änderung des Bearbeitungszwecks

der biometrischen Daten von den Betroffenen durch die zentrale Speicherung der Daten nicht kontrollierbar ist, sind technische Lösungen vorzuziehen, welche die Zweckbindung ausreichend gewährleisten. Unter dem Aspekt der Zweckbindung ist die dezentrale Speicherung der biometrischen Daten auf einem sich in der Nutzersphäre der Betroffenen befindenden Datenträger und nicht, wie vorliegend, eine zentrale Speicherung der Daten vorzusehen. Es kann an dieser Stelle auf die Empfehlung Nr. 2 verwiesen werden.

6.7 Datenrichtigkeit (Zuverlässigkeit, Anwendbarkeit)

Aus Datenschutzgründen sollte die False Acceptance Rate (FAR) vermindert werden, ohne aber die False Rejection Rate (FRR) zu stark zu beeinträchtigen. Gleichzeitig sollte ein optimaler Schwellenwert gewählt werden. Jedes biometrische System weist einen gewissen Prozentsatz an FAR auf. Die Verifizierung kann infolgedessen nicht zu 100 % zuverlässig erfolgen.

Für Personen, denen biometrische Merkmale fehlen oder deren biometrische Merkmale z.B. aufgrund des Alters, Narben oder sonstiger Gründe nicht oder nur schlecht eingelesen werden können, muss eine äquivalente Anwendbarkeit des Erkennungssystems geplant und eingesetzt werden.

Die Anzahl der vom TC XX verwendeten Minutien pro Template liegt innerhalb der Bandbreite des Zulässigen. Diejenigen Personen, die das biometrische System aufgrund fehlender oder für das System nicht genügender biometrischer Merkmale nicht nutzen können, können ihre Reservationen mittels PIN vornehmen und haben damit eine äquivalente Alternative. Abgesehen davon, dass der EDÖB der Ansicht ist, die zentrale Speicherung sei unverhältnismässig und daher eine dezentrale Speicherung auf einem Speichermedium in der Nutzersphäre der betroffenen Person einzuführen (vgl. Empfehlung Nr. 2), hat der EDÖB zur Datenrichtigkeit keine Bemerkungen.

6.8 Datensicherheit

Die Datensicherheit ist beim TC XX, gerade in Anbetracht der Sensibilität der verwendeten Personendaten, zu wenig gewährleistet. Die Rechner müssen physisch besser gesichert werden, um die Wahrscheinlichkeit eines Diebstahls zu verringern. Zudem müssen die Zugangs- und Zutrittsberechtigung genauer geregelt und reduziert werden, um auch hier die Risiken zu senken. Eine Umgestaltung des Netzwerks sollte ausserdem die Sicherheit der Datenübertragung erhöhen.

Empfehlung Nr. 5:

Um die zurzeit ungenügende Datensicherheit zu erhöhen, insbe-sondere auch in Anbetracht der Sensibilität der fraglichen Daten, hat der TC XX bis zum 31.12.2010

a. die physische Sicherung des PC «Biometrie» und des Sekretariats-PC durch geeignete Massnahmen verbessert.

b. die Zutrittsberechtigungen zum PC «Biometrie» und zum Sekretariats-PC regelt, wobei die Anzahl der Zutrittsberechtigten auf ein Minimum zu reduzieren ist.

c. die Zugangsberechtigungen zu sämtlichen vom TC XX gespeicherten Personendaten, inkl. Backups, regelt, wobei die Anzahl der Zutrittsberechtigten auf ein Minimum zu reduzieren ist.

d. die kabellose Datenübertragung zwischen dem PC «Biometrie» und dem Sekretariats-PC und zwischen dem Sekretariats-PC und dem Modem/Router durch eine Übermittlung via Kabel ersetzt.

6.9 Auskunftsrecht

Die Mitglieder haben jederzeit die Möglichkeit, ihre persönlichen Daten einzusehen und aktualisieren zu lassen. Das Auskunftsrecht der Mitglieder wird gewährleistet. Der EDÖB hat dazu keine Bemerkungen.

7. Schlussfolgerungen

7.1 Bezüglich der Kontrolle der Erhebung biometrischer Daten

Zum Zweck der Eindämmung von Missbräuchen bei der Reservation und Nutzung der Tennisplätze hat der TC XX im Sommer 2009 ein neues Reservationssystem eingeführt, bei dem neben der Personalien der Mitglieder auch biometrische Daten in Form von Templates der Fingerabdrücke erhoben und gespeichert werden.

Die durchgeführte Datenschutzkontrolle konnte dem EDÖB einen vertieften Einblick in das neue Reservationssystem liefern. Die vom TC XX zu Verfügung gestellten Unterlagen und Dokumente haben es dem EDÖB erlaubt, die damit verbundene Datenbearbeitung auf die Einhaltung der Datenschutzbestimmungen zu überprüfen.

Der EDÖB gelangt zu einer kritischen Gesamtbeurteilung des biometrischen Reservationssystems. Die Datenschutzkontrolle hat gezeigt, dass die seit der Einführung des neuen biometrischen Reservationssystems erfolgte Bearbeitung von Personendaten

durch den TC XX nicht in allen Aspekten datenschutzkonform verläuft. Wo Änderungen vorgenommen werden müssen oder wo Verbesserungsbedarf besteht, hat dies der EDÖB mit Begründung erläutert.

7.2 Verfahren und weiteres Vorgehen

Der vorliegende Kontrollbericht enthält eine Reihe von Feststellungen sowie Empfehlungen, welche vom EDÖB auf Basis der durchgeführten Kontrolle verfasst wurden. Der vorliegende Kontrollbericht wird dem TC XX zur Kenntnisnahme zugestellt. Innert Frist von 30 Tagen nach Zustellung hat der TC XX dem EDÖB mitzuteilen, ob seitens des TC XX irgendwelche Bemerkungen dazu vorliegen und ob der TC XX die Empfehlungen akzeptiert. Falls die Empfehlungen akzeptiert werden, lässt der TC XX innert derselben Frist dem EDÖB einen Vorschlag für die Regelung der Löschristen zukommen (vgl. Empfehlung Nr. 4). Für den Fall, dass der TC XX die Empfehlungen nicht akzeptiert oder umsetzt, kann der EDÖB die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen (Art- 29 Abs. 4 DSG).

In Anbetracht der Sensibilität der bearbeiteten Daten und der Reaktionen einiger Clubmitglieder ist die Notwendigkeit der Kontrolle des neuen Reservationssystems des TC XX in Bezug auf den Datenschutz offensichtlich. Die Feststellungen und Empfehlungen des EDÖB zeigen nun die Richtung auf, die andere private Betreiber von Freizeitanlagen bei der Umsetzung biometrischer Systeme einzuschlagen haben.

Aus besagten Gründen besteht ein grundsätzliches Interesse daran, die Öffentlichkeit für diese Art der Datenerhebung zu sensibilisieren und sie insbesondere über die erfolgte Datenschutzkontrolle beim TC XX und die diesbezüglichen Ergebnisse zu informieren. Gestützt auf Art. 30 Abs. 2 DSG wird der EDÖB daher den vorliegenden Kontrollbericht in einer angepassten und anonymisierten Version publizieren. Selbstverständlich erfolgt die Publikation unter dem Vorbehalt, dass keine aus Sicht des TC XX (und dem Systemlieferanten) vertraulichen Daten, welche Geschäftsgeheimnisse offenbaren oder die Konkurrenzfähigkeit beeinflussen könnten, bekannt gegeben werden. Der TC XX wird daher aufgefordert, den Schlussbericht auf solche vertraulichen Inhalte hin zu überprüfen und dem EDÖB mit Frist von 30 Tagen entsprechend schriftliche Rückmeldung zu erstatten.

4.2 Öffentlichkeitsprinzip

4.2.1 Empfehlung an das Bundesamt für Gesundheit: «Interessenerklärungen von Kommissionsmitgliedern»

Bern, den 12. Februar 2010

Empfehlung

gemäss

Art. 14 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung

zum Schlichtungsantrag von

X
(Antragstellerin)

gegen

Bundesamt für Gesundheit

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Die Antragstellerin (Journalistin) reichte beim Bundesamt für Gesundheit (BAG) am 18. Juni 2009 gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ, SR 152.3) ein Gesuch um Zugang zur «Déclaration complète des conflits d'intérêt»[1] der Mitglieder der Eidgenössischen

[1] Das Formular «Interessenerklärung für die Mitglieder der Eidgenössischen Kommission für Impffragen»/«Déclaration d'intérêts pour les membres de la commission fédérale pour les vaccinations» sind veröffentlicht auf der Site www.ekif.ch > Themen > Die Kommissionen > Unabhängigkeit

Impfkommission (EKIF) und der Arbeitsgruppe «Impfung gegen humane Papillomaviren» ein.

2. Das BAG lehnte mit Schreiben vom 17. Juli 2009 den Zugang zu den Interessenerklärungen mit der Begründung ab, dass «La Commission fédérale pour les vaccinations est une commission consultative. Au plan légal les commissions d'administration qui ont une fonction consultative ne tombent pas dans le champ d'application de la loi sur la transparence […] et leurs documents ne sont donc pas soumis non plus cette loi (…). Le Groupe de travail constitué pour l'élaboration du rapport 'Impfung gegen Papillomaviren (HPV)' étant un sous-groupe de la Commission fédérale pour les vaccinations avec des experts externes n'est de ce fait pas non plus soumis à la LTrans. S'agissant d'un document de la Commission, la déclaration complète des conflits d'intérêt n'est donc pas accessible.»

3. Am 17. Juli 2009 reichte die Antragstellerin beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) einen Schlichtungsantrag ein.

4. Auf Anfrage begründete das BAG dem Beauftragten mit Schreiben vom 5. August 2009 detailliert die Zugangsverweigerung. Es verwies u.a. darauf, dass es sich bei der EKIF «um eine beratende Verwaltungskommission im Sinne von Art. 8a der Regierungs- und Verwaltungsorganisationsverordnung (RVOV; SR 172.010.1) [handelt]. […] Die EKIF verfügt als beratende Kommission über keine Verfügungskompetenz. Gemäss den Ausführungen in der Botschaft zum Öffentlichkeitsgesetz[2] sind solche Kommissionen dem Öffentlichkeitsgesetz (BGÖ; SR 152.3) nicht unterstellt, fallen also nicht in den persönlichen Geltungsbereich des Gesetzes (Art. 2 BGÖ). In gleicher Weise äussert sich das Bundesamt für Justiz (BJ) in den erläuternden Dokumenten, die es bei der Einführung des Öffentlichkeitsgesetzes der Bundesverwaltung zur Verfügung gestellt hat (Häufig gestellte Fragen, S. 5/6)[3].» Bezüglich der Arbeitsgruppe «Impfung gegen humane Papillomaviren» hielt das BAG fest, dass neben Mitgliedern der EKIF zusätzliche externe Spezialisten aus dem Fachgebiet Einsitz nehmen. «Bezüglich Unterstellung unter das BGÖ muss für solche kommissionsinterne Arbeitsgruppen das Gleiche gelten wie für die EKIF. Da die EKIF nicht in den Geltungsbereich des BGÖ fällt, sind auch die von ihr erstellten bzw. empfangenen Dokumente nicht dem Öffentlichkeitsprinzip unterstellt und damit nicht zugänglich. Gemäss den erwähnten Ausführungen in der Botschaft zum BGÖ werden die Dokumente zugänglich, wenn sie an eine dem Gesetz unterstellte Behörde übermittelt worden sind. Das ist bei den von Ihnen verlangten Interessenerklärungen der Kommissionsmitglieder nicht der Fall. Die Erklärungen werden beim

[2] Botschaft zum Öffentlichkeitsgesetz vom 12. Februar 2003, BBl 2003 1986.
[3] http://intranet.bj.admin.ch/inbj-publ/bj/de/home/dienstleistungen/wissensmanagement/oeffprinzip.html (Stand: 12.2.2010)

Kommissionssekretariat aufbewahrt. Dieses ist dem BAG administrativ zugeordnet und wird in der Sektion Impfungen, Abteilung Übertragbare Krankheiten des Bereichs Öffentliche Gesundheit geführt. Nur falls das Kommissionssekretariat, das Präsidium oder mindestens drei Mitglieder der EKIF bezüglich der Unabhängigkeit eines Mitglieds Zweifel haben, wird der fragliche Fall dem Eidgenössischen Departement des Innern zur Beurteilung vorgelegt. Erst durch diese Weiterleitung käme die entsprechende Erklärung in den Besitz einer dem BGÖ unterstellten Behörde und eine eventuelle Herausgabe müsste dann nach den Regeln des BGÖ beurteilt werden. Ein solcher Fall ist bisher aber nicht eingetreten.»

5. Am 21. September 2009 reichte die Antragstellerin eine Rechtsverzögerungsbeschwerde beim Bundesverwaltungsgericht ein, weil der Beauftragte das Schlichtungsverfahren nicht innerhalb der vom Gesetz vorgesehenen 30 Tage durchgeführt hat.

6. Mit Urteil vom 16. Dezember 2009 (Ref. A-6032/2009) anerkannte das Bundesverwaltungsgericht die Rechtsverzögerung und lud den Beauftragten ein, bis Ende Januar 2010 ein Schlichtungsverfahren durchzuführen und eine Empfehlung zu erlassen.

7. Am 20. Januar 2010 führte der Beauftragte eine Schlichtungssitzung mit der Antragstellerin und zwei Vertretern des BAG durch. Dabei verwies der Beauftragte zum einen auf die Teilrevision der RVOV (Art. 8*a* ff. RVOV) sowie auf die Botschaft[4] zur Änderung des Parlamentsgesetzes, wonach ausserparlamentarische Kommissionen organisationsrechtlich zur dezentralen Bundesverwaltung gehören. Die Beteiligten vereinbarten, dass das BAG die Frage der Anwendbarkeit des Öffentlichkeitsgesetzes auf Verwaltungskommissionen nochmals prüft und – bei positiver Beantwortung der Frage – die betroffenen Personen gemäss Art. 11 BGÖ anhört.

8. Das BAG teilte in einer Stellungnahme zuhanden der Antragstellerin und des Beauftragten mit, dass es nach nochmaliger eingehender Prüfung an der Verweigerung der Herausgabe der verlangten Dokumente festhalte. Dabei wiederholte es seine Standpunkte in Bezug auf die Nichtanwendbarkeit des Öffentlichkeitsgesetzes auf die EKIF und die besagte Arbeitsgruppe (s. Ziffer I.4.). In Bezug auf den vom Beauftragten im Schlichtungsverfahren angeführten Hinweis auf die Änderung des Parlamentsgesetzes ändere sich nichts an dieser Beurteilung.

9. Auf Anfrage erklärte sich die Antragstellerin schriftlich damit einverstanden, dass diese Empfehlung auf Deutsch verfasst werden kann.

[4] BBl 2006 8009, 8012

II. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zieht in Erwägung:

A. Schlichtungsverfahren und Empfehlung gemäss Art. 14 BGÖ

1. Gemäss Art. 13 BGÖ kann eine Person einen Schlichtungsantrag beim Beauftragten einreichen, wenn die Behörde den Zugang zu amtlichen Dokumenten einschränkt, aufschiebt oder verweigert, oder wenn die Behörde innert der vom Gesetz vorgeschriebenen Frist keine Stellungnahme abgibt.

   Der Beauftragte wird nicht von Amtes wegen, sondern nur auf Grund eines schriftlichen Schlichtungsantrags tätig.[5] Berechtigt, einen Schlichtungsantrag einzureichen, ist jede Person, die an einem Gesuchsverfahren um Zugang zu amtlichen Dokumenten teilgenommen hat. Für den Schlichtungsantrag genügt einfache Schriftlichkeit. Aus dem Begehren muss hervorgehen, dass sich der Beauftragte mit der Sache befassen soll. Der Schlichtungsantrag muss innert 20 Tagen nach Empfang der Stellungnahme der Behörde schriftlich eingereicht werden.

2. Die Antragstellerin hat ein Zugangsgesuch nach Art. 10 BGÖ beim BAG eingereicht und eine ablehnende Antwort erhalten. Als Teilnehmerin an einem vorangegangenen Gesuchsverfahren ist sie zur Einreichung eines Schlichtungsantrags berechtigt. Der Schlichtungsantrag wurde formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Empfang der Stellungnahme der Behörde) beim Beauftragten eingereicht.

3. Das Schlichtungsverfahren kann auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten stattfinden. Die Festlegung des Verfahrens im Detail obliegt alleine dem Beauftragten.

   Kommt keine Einigung zu Stande oder besteht keine Aussicht auf eine einvernehmliche Lösung, ist der Beauftragte gemäss Art. 14 BGÖ gehalten, aufgrund seiner Beurteilung der Angelegenheit eine Empfehlung abzugeben.

[5] BBl 2003 2023

B. Sachlicher Geltungsbereich

1. Das BAG stellt bei seiner Zugangsverweigerung zum einen auf die Botschaft zum Öffentlichkeitsgesetz[6] ab. Darin heisst es, dass Verwaltungskommissionen, die gegenüber Bundesrat und Verwaltung beratende Funktionen haben, nicht in den Geltungsbereich des Öffentlichkeitsgesetzes fallen. Der Bundesverwaltung übermittelte Dokumente unterstehen indes dem Öffentlichkeitsgesetz. Zum anderen verweist das BAG auf das Dokument «Häufig gestellte Fragen»[7] des Bundesamtes für Justiz, welches in Bezug auf Verwaltungskommissionen festhält: «Sie zählen nicht zur Bundesverwaltung und erlassen keine Verfügungen; daher fallen sie selbst nicht in den Geltungsbereich des Öffentlichkeitsgesetzes.»

2. Demgegenüber vertritt Thomas Sägesser im Handkommentar zum Öffentlichkeitsgesetz[8] die Meinung, das Kriterium der beratenden Funktion für die Anwendbarkeit des Öffentlichkeitsgesetzes sei nicht entscheidend. Vielmehr rechnet er die Verwaltungskommissionen der Exekutivverwaltung zu, womit diese dem Öffentlichkeitsgesetz unterstehen.

3. Das Öffentlichkeitsgesetz findet in erster Linie Anwendung auf die Bundesverwaltung (Art. 2 Abs. 1 Bst. a BGÖ). Zum Bestand der Bundesverwaltung gehören nebst der so genannten zentralen Bundesverwaltung (wie Departemente, Bundeskanzlei, Generalsekretariate, Gruppen und Ämter der Departemente) auch die dezentralen Verwaltungseinheiten (Art. 2 des Regierungs- und Verwaltungsorganisationsgesetzes, RVOG, SR 172.010; Art. 6ff. RVOV). Es stellt sich daher die grundsätzliche Frage, ob Verwaltungskommissionen der (zentralen oder dezentralen) Bundesverwaltung zuzuordnen sind.

   Bei der EKIF handelt es sich um eine Verwaltungskommission mit beratender Funktion im Sinne von Art. 8a Abs. 2 RVOV. Im Anhang zur RVOV wird sie als gesellschaftsorientierte ausserparlamentarische Kommission qualifiziert.

   Ausserparlamentarische Kommissionen beraten den Bundesrat und die Bundesverwaltung ständig bei der Wahrnehmung ihrer Aufgaben (Art. 57a RVOG). Sie sind ihrer Funktion nach entweder Verwaltungs- oder Behördenkommissionen (Art. 8a Abs. 1 RVOV). Die Grenzen zwischen diesen beiden Kommissionen sind fliessend. Der Bundesrat führt dazu in seinem Bericht zum Anhang der RVOV aus: «Behördenkommissionen mit einer eng begrenzten Entscheidungskompetenz können Verwaltungskommissionen gegenüberstehen, die in gesellschaftlich brisanten Bereichen (z.B. Ethik(...), Genetik(...) und Strahlenschutz(...)) aufgrund von

[6] BBl 2003 1986

[7] Bundesamt für Justiz, «Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen», 29.06.06, Ziffer 2.4

[8] Thomas Sägesser, in: Brunner / Mader (Hrsg.), Stämpflis Handkommentar zum BGÖ, Art. 2, RZ 24

hochwertigem Spezialistenwissen einen sehr grossen Einfluss auf die Entscheidfindung besitzen»[9]. Gleiches gilt aus Sicht des Beauftragten für die EKIF. Ihre Mitglieder verfügen über ein hochwertiges Fachwissen und haben bedeutenden Einfluss auf die Entscheidfindung des BAG (konkret auf die Abteilung Übertragbare Krankheiten, Sektion Impfungen) in Sachen Impfempfehlungen.

Der Bundesrat hat in letzter Zeit verschiedentlich festgehalten, dass ausserparlamentarische Kommissionen organisationsrechtlich der dezentralen Bundesverwaltung zuzuordnen sind.[10] Dementsprechend hat er mit der Teilrevision der RVOV die ausserparlamentarischen Kommissionen systematisch dem «2. Kapitel: Die Verwaltung» zugeordnet. Gleichzeitig hat er mit Art. 8*f* RVOV eine Pflicht zur Offenlegung der Interessenbindungen für Kommissionsmitglieder statuiert. Vorliegend findet diese Bestimmung jedoch keine Anwendung, da die Offenlegungspflicht gemäss Übergangsbestimmungsartikel bis zu den Gesamterneuerungswahlen 2011 nur für Mitglieder neu eingesetzter ausserparlamentarischer Kommissionen gilt.

4. In Bezug auf die Qualifikation der Verwaltungskommissionen teilt der Beauftragte demzufolge die Meinung von Sägesser (s.o. II.B.2.). Die EKIF ist eine ausserparlamentarische Verwaltungskommission und als solche der *dezentralen* Bundesverwaltung zuzurechnen. Folglich gelangt vorliegend das Öffentlichkeitsgesetz zur Anwendung (Art. 2 Abs. 1 Bst. a BGÖ).

Demnach sind die Dokumente der EKIF und der Arbeitsgruppe «Impfung gegen humane Papillomaviren» sowie vorhandene Interessenerklärungen nach Massgabe der Bestimmungen des Öffentlichkeitsgesetzes grundsätzlich zugänglich.

5. Die Interessenerklärungen enthalten nebst den Daten der einzelnen Mitglieder auch Angaben zu jenen Personen (insbesondere Unternehmen aus der Pharmabranche), mit welchen die Mitglieder in Beziehung stehen (z.B. Beteiligungen, Beratertätigkeiten, Honorare für Expertisen, Kostenübernahme für Teilnahme an Kongressen[11]). Die Antragstellerin möchte Zugang zu allen Personendaten erwirken. Eine Anonymisierung, wie in Art. 9 Abs. 1 BGÖ vorgesehen, fällt somit nicht in Betracht. Gemäss Art. 9 Abs. 2 BGÖ beurteilt sich eine mögliche Bekanntgabe der Personendaten nach Art. 19 DSG. Vorliegend besteht weder eine gesetzliche

[9] Bericht des Bundesrates vom 12. Dezember 2008 «Der Anhang zur Regierungs- und Verwaltungsorganisationsverordnung (RVOV)»; in VPB 2009.6 (S. 57-89)

[10] s. Botschaft über die Neuordnung der parlamentarischen Kommissionen: «Da die ausserparlamentarischen Kommissionen für den Bundesrat oder die Bundesverwaltung tätig sind, werden sie zum Bestand der Bundesverwaltung gerechnet.» (BBl 2007 6641, 6651); sowie Botschaft zur Änderung des Parlamentsgesetzes: «Ausserparlamentarische Kommissionen gehören gemäss Artikel 6 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 19982 (RVOV) organisationsrechtlich zur dezentralen Bundesverwaltung.» (BBl 2006 8009, 8012)

[11] ausführliche Umschreibung auf dem Formular «Interessenerklärung für die Mitglieder der Eidgenössischen Kommission für Impffragen», s. Fussnote 1

Grundlage, welche die Datenbekanntgabe legitimieren würde, noch ist eine Ausnahme nach Art. 19 Abs. 1 lit. a-d DSG gegeben. Eine Bekanntgabe der Personendaten kann einzig im Rahmen von Art. 19 Abs. 1*bis* DSG erfolgen. Gemäss dieser Bestimmung kann eine Behörde gestützt auf das Öffentlichkeitsgesetz Personendaten dann bekannt geben, wenn diese im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen und wenn an deren Bekanntgabe ein überwiegendes öffentliches Interesse besteht.

6. In Ausnahmefällen kann trotz einer Beeinträchtigung der Privatsphäre der Zugang zu Dokumenten mit Personendaten gewährt (Art. 7 Abs. 2, zweiter Teilsatz BGÖ) und – da selbstredend eine Anonymisierung nicht möglich ist – Personendaten bekannt gegeben werden (Art. 19 Abs. 1*bis* DSG). Voraussetzung dafür ist allerdings, dass die Behörde im Rahmen der Interessenabwägung zum Schluss gelangt, dass das öffentliche Interesse am Zugang das Recht einer Drittperson auf Schutz ihrer Privatsphäre überwiegt (Art. 6 Abs. 1 der Verordnung über das Öffentlichkeitsprinzip der Verwaltung, Öffentlichkeitsverordnung, VBGÖ, SR 152.31). Für diese Güterabwägung liefert Art. 6 Abs. 2 VBGÖ Anhaltspunkte für jene Fälle, in denen ein überwiegendes öffentliches Interesse vorliegen kann. Ein öffentliches Interesse am Zugang kann namentlich überwiegen, wenn die Zugänglichmachung dem *Schutz der öffentlichen Gesundheit* dient (Art. 6 Abs. 1 Bst. b VBGÖ).

In Bezug auf das Interesse der betroffenen Personen am Schutz ihrer Privatsphäre kann festgehalten werden, dass die Offenlegung der Interessenerklärungen ein Bekanntwerden der Beziehungen zwischen den Mitgliedern der EKIF (und allfälliger Arbeitsgruppen) und wirtschaftlichen Unternehmen zur Folge hat. Aufgrund der Funktion der EKIF und insbesondere aufgrund der Qualität der betroffenen Daten gelangt der Beauftragte zur Ansicht, dass die Offenlegung dieser Kontakte lediglich als *geringfügiger Eingriff* in die Persönlichkeit der betroffenen Personen zu qualifizieren ist.

Den privaten Interessen der Betroffenen steht das Interesse der Bevölkerung gegenüber, weil der Zugang dem Schutz der öffentlichen Gesundheit dienen kann. Die EKIF ist sich bewusst, dass ihre Impfempfehlungen einen wichtigen Einfluss auf die öffentliche Gesundheit haben. Daher erachtet sie es als notwendig, «mit geeigneten Massnahmen sicherzustellen, dass die Prüfung der Erwägungen, die diesen Empfehlungen zu Grunde liegen, unabhängig und ohne direkten oder indirekten Druck erfolgt.»[12] Damit bringt sie zum Ausdruck, welche Bedeutung sie selber den Interessenabklärungen hinsichtlich der Unabhängigkeit ihrer Mitglieder beimisst. Vorliegend geht es nicht nur um ein *allgemeines* öffentliches Interesse an Transparenz in der Verwaltung. Vielmehr besteht ein zum Schutz der öffentlichen

[12] http://www.bag.admin.ch/ekif/04419/04422/index.html?lang=de (Stand: 12.2.2010)

Gesundheit *spezifisches* Interesse der Bevölkerung zu wissen, ob und welche Interessenbeziehungen zwischen den Mitgliedern der EKIF (bzw. der besagten Arbeitsgruppe) und der Pharmaindustrie bestehen. Einerseits haben Impfempfehlungen direkt Einfluss auf die Gesundheit der gesamten Bevölkerung. Anderseits kann zwischen den Empfehlungen der EKIF und der Verwendung bestimmter Impfprodukte einzelner Unternehmen eine Wechselwirkungen bestehen. Durch die Offenlegungen der Interessenklärungen der Mitglieder der EKIF (bzw. allfälliger Arbeitsgruppen) wird für die Bevölkerung erkennbar, ob und insbesondere welche Beziehungen bestehen. Dies erlaubt ihr auch eine Beurteilung der Unabhängigkeit der EKIF.

Nach summarischer Prüfung gelangt der Beauftragte daher zum Schluss, dass zum Schutz der öffentlichen Gesundheit ein berechtigtes und überwiegendes öffentliches Interesse daran besteht zu erfahren, ob und welche Beziehungen zwischen den Mitgliedern der EKIF (bzw. der Arbeitsgruppe «Impfung gegen humane Papillomaviren») und Pharmaunternehmen existieren.

7. Der Beauftragte empfiehlt dem BAG, die betroffenen Personen (Mitglieder der EKIF und der Arbeitsgruppe sowie die auf den Interessenklärungen aufgeführten natürlichen und juristischen Personen) gemäss Art. 11 BGÖ anzuhören, sofern es die Gewährung des Zugangs in Betracht zieht.

III Aufgrund dieser Erwägungen empfiehlt der Datenschutz- und Öffentlichkeitsbeauftragte:

1. Nach Anhörung der betroffenen Personen (Art. 11 BGÖ) gewährt das Bundesamt für Gesundheit den Zugang zu den Interessenerklärungen der Mitglieder der EKIF und – sofern vorhanden – zu denjenigen der Arbeitsgruppe «Impfung gegen humane Papillomaviren».

2. Das Bundesamt für Gesundheit erlässt eine Verfügung nach Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG, SR 172.021), wenn es in Abweichung von Ziffer 1 den Zugang nicht gewähren will.

   Das Bundesamt für Gesundheit erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung (Art. 15 Abs. 3 BGÖ).

3. Die Antragstellerin kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Bundesamt für Gesundheit den Erlass einer Verfügung nach Artikel 5 VwVG verlangen, wenn sie mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

4. Gegen die Verfügung kann die Antragstellerin beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

5. Diese Empfehlung wird veröffentlicht. Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten wird der Name der Antragstellerin anonymisiert (Art. 13 Abs. 3 VBGÖ).

6. Die Empfehlung wird eröffnet:

   - X
   - Bundesamt für Gesundheit

     3003 Bern

Hanspeter Thür

4.2.2 Empfehlung an das Bundesamt für Sozialversicherungen: «IV-Checkliste» (I)

Bern, den 16. März 2010

Empfehlung

gemäss

Art. 14 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung

zum Schlichtungsantrag von

Y
(Antragsteller)

gegen

Bundesamt für Sozialversicherung (BSV)

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Der Antragsteller (Anwalt) reichte gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ, SR 152.3) am 11. September 2008 beim Bundesamt für Sozialversicherung (BSV) ein Gesuch um Zugang zur IV-Checkliste ein. Der Antragsteller hat von der Existenz dieses Dokumentes aufgrund von Berichterstattungen in der Presse Kenntnis erhalten.

2. Das BSV hat mit Schreiben vom 29. September 2008 dem Antragssteller den Zugang zum fraglichen Dokument verweigert. Es teilte ihm mit, dass «Das verlangte Dokument […] unter eine der vom Öffentlichkeitsgesetz vorgesehenen Ausnahmebestimmungen (Art. 7 BGÖ) [fällt]. Würde der Zugang gewährt, so würde die zielkonforme Durchführung einer konkreten behördlichen Massnahme beeinträchtigt (Art. 7 Abs. 1 Bst. b BGÖ). Insbesondere würden eine effektive Missbrauchsbekämpfung nach Art. 59 Abs. 5 IVG sowie die Abklärung der versicherungsmässigen Voraussetzungen nach Art. 57 Abs. 1 Bst. c IVG stark gefährdet.»

3. Mit Schreiben vom 07. Oktober 2008 reichte der Antragsteller beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (nachfolgend Beauftragter) einen Schlichtungsantrag gemäss Art. 13 BGÖ ein. Er machte geltend, dass die Begründung des BSV nicht stichhaltig sei, und betonte u.a., dass das Öffentlichkeitsgesetz die Transparenz fördere und damit das Vertrauen der Bevölkerung in die Verwaltung stärke. Zudem vertrat der Antragssteller die Ansicht, dass die Ausnahmebestimmungen nach Art. 7 BGÖ restriktiv gehandhabt werden müssten, damit das Öffentlichkeitsgesetz nicht zum Papiertiger verkomme.

4. Auf Aufforderung des Beauftragten hin reichte das BSV am 17. Oktober 2008 eine Stellungnahme sowie die IV-Checkliste ein.

   Die IV-Checkliste des BSV enthält einen Abschnitt A mit dem Titel «Allgemeine Angaben» über einen Versicherten und einen Abschnitt B mit dem Titel «Bewertung». Dieser besteht aus einem standardisierten Fragenkatalog mit 19 so genannten Risikofaktoren, welche mit einer bestimmten Punktzahl gewichtet werden. Der Sachbearbeiter trägt je nach Aussage des Versicherten bei jedem Risikofaktor die vorgegebene Punktzahl in der Ja-Spalte ein.

   In seiner Stellungnahme führte das BSV aus, dass die Invalidenversicherung seit der 5. IV-Revision neu die Kompetenz habe, Spezialistinnen und Spezialisten für die Bekämpfung des ungerechtfertigten Leistungsbezuges beizuziehen. Das BSV wies u.a. darauf hin, dass die IV-Checkliste ein wichtiges Element in Rahmen der Bekämpfung des Versicherungsbetruges in der Invalidenversicherung darstelle. Sie sei zusammen mit einem Konzept und Weisungen den kantonalen IV-Stellen zugestellt worden. In dem dreistufigen Konzept gehe es in der ersten Phase darum, «von der Gesamtheit von gegenwärtig 300'000 Rentenbezügern bzw. Antragsstellern, eine Gruppe von Versicherten auszuscheiden, bei der Hinweise für einen Anfangsverdacht betreffend eines Versicherungsbetruges vorliegen. Das entsprechende Arbeitsinstrument dazu ist die Checkliste. Nur mit einer solchen Vorausscheidung kann das Arbeitsvolumen bewältigt werden. Wird mittels der Checkliste ein Total von mindestens 20 Punkten erreicht, so wird der Fall IV-intern an

BVM(-)-Spezialisten weitergeleitet, welche darüber entscheiden ob und allenfalls welche weiteren Ermittlungen durchzuführen sind.»

Das BSV führt weiter aus, dass «Die Checkliste […] bereits in den Privatversicherungsunternehmen ein bewährtes Hilfsmittel zur Sensibilisierung und Unterstützung der Sachbearbeiter hinsichtlich Missbrauchserkennung [ist]. Das konsequente und sorgfältige Anwenden der Checkliste ermöglicht frühzeitig eine effiziente und zielgerichtete Dossierprüfung und sie unterstützt die Sachbearbeitenden der IV-Stellen bei der Entscheidfindung, ob es sich allfällig um einen möglichen Betrugsfall handeln könnte. Auf Grund der Erfahrung in der Privatassekuranz kann davon ausgegangen werden, dass die IV-Checkliste ihre Wirksamkeit in der Triagierung verlieren wird, wenn sie der Öffentlichkeit zugänglich gemacht wird. Denn sobald die einzelnen Kriterien und ihre Gewichtungen gemäss Checkliste öffentlich bekannt sind, werden gesuchstellende Versicherte mit unlauteren Absichten ihr Verhalten und ihre Angaben so anpassen und verändern, dass damit die heute mögliche Triage wirkungslos wird. Aus diesem Grund muss der Zugang zur gesamten Checkliste verweigert bleiben.»

5. Weitere Informationen zur IV-Checkliste sowie zum Konzept der Missbrauchsbekämpfung finden sich auf der Webseite des BSV, beispielsweise im «Faktenblatt Betrugsbekämpfung in der Invalidenversicherung»[1] sowie in den Medienmitteilungen vom 20. April 2009 und vom 27. August 2009[2].

   In der vom BSV herausgegebenen Zeitschrift «Soziale Sicherheit CHSS» werden neben der Beschreibung des Konzeptes auch einzelne Risikofaktoren aus der IV-Checkliste bekannt gegeben, so häufiger Arztwechsel, widersprüchliche Krankengeschichte (Anamnese), objektive Falschangaben der versicherten Person und Migrationshintergrund[3].

6. Von den Medien wurden folgende Risikofaktoren und Bewertungen der IV-Checkliste im Jahr 2008 und 2009 veröffentlicht:

   - In der Sendung «Rendez-vous» des Schweizer Radio DRS[4] vom 09. September 2008 und in den Nachrichtensendungen des Schweizer Fernsehens SF[5] vom 09. September 2008 war die IV-Checkliste Thema. Dabei wurde der Risikofaktor Migrationshintergrund bekannt. Auf der Webseite des Radiosenders wird zudem erwähnt, dass die Checkliste dem Radio DRS vorliege.

[1] www.news-service.admin.ch/NSBSubscriber/message/de/28710
[2] www.bsv.admin.ch/dokumentation/medieninformationen/01429/index.html?lang=de
[3] www.bsv.admin.ch > Dokumentation > Publikationen >Soziale Sicherheit CHSS; Beitrag Betrugsbekämpfung in der Invalidenversicherung – eine Standortbestimmung, in: CHSS 3/2009, S. 168 ff.
[4] http://www.drs.ch/www/de/drs/sendungen/rendez-vous/2753.bt10048530.html
[5] www.tagesschau.sf.tv/Nachrichten/Archiv/2008/09/09/Schweiz/Stellt-die-IV-Auslaender-unter-Generalverdacht www.sf.tv/sendungen/10vor10/index.php?docid=20080909

- In der Zeitung Bund[6] wird der Risikofaktor Migrationshintergrund und dessen Bewertung mit 3 Punkten sowie die Risikofaktoren Simulation und Hinweise auf Missbrauch sowie deren Bewertung mit je 20 Punkten bekannt.
- In der Online-Ausgabe der Zeitung 20min[7] werden die Risikofaktoren Mirgrationshintergrund mit der Bewertung von 3 Punkten, Schleudertrauma mit der Bewertung von 5 Punkten, widersprüchliches Krankheitsbild mit der Bewertung von 10 Punkten, sowie Hinweis auf Missbrauch oder Simulation mit der Bewertung von je 20 Punkten bekannt.

7. Die IV-Checkliste war auch Gegenstand einer parlamentarischen Anfrage (08.1108 Anfrage Schenker)[8]. In seiner Antwort erwähnt der Bundesrat, dass die Liste 19 Risikofaktoren umfasse und eine vertiefte Abklärung des Falls erst erfolge, wenn eine Punktzahl von insgesamt 20 Punkten erreicht werde. Bekannt werden die Risikofaktoren Migrationshintergrund und dessen Bewertung mit 3 Punkten, unverhältnismässiger Arztwechsel, widersprüchliche Krankengeschichte (Anamnese) sowie objektive Falschangaben der versicherten Person.

8. Zusammenfassend kann festgehalten werden, dass folgende Fakten gegenwärtig öffentlich bekannt sind:

   - Das BSV publizierte in seiner Zeitschrift «Soziale Sicherheit», dass die Invalidenversicherung eine Checkliste mit rund 20 unterschiedlichen Risikofaktoren einsetzt. Dabei wurden die Risikofaktoren 1, 3.3, 4.2 und 5.4 genannt. Die Zeitschrift ist ein Publikationsorgan[9] im Sinne von Art. 6 Abs. 3 BGÖ und ist auf der Webseite des BSV veröffentlicht.
   - Der Bundesrat gibt in seiner Antwort zur parlamentarischen Anfrage 08.1108 die Risikofaktoren 1, 3.3, 4.2 und 5.4 bekannt. Er informiert auch darüber, dass der Risikofaktor 5.4 drei Punkte aufweist und eine vertiefte Abklärung erst vorgenommen wird, wenn anhand der Checkliste ein Total von mindestens 20 Punkten erreicht wird.
   - In diversen Medien wurde der Risikofaktor 5.4 und dessen Bewertung mit 3 Punkten publiziert. Zudem wurde der Sprecher des BSV[10] zitiert, wonach die Risikofaktor 2 und 3.1 mit je 20 Punkten, der Risikofaktor 3.5 mit 5 Punkten sowie der Risikofaktor 3.3 mit 10 Punkten bewertet werden.

[6] Der Bund, 10.09.2008
[7] www.20min.ch/print/story/27108380
[8] www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20081108
[9] Pascal Mahon/Olivier Gonin, in: Brunner/Mader, (Hrsg.), Handkommentar zum BGÖ, Art. 6 Rz 65
[10] www.20min.ch/print/story/27108380; Der Bund, 10.09.2008

- Gemäss Medienbericht verwendet die IV-Stelle Bern in der Bekämpfung des Versicherungsbetruges diese Checkliste nicht generell. Zudem betrachtet sie die Prüfung jedes Einzelfalls anhand der Liste als zu aufwendig[11].

II. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zieht in Erwägung:

A. Schlichtungsverfahren und Empfehlung gemäss Art. 14 BGÖ

1. Gemäss Art. 13 BGÖ kann eine Person einen Schlichtungsantrag beim Beauftragten einreichen, wenn die Behörde den Zugang zu amtlichen Dokumenten einschränkt, aufschiebt oder verweigert, oder wenn die Behörde innert der vom Gesetz vorgeschriebenen Frist keine Stellungnahme abgibt.

   Der Beauftragte wird nicht von Amtes wegen, sondern nur auf Grund eines schriftlichen Schlichtungsantrags tätig[12]. Berechtigt, einen Schlichtungsantrag einzureichen, ist jede Person, die an einem Gesuchsverfahren um Zugang zu amtlichen Dokumenten teilgenommen hat. Für den Schlichtungsantrag genügt einfache Schriftlichkeit. Aus dem Begehren muss hervorgehen, dass sich der Beauftragte mit der Sache befassen soll. Der Schlichtungsantrag muss innert 20 Tagen nach Empfang der Stellungnahme der Behörde schriftlich eingereicht werden.

2. Der Antragsteller hat ein Zugangsgesuch nach Art. 10 BGÖ beim BSV eingereicht und eine ablehnende Antwort erhalten. Als Teilnehmer an einem vorangegangenen Gesuchsverfahren ist er zur Einreichung eines Schlichtungsantrags berechtigt. Der Schlichtungsantrag wurde formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Empfang der Stellungnahme der Behörde) beim Beauftragten eingereicht.

3. Das Schlichtungsverfahren kann auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten stattfinden. Die Festlegung des Verfahrens im Detail obliegt alleine dem Beauftragten.[13]

   Kommt keine Einigung zu Stande oder besteht keine Aussicht auf eine einvernehmliche Lösung, ist der Beauftragte gemäss Art. 14 BGÖ gehalten, aufgrund seiner Beurteilung der Angelegenheit eine Empfehlung abzugeben.

B. Sachlicher Geltungsbereich

1. Das Öffentlichkeitsgesetz schreibt die Vermutung des freien Zugangs zum amtlichen Dokument fest (Art. 6 Abs. 1 BGÖ). Wenn die angefragte Behörde den Zugang

[11] Der Bund, 10.09.2008
[12] BBl 2003 2023
[13] BBl 2003 2024

aufschiebt, einschränkt oder verweigert, muss sie begründen, welche der Ausnahmen der Art. 7 und 8 BGÖ vorliegen. Die abschliessend aufgezählten Ausnahmebestimmungen sind durch unbestimmte Rechtsbegriffe geprägt[14]. Gemäss Art. 12 Abs. 4 BGÖ wird die Behörde aber angewiesen, *summarisch* die Verweigerung, die Einschränkung oder den Aufschub des Zugangs zu begründen. Auch die Botschaft verlangt die Begründung von negativen Stellungnahmen[15]. Insofern trägt die Behörde die Beweislast zur Widerlegung der Vermutung auf den Zugang zu amtlichen Dokumenten[16]. Demzufolge ist erforderlich, dass Behörden bei einer ablehnenden Stellungnahme nicht bloss den Wortlaut der Ausnahmebestimmung des Öffentlichkeitsgesetzes wiedergeben, sondern ihren Entscheid in einer Weise motivieren, die es der antragstellenden Person erlaubt, den Entscheid zumindest in den Grundzügen nachzuvollziehen[17].

Das BSV verweigerte dem Antragssteller den Zugang zur IV-Checkliste, indem es lediglich die Ausnahmebestimmung nach Art. 7 Abs. 1 Bst. b BGÖ (Beeinträchtigung der zielkonformen Durchführung konkreter behördlicher Massnahmen) wiedergegeben und auf die IV- Bestimmungen Art. 57 Abs. 1 Bst. c IVG (Prüfung der versicherungsmässigen Voraussetzungen des Leistungsbezugs) sowie Art. 57 Abs. 1 Bst. c IVG (Einsetzung von Spezialisten für die Bekämpfung des ungerechtfertigten Leistungsbezugs) verwiesen hat.

Der Beauftragte kommt zum Schluss, dass die Stellungnahme des BSV den Anforderungen einer summarischen Begründung gemäss Art. 12 Abs. 4 BGÖ nicht genügt.

2. Eine wirksame Missbrauchsbekämpfung im Versicherungsbereich ist im öffentlichen Interesse[18]. Eine entsprechende gesetzliche Grundlage für die Bekämpfung nicht geschuldeter Leistungen mit Hilfe des Einsatzes von Spezialisten ist in der Invalidenversicherung vorhanden[19]. Es ist wichtig hervorzuheben, dass es im vorliegenden Schlichtungsverfahren nicht um eine Bewertung des Inhaltes oder der Tauglichkeit der IV-Checkliste als Instrument der Missbrauchsbekämpfung geht, sondern einzig um die Beurteilung, *ob und in welchem Umfang der Zugang zu dieser Liste gemäss Öffentlichkeitsgesetz* gewährt werden kann.

3. Das Öffentlichkeitsgesetz dient der Transparenz der Verwaltung und soll das Vertrauen des Bürgers in die staatlichen Institutionen und ihr Funktionieren fördern.

[14] Stephan C. Brunner, Interessenabwägung im Vordergrund, digma 4/2004, S. 163
[15] BBl 2003 2023
[16] Pascal Mahon/Olivier Gonin, in: Brunner/Mader, (Hrsg.), Handkommentar zum BGÖ, Art. 6 Rz 11; BBl 2003 2002
[17] Empfehlung BFM / Kriterienliste Safe Countries vom 30. Juli 2007, Ziffer II.B.1.
[18] so auch das BGE 8C 239 / 2008 Erw. 6.4.1 mit Verweisen
[19] Art. 59 Abs. 5 IVG

Es bildet eine wesentliche Voraussetzung für eine sinnvolle demokratische Mitwirkung am politischen Entscheidfindungsprozess und für eine wirksame Kontrolle staatlicher Behörden[20]. Das Öffentlichkeitsgesetz gibt grundsätzlich jeder Person das Recht, Einsicht in amtliche Dokumente des Bundes und Auskünfte über den Inhalt amtlicher Dokumente zu erhalten (Art. 6 Abs. 1 BGÖ). Der Gesetzgeber hat in Art. 7 BGÖ abschliessend neun Ausnahmebestimmungen vorgesehen, aufgrund welcher der Zugang zu einem Dokument eingeschränkt, aufgeschoben oder verweigert werden kann. Davon schützen sechs öffentliche Interessen (Abs. 1 Bst. a-f) und drei private Interessen (Abs. 1 Bst. g-h und Abs. 2). In Art. 8 BGÖ sind die besonderen Fälle aufgelistet, in denen das Recht auf Zugang zu amtlichen Dokumenten unmittelbar durch das Gesetz verwehrt (Abs. 1-4) oder gewährt (Abs. 5) wird.

4. Ob ein Geheimhaltungsgrund nach Art. 7 Abs. 1 BGÖ wirksam ist, hängt *nich*t von einer Abwägung der Interessen der Verwaltung an der Geheimhaltung und des Interesses des Gesuchstellers auf Zugang ab. Der Gesetzgeber hat diese Interessenabwägung bereits vorweggenommen, indem er in Art. 7 Abs. 1 BGÖ abschliessend die Fälle der überwiegenden öffentlichen oder privaten Interessen aufzählt, welche das öffentliche Interesse auf Zugang überwiegen[21]. Eine solche Abwägung darf die Behörde nur im Fall von Art. 7 Abs. 2 BGÖ vornehmen, falls ein Dokument Personendaten enthält, die nicht anonymisiert werden können[22]. Der im Öffentlichkeitsgesetz verankerte Schutzmechanismus von Geheimhaltungsinteressen beruht nach Art. 7 Abs. 1 BGÖ einzig auf dem Bestehen oder Nichtbestehen eines Schadensrisikos. Dabei müssen kumulativ folgende zwei Bedingungen vorliegen: Erstens das von der Behörde geltend gemachte Interesse (Bst. a-f) wird durch die Offenlegung erheblich beeinträchtigt, und zweitens besteht ein ernsthaftes Risiko, dass die Beeinträchtigung eintritt[23]. Ist eine Beeinträchtigung lediglich denkbar oder im Bereich des Möglichen, darf der Zugang nicht verweigert werden. Damit die Ausnahme wirksam wird, muss der Schaden «nach dem üblichen Lauf der Dinge» mit hoher Wahrscheinlichkeit eintreffen. Im Zweifelsfall ist der Zugang zu gewähren[24].

5. Falls ein amtliches Dokument aus der Sicht der Behörde Informationen enthält, deren Bekanntwerden ein Schadensrisiko beinhaltet, bedeutet das nicht, dass das ganze Dokument oder bestimmte Informationen daraus unbesehen und stets als

[20] BGE 133 II 209 Erw.2.3.1

[21] Bertil Cottier/Rainer J. Schweizer/Nina Widmer, in: Brunner/Mader, (Hrsg.), Handkommentar zum BGÖ, Art. 7 Rz. 5

[22] Art. 7 Abs. 2 BGÖ, Art. 9 BGÖ und Art. 6 VBGÖ

[23] Bertil Cottier/Rainer J. Schweizer/Nina Widmer, in: Brunner/Mader, (Hrsg.), Handkommentar zum BGÖ, Art. 7 Rz 4

[24] Bertil Cottier/Rainer J. Schweizer/Nina Widmer, in: Brunner/Mader, (Hrsg.), Handkommentar zum BGÖ, Art. 7 Rz 4.; BBl 2003 2009, Empfehlung vom 29. August 2008, Ziffer II.B.4; Stephan C. Brunner, Interessenabwägung im Vordergrund, digma 4/2004, S. 162

Ausnahmefall nach Art. 7 BGÖ zu betrachten sind. Vielmehr müssen die fraglichen Passagen «ein gewisses Gewicht»[25] aufweisen, um überhaupt eine reelle Beeinträchtigung der angerufenen Interessen hervorrufen zu können. Die Behörde ist verpflichtet, bei jeder Gesucherteilung das Verhältnismässigkeitsgebot[26] zu beachten. Es verlangt im Falle einer Beschränkung, immer die mildeste mögliche Variante zu wählen[27]. Die Behörde hat demnach durch Güterabwägung zu prüfen, ob anstelle einer vollkommenen Verweigerung das amtliche Dokument teilweise zugänglich gemacht werden kann, oder ob allenfalls ein Aufschub in Frage kommt.

6. Die IV-Checkliste enthält keine Personendaten[28]. Sie ist ein *standardisierter* Fragenkatalog, weshalb ihre Herausgabe die Privatsphäre eines Dritten nicht beeinträchtigt. Demnach ist Art. 7 Abs. 2 BGÖ nicht anwendbar, die Interessenabwägung zwischen öffentlichen Interessen auf Herausgabe und privaten Interessen auf Wahrung der Privatsphäre Dritter entfällt.

7. Wie oben ausgeführt (siehe oben I./5 bis I./7) wurden Teile des standardisierten Fragenkataloges bereits veröffentlicht. Das BSV verweigert jedoch den Zugang zur IV-Checkliste in seiner Gesamtheit. Es argumentiert, die Veröffentlichung hätte eine hohe Gefährdung von behördlichen Massnahmen zur Folge.

   Nach Ansicht des Beauftragten ist dies widersprüchlich, weil das BSV Teile des Fragenkatalogs aktiv[29] bekannt gegeben hat (so sind sieben der 19 Risikofaktoren öffentlich bekannt sind, teilweise sogar mit ihrer Bewertung. Bei diesen Risikofaktoren und deren Gewichtungen besteht somit keine Geheimhaltungsinteresse mehr, womit die Einschätzung des Schadensrisikos hier nicht mehr relevant ist. Deshalb kann sich das BSV nicht auf die Ausnahme nach Art. 7 Abs. 1 Bst. b BGÖ berufen.

   Der Beauftragte kommt daher zum Schluss, dass der Zugang zu den bekannten Risikofaktoren 1, 2, 3.1, 3.3, 3.5, 4.2 und 5.4 ebenso wie zu den bekannten Bewertungszahlen der Risikofaktoren 2, 3.1, 3.3, 3.5 und 5.4 nicht verweigert werden darf. Auch darf der Zugang zu den bereits veröffentlichten Informationen, wonach es 19 Kriterien gibt und beim Erreichen von 20 Punkten der Fall an den Spezialisten überwiesen wird, nicht verweigert werden.

8. Zu prüfen bleibt, ob der Zugang zu den noch nicht bekannten Risikofaktoren bzw. Informationen gewährt werden kann.

[25] Votum Bundesrat Blocher, Amtliches Bulletin, Art. 7, 2004 N 1262
[26] Urteil des Bundesverwaltungsgerichtes vom 15. September 2009, A-3631/2009, Erw.2.6, Erw. 3.4.1, Erw. 3.5.1 und Erw. 4.; BGE 133 II 209 Erw. 2.3.3
[27] Bundesamt für Justiz, Leitfaden Gesuchsbeurteilung und Checkliste, Ziffer 2.4
[28] Art. 3 Bst. a DSG
[29] Pascal Mahon/Olivier Gonin, in: Brunner/Mader, (Hrsg.), Handkommentar zum BGÖ, Art. 6 Rz 62 ff.

9. Im Abschnitt A «Allgemeine Angaben» sind Rubriken wie z.B. AHV-Nummer, Teilerwerbstätigkeit, Arbeitnehmer oder Selbstständigerwerbender aufgelistet. Der Sachbearbeiter füllt sie im Einzelfall mit Angaben des Versicherten aus. Es ist nicht ersichtlich, weshalb diese Rubriken nicht bekannt gegeben werden können. Auch sind die Angaben am Schluss des Dokuments allgemeiner Natur (Datum, Fallbearbeiter etc.) und können bekannt gegeben werden.

10. In Bezug auf Abschnitt B «Bewertung», der den standardisierten Fragenkatalog (eigentliche Checkliste) enthält, beruft sich das BSV auf die Ausnahmebestimmung Art. 7 Abs. 1 Bst. b BGÖ. Diese Norm ermöglicht die *Geheimhaltung der Durchführung* einer Massnahme, während Bst. a, sich auf die *Geheimhaltung der Vorbereitung einer Massnahme*, d.h. der Meinungs- und Willensbildung bezieht. Geschützt werden durch Bst. b die Vorkehrungen, welche die Behörden treffen, um ihre Ziele zu erreichen. Die Geheimhaltung dieser Vorkehrungen muss der Schlüssel zu ihrem Erfolg darstellen[30]. Mit andern Worten muss das Bekanntwerden der konkreten behördlichen Massnahme dazu führen, dass die Behörde ihr Ziel «'nach dem gewöhnlichen Lauf der Dinge' mit hoher Wahrscheinlichkeit»[31] nicht mehr im gesetzten Rahmen erreichen kann. Diese Geheimhaltungsnorm schützt in erster Linie Ermittlungen, Inspektionen, administrative Überwachungen (die vor allem im Steuer- und Zollbereich sowie im Bereich der sozialen Sicherheit zahlreich sind) und behördliche Aufklärungskampagnen[32].

11. Entscheidend für das Vorliegen des Ausnahmegrundes von Art. 7 Abs. 1 Bst. b BGÖ ist, ob durch das Bekanntwerden des standardisierten Fragekatalogs (Risikofaktoren) erstens eine Triage der möglichen Missbrauchsfälle und zweitens eine effiziente und zielgerichtete Dossierbehandlung mit hoher Wahrscheinlichkeit nicht mehr möglich ist.

12. Mit dem standardisierten Fragenkatalog soll nach dem dreistufigen Konzept des BSV in einer ersten Phase die Gruppe von Versicherten mit Betrugsverdacht herausgefiltert werden (Triage): Er dient laut BSV den IV-Sachbearbeitern zur Sensibilisierung der Missbrauchserkennung und Entscheidung, ob ein Fall intern den Spezialisten weitergeleitet werden soll. Er soll gemäss BSV «frühzeitig eine effiziente und zielgerichtete Dossierprüfung» ermöglichen, weil «Nur mit einer solchen Vorausscheidung […] das Arbeitsvolumen bewältigt werden» [kann].

13. Das BSV hat in seiner Stellungnahme als Begründung lediglich auf die Ausnahmebestimmung Art. 7 Abs. 1 Bst. b BGÖ verwiesen und pauschal festgehalten: «Auf

[30] Bertil Cottier/Rainer J. Schweizer/Nina Widmer, in: Brunner/Mader, (Hrsg.), Handkommentar zum BGÖ, Art. 7 Rz 23 f.

[31] Stephan C. Brunner, Interessenabwägung im Vordergrund, digma 4/2004, S. 163

[32] Bertil Cottier/Rainer J. Schweizer/Nina Widmer, in: Brunner/Mader, (Hrsg.), Handkommentar zum BGÖ, Art. 7 Rz 25; A-3631/2009 Erw.2.2

Grund der Erfahrung in der Privatassekuranz kann davon ausgegangen werden, dass die IV-Checkliste ihre Wirksamkeit in der Triagierung verlieren würde, wenn sie der Öffentlichkeit zugänglich gemacht wird. Denn sobald die einzelnen Kriterien und ihre Gewichtungen gemäss Checkliste öffentlich bekannt sind, werden gesuchstellende Versicherte mit unlauteren Absichten ihr Verhalten und ihre Angaben so anpassen und verändern, dass damit die heute mögliche Triage wirkungslos wird.»

14. Es ist für den Beauftragten aufgrund der Ausführungen des BSV nicht nachvollziehbar, inwiefern aufgrund der Veröffentlichung der einzelnen Risikofaktoren und deren Gewichtung eine Triage wirkungslos werden sollte. Ein Teil der Risikofaktoren, immerhin sieben von 19, sind bereits publiziert worden. Das BSV hat nicht geltend gemacht, dass diese von ihm (bekannt gemachten) Veröffentlichungen negative Auswirkungen auf die Triage gehabt haben.

15. Vom standardisierten Fragebogen, den der Sachbearbeiter zum Zeitpunkt der Triage (d.h. der Vorausscheidung von mutmasslichen Missbrauchsfällen) einsetzt, ist die konkrete Vorbereitung einer Massnahme im Einzelfall (Einleitung eines Ermittlungsverfahrens) zu unterscheiden, wie beispielsweise die Bekanntgabe von Ermittlungsmethoden oder die Tatsache einer laufenden Ermittlung. Hier wäre aus der Sicht des Beauftragten die Überführung einer Person wegen Verdacht auf Versicherungsbetrug sehr wohl gefährdet. Vorliegend steht jedoch ein standardisierter Fragebogen, der als *Arbeitsinstrument und Hilfsmittel* dient, im Mittelpunkt.

16. Aus Sicht des Beauftragten ist nicht mit hoher Wahrscheinlichkeit davon auszugehen, dass der standardisierte Fragenkatalog nach der Zugänglichmachung nicht mehr der Sensibilisierung der Sachbearbeiter dienen könnte und als Arbeitsinstrument einsetzbar wäre. Es ist nicht davon auszugehen, dass eine effiziente Triage in der Missbrauchserkennung erheblich beeinträchtigt und von einem ernsthaften Schadensrisiko auszugehen ist, weil das BSV die IV-Checkliste nicht zurückgezogen hat und die IV-Stellen diese weiterhin als Arbeitsinstrument verwenden.

    Der Beauftragte kommt daher zum Schluss, dass der Zugang zum gesamten Dokument nicht verweigert werden darf.

III. Aufgrund dieser Erwägungen empfiehlt der Datenschutz- und Öffentlichkeitsbeauftragte:

1. Das Bundesamt für Sozialversicherung gewährt den Zugang zur IV-Checkliste.

2. Das Bundesamt für Sozialversicherung erlässt eine Verfügung nach Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG, SR 172.021), wenn es in Abweichung von Ziffer 1 den Zugang nicht gewähren will.

   Das Bundesamt für Sozialversicherung erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung (Art. 15 Abs. 3 BGÖ).

3. Der Antragsteller kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Bundesamt für Sozialversicherung den Erlass einer Verfügung nach Artikel 5 VwVG verlangen, wenn er mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

4. Gegen die Verfügung kann der Antragsteller beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

5. Diese Empfehlung wird veröffentlicht. Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten wird der Name der Antragsteller anonymisiert (Art. 13 Abs. 3 VBGÖ).

6. Die Empfehlung wird eröffnet:

   - X
   - Bundesamt für Sozialversicherung

     3003 Bern

Hanspeter Thür

4.2.3 Empfehlung an Swissmedic: «Zulassungsdossiers einzelner Medikamente»

Bern, den 30. März 2010

Empfehlung

gemäss

Art. 14 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung

zu den Schlichtungsanträgen von

Antragstellerin A
Antragstellerin B
Antragstellerin C
Antragstellerin D
Antragstellerin E

gegen

Swissmedic Schweizerisches Heilmittelinstitut, Bern

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Die Antragstellerinnen A und B (Wissenschaftlerinnen) reichten am 7. Dezember 2007 gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ, SR 152.3) beim Schweizerischen Heilmittelinstitut

(Swissmedic) ein Zugangsgesuch zu zahlreichen Dokumenten im Zusammenhang mit der Zulassung verschiedener Medikamente (Zulassungsdossiers) ein. Das Zugangsgesuch enthielt in der Beilage eine Auflistung mit den gewünschten Dokumenten.

2. Am 21. Dezember 2007 teilte Swissmedic den Antragstellerinnen A und B mit, dass es angesichts des Umfangs des Gesuchs nicht in der Lage sei, die gesetzliche Frist von 20 Tagen einzuhalten («l'institut ne sera pas en mesure de tenir le délai légal de 20 jours.»). Weiter wies Swissmedic darauf hin, dass die Zusammenstellung der gewünschten Dokumente mehrere Tage beanspruchen würde. Gemäss Swissmedic sei es daher «fort probable que la facture dépassera nettement CHF 2000.-.»

3. Am 4. März 2008 gab Swissmedic den Antragstellerinnen A und B in einer «ersten Stellungnahme» Einschätzungen betreffend die Zugangsgewährung respektive -verweigerung zu den einzelnen Dokumenten ab. Weiter teilte Swissmedic den Antragstellerinnen mit, dass die Gebühren mindestens 10'000.- SFr. betragen würden, und verlangte von ihnen entsprechend Art. 16 Abs. 2 der Verordnung über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsverordnung, VBGÖ, SR 152.31) eine Bestätigung für das Festhalten am Zugangsgesuch.

4. Am 10. Juni 2008 reichten die Antragstellerinnen A und B ein neues Zugangsgesuch mit einer gekürzten Dokumentenliste ein.

5. Am 26. Juni 2008 teilte Swissmedic den Antragstellerinnen A und B mit, dass es das Gesuch sorgfältig geprüft und festgestellt habe, dass seine Bearbeitung mit viel Arbeit und Zeit verbunden sei. Daher sei Swissmedic zum Schluss gekommen, dass die Dokumente erst Mitte September 2008 bereitgestellt werden könnten. Swissmedic informierte die Antragstellerinnen darüber, dass die Gebühren mindestens 10'000.- SFr. betragen würden. Fristgemäss teilten A und B dem Institut am 3. Juli 2008 mit, dass sie in Kenntnis der Gebühren an ihrem Zugangsgesuch festhielten. Gleichentags reichten die Antragstellerinnen beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) einen Schlichtungsantrag betreffend die Höhe der Gebühren ein.

6. Mit Schreiben vom 12. September 2008 teilte Swissmedic den Antragstellerinnen A und B mit, dass sie offensichtlich nicht Angaben zu einem oder mehreren bestimmten Medikamenten erhalten, sondern vor allem mehr darüber wissen wollten, wie Swissmedic das Öffentlichkeitsgesetz anwende. Angesichts des enormen Volumens der nachgefragten Dokumente, der verschiedenen Themenbereiche, des immensen Aufwands für die Bearbeitung und der Tatsache, dass die Antragstellerinnen nicht an den eigentlichen Inhalten, sondern lediglich an der Anwendung des Öffentlichkeitsgesetzes durch das Institut interessiert

seien, betrachte Swissmedic das Zugangsgesuch als rechtsmissbräuchlich. Daher werde das Zugangsgesuch vom 10. Juni 2008 nicht behandelt. Die Antragstellerinnen A und B reichten am 3. Oktober 2008 beim Beauftragen einen zweiten Schlichtungsantrag ein.

7. Am 5. Januar 2009 reichten die Antragstellerinnen A und B beim Bundesverwaltungsgericht eine Rechtsverzögerungsbeschwerde gegen den Beauftragten ein. Das Gericht anerkannte in seinem Urteil vom 16. April 2009 (A-75/2009) die unrechtmässige Rechtsverzögerung und lud den Beauftragten ein, innerhalb von 30 Tagen das Schlichtungsverfahren durchzuführen und eine Empfehlung zu erlassen.

8. Anlässlich zweier vom Beauftragten durchgeführter Schlichtungsverhandlungen einigten sich die Antragstellerinnen A und B und Swissmedic über den Umfang der Dokumente, ein zeitlich gestaffeltes Vorgehen bei der Zugangsgewährung sowie über den geschuldeten Gebührenbetrag. Unter anderem sollte Swissmedic in einem ersten Schritt und «sous réserve des dispositions de la LTrans» bis Ende November 2009 Zugang zu den Zulassungsunterlagen von zwei Medikamenten gewähren. Da eine Schlichtung zustande kam, musste der Beauftragte keine Empfehlung erlassen.

9. Im Rahmen der Umsetzung der Einigung hörte Swissmedic entsprechend den Vorgaben von Art. 11 BGÖ die betroffenen Pharmaunternehmen (Antragstellerinnen C, D[1], E) an. Dabei stellte das Institut C, D und E die fraglichen Dokumente mit Schwärzungsvorschlägen zu. In ihren Antwortschreiben an Swissmedic sprachen sich diese Pharmaunternehmen gegen eine Zugangsgewährung aus. Sie argumentierten dabei u.a. wie folgt:

   - C und D (vertreten durch denselben Rechtsanwalt) machten geltend, dass die Unterlagen ihrer Zulassungsdossiers Geheimnisse im Sinne von Art. 7 Abs. 1 Bst. g BGÖ beinhalten und jede Veröffentlichung die Privatsphäre von C und D beinträchtige. Die Offenlegung gehe mit einem erheblichen Missbrauchsrisiko einher. Dies gelte insbesondere für die Swissmedic-internen Unterlagen, da u.a. Konkurrenten negative Bemerkungen ausnutzen respektive Kenntnis von künftigen Absichten und Plänen von C und D erlangen könnten. Weiter wird darauf verwiesen, dass «Art. 39 Ziff. 3 TRIPs[2] und Art. 12 HMG[3] einen Schutz von Zulassungsdossiers gewähren, der de facto obsolet wird, wenn Zulassungsdossiers ganz oder teilweise offengelegt (sic!) werden.» C und D stellten einen Hauptantrag auf vollständige Zugangsverweigerung und einen Eventualantrag auf teilweise Verweigerung mit zusätzlichen Schwärzungen.

[1] Antragstellerin D hat während des laufenden Schlichtungsverfahrens das Arzneimittelprodukt von C übernommen. Aus diesem Grund nimmt D als betroffene Drittperson am Verfahren teil.
[2] TRIPS-Abkommen (Abkommen vom 15. April 1994 zur Errichtung der Welthandelsorganisation, SR 0.632.20)
[3] Bundesgesetz über Arzneimittel und Medizinprodukte (Heilmittelgesetz, HMG, SR 812.21)

- Die Antragstellerin E hielt vorweg fest, dass sie dem «Gesuch nicht entsprechen» könne. Weiter vertrat sie die Ansicht, sie habe für das Zulassungsverfahren ihres Medikaments «ein bearbeitetes, gewichtetes Kondensat von Dokumenten wie Informationen erstellt, das als solches nicht öffentlich zugänglich ist und als Geschäftsgeheimnis gilt. Zugänglichmachung von Zulassungsdossiers kann den Konkurrenten einen ungerechtfertigten Vorsprung oder anderswie ungerechtfertigte Informationen geben, was Art. 39 Ziff. 3 TRIPs verhindern will.»

10. Gestützt auf die Stellungnahmen nahm Swissmedic in einigen Unterlagen der Zulassungsdossiers weitere Abdeckungen vor und informierte die Betroffenen am 17. November 2009 darüber, dass es an seiner Haltung, einen teilweisen Zugang zu den Unterlagen der Zulassungsdossiers zu gewähren, festhalte. Swissmedic wies auf die Möglichkeit zur Einreichung eines Schlichtungsantrags gemäss Art. 13 Art. 1 Bst. c BGÖ hin. C, D und E reichten je einen Schlichtungsantrag ein.

11. Swissmedic informierte ebenso die Antragstellerinnen A und B über die ablehnenden Stellungnahmen der betroffenen Pharmaunternehmen, worauf die Antragstellerinnen A und B beim Beauftragten je einen Schlichtungsantrag gemäss Art. 13 Abs. 1 Bst. a BGÖ einreichten.

12. Auf Anfrage reichte Swissmedic dem Beauftragten Stellungnahmen zu den einzelnen Schlichtungsanträgen sowie eine detaillierte Auflistung mit Begründungen für die vorgenommenen Schwärzungen der zu beurteilenden Dokumente ein. Swissmedic anerkannte die grundsätzliche Anwendbarkeit des Öffentlichkeitsgesetzes für Zulassungsunterlagen. Ergänzend hielt das Institut dazu fest, dass die Frage der Zugangsgewährung zu Zulassungsunterlagen schwierig und heikel sei, da es nur unzureichend einzuschätzen vermöge, «ob die durch die Zulassungsinhaberinnen jeweils geltend gemachten Geheimhaltungsinteressen auch tatsächlich bestehen bzw. welches Gewicht ihnen zukommt.» Schwierigkeiten ergeben sich u.a. daraus, dass sich das geltend gemachte Geheimhaltungsinteresse nicht nur aus dem Charakter des jeweiligen Dokuments respektive der jeweiligen Einzelinformation alleine erschliesse, sondern sich auch aus der Vielzahl von für sich nicht unbedingt geheimhaltungswürdigen einzelnen Informationen ergebe, die sich für Konkurrentinnen zu einem Mosaik zusammensetzen liessen, welches für sie ein Bild der Strategie der Zulassungsinhaberinnen für die Entwicklung und Vermarktung ihres betreffenden Produkts zu geben vermöge. Insbesondere bei Zulassungsdossiers für Originalpräparate (Erstanmelderschutz) würden die vertraulichen Daten unter Einsatz von erheblichen Investitionen erstellt. Swissmedic bezeichnete das vorliegende Verfahren als Präzedenzfall. Das Institut erwarte künftig eine Vielzahl von Zugangsgesuchen, weil vermehrt

Pharmaunternehmen auf diesem Weg Einsicht in die Unterlagen von Konkurrenzpräparaten erlangen wollten. Swissmedic verwies dabei auch auf den enormen Arbeitsaufwand, den die Behandlung solcher Gesuche bei ihm und bei den anzuhörenden Pharmaunternehmen verursache. Weiter verwies Swissmedic auf die Schwierigkeit, bei Zulassungsunterlagen eine klare Abgrenzung zwischen ‚Personendatum' und ‚Geschäfts- und Fabrikationsgeheimnis' vornehmen zu können. So handle es bei den Personendaten oftmals auch um Geschäfts- und Fabrikationsgeheimnisse. Dies gelte insbesondere dann, wenn – wie von den angehörten Unternehmen geltend gemacht – «eine Zusammenstellung von bereits bekannten Informationen im Sinne einer Wertschöpfung (mit teilweisem hohen Aufwand) einen Geheimnischarakter nach sich zieht und somit ein Zugang zu solchen Informationen zu schützen ist.» Swissmedic präzisierte u.a.:

- in Bezug auf den Schlichtungsantrag von A und B, «que l'institut ne refusait pas l'accès aux documents conformément à l'accord signé en date du 2 juin 2009, mais vertu de la LTrans, l'institut avait consulté les personnes concernées, dans la mesure où les documents contiennent des données personnelles.»
- in Bezug auf die von C, D und E geltend gemachten Art. 12 HMG und Art. 39 Ziff. 3 des TRIPS-Abkommens (SR 0.632.20), dass die Verweise nicht zielführend seien, weil diese Bestimmungen keine Geheimhaltung von Zulassungsunterlagen von Originalpräparaten vorsähen, sondern die Bezugnahme eines zeitlich späteren Zuganglassungsgesuchs auf diese Unterlagen regelten. Dasselbe gelte für den ohnehin nicht direkt anwendbaren Art. 39 Ziff. 3 des TRIPS-Abkommens.

II. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zieht in Erwägung:

A. Schlichtungsverfahren und Empfehlung gemäss Art. 14 BGÖ

1. Gemäss Art. 13 BGÖ kann eine Person einen Schlichtungsantrag beim Beauftragten einreichen, wenn die Behörde den Zugang zu amtlichen Dokumenten einschränkt, aufschiebt oder verweigert, oder wenn die Behörde innert der vom Gesetz vorgeschriebenen Frist keine Stellungnahme abgibt. Nach Art. 11 BGÖ angehörte Personen sind ebenfalls berechtigt einen Schlichtungsantrag einzureichen, wenn die Behörde gegen ihren Willen den Zugang gewähren will.

Der Beauftragte wird nicht von Amtes wegen, sondern nur auf Grund eines Schlichtungsantrags tätig[4]. Berechtigt, einen Schlichtungsantrag einzureichen, ist jede Person, die an einem Gesuchsverfahren um Zugang zu amtlichen Dokumenten teilgenommen hat.

Für den Schlichtungsantrag genügt einfache Schriftlichkeit. Aus dem Begehren muss hervorgehen, dass sich der Beauftragte mit der Sache befassen soll. Der Schlichtungsantrag muss innert 20 Tagen nach Empfang der Stellungnahme der Behörde schriftlich eingereicht werden.

2. A und B haben ein Zugangsgesuch nach Art. 10 BGÖ bei Swissmedic eingereicht und eine ablehnende Antwort erhalten. Als Teilnehmerinnen an einem vorangegangenen Gesuchsverfahren sind sie sowie die angehörten Pharmaunternehmen zur Einreichung eines Schlichtungsantrags berechtigt. Alle Schlichtungsanträge wurden formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Empfang der Stellungnahme der Behörde) beim Beauftragten eingereicht.

3. Das Schlichtungsverfahren kann auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten stattfinden. Die Festlegung des Verfahrens im Detail obliegt alleine dem Beauftragten[5].

   Kommt keine Einigung zu Stande oder besteht keine Aussicht auf eine einvernehmliche Lösung, ist der Beauftragte gemäss Art. 14 BGÖ gehalten, aufgrund seiner Beurteilung der Angelegenheit eine Empfehlung abzugeben.

B. Sachlicher Geltungsbereich

1. Das Öffentlichkeitsgesetz findet sowohl auf die Verwaltungseinheiten der zentralen wie auch der dezentralen Bundesverwaltung Anwendung (Art. 2 Abs. 1 Bst. a BGÖ)[6]. Swissmedic ist Teil der dezentralen Bundesverwaltung[7].

   Swissmedic fällt in den Geltungsbereich des Öffentlichkeitsgesetzes.

2. Die Antragstellerinnen C und D machen u.a. geltend, dass Art. 12 HMG und Art. 39 Ziff. 3 des TRIPS-Abkommens einen Schutz von Zulassungsdossiers vorsehen und daher kein Zugang gewährt werden könne.

   Es gilt somit zu prüfen, ob diese beiden Normen Spezialbestimmungen im Sinne von Art. 4 BGÖ darstellen und damit das Öffentlichkeitsgesetz nicht zur Anwendung gelangt. Gemäss Art. 4 BGÖ bleiben Spezialbestimmungen anderer Bundesgesetze vorbehalten, die entweder bestimmte Informationen als geheim

[4] BBl 2003 2023
[5] BBl 2003 2024
[6] BBl 2003 1986
[7] s. Anhang der Regierungs- und Verwaltungsorganisationsverordnung (SR 172.010.1) sowie BBl 2003 1986

bezeichnen oder die von Öffentlichkeitsgesetz abweichende Voraussetzungen für den Zugang zu bestimmten Informationen vorsehen.

Art. 12 HMG und 39 Ziff. 3 des TRIPS-Abkommens enthalten weder spezifische Geheimhaltungsbestimmungen noch regeln sie Fragen des Informationszugangs. Darüber hinaus richtet sich Art. 39 Ziff. 3 des TRIPS-Abkommens an die Mitgliedstaaten und verleiht dem Einzelnen keinen gerichtlich durchsetzbaren Rechtsanspruch; diese Norm ist also nicht direkt anwendbar. Diese beiden Artikel sind somit keine Spezialbestimmungen im Sinne von Art. 4 BGÖ.

Demgegenüber stellt sich die Frage, ob Art. 61 HMG (*Schweigepflicht*) und Art. 62 HMG (*Vertraulichkeit von Daten*) Spezialbestimmungen im Sinne von Art. 4 BGÖ darstellen.

Die in Art. 61 HMG festgehaltene Schweigepflicht regelt nur in allgemeiner Weise die Vertraulichkeit von Daten im Bereich des Heilmittelrechts. Diese Schweigepflicht verfolgt damit keinen wesentlich anderen Zweck als das Amtsgeheimnis[8], das nicht als Spezialbestimmung im Sinne von Art. 4 BGÖ gilt. Zudem hat der Bundesrat in seiner Antwort zur Motion «Zulassung von Arzneimitteln. Transparenz bei der Einsichtnahme in die Unterlagen» ausdrücklich festgehalten, dass «Artikel 62 HMG […] denn auch nicht als spezialgesetzliche Zugangsregelung im Sinne von Art. 4 BGÖ zu betrachten [ist]» [9].

Weder Art. 12 HMG und Art. 39 Ziff. 3 des TRIPS-Abkommens noch Art. 61 und Art. 62 HMG sind Spezialbestimmungen im Sinne von Art. 4 Bst. a BGÖ.

3. Dem Öffentlichkeitsgesetz unterliegen Informationen, die auf einem beliebigen Informationsträger (Art. 5 Abs. 1 Bst. a BGÖ) aufgezeichnet sind und sich im Besitz einer Behörde befinden (Bst. b). Vorliegend handelt es sich dabei zum einen um Angaben und Unterlagen, welche die Pharmaunternehmen für die Beurteilung ihrer Gesuche um Zulassung eines Arzneimittels oder eines Verfahrens eingereicht haben (Art. 10f. HMG). Zum anderen sind damit jene Unterlagen gemeint, die Swissmedic für die Zulassungsbeurteilung selber erstellt hat. Die Gesamtheit aller Informationen und Unterlagen betrifft die Erfüllung einer öffentlichen Aufgabe durch Swissmedic.

[8] BBl 2003 1990

[9] Motion Teuscher 02.3748; u.a. heisst es in der Antwort des Bundesrates: «Der Gesetzgeber geht somit nicht davon aus, dass sämtliche Informationen, die gestützt auf das HMG gesammelt werden, grundsätzlich vertraulich sind. Er sieht im Gegenteil eine Lösung vor, die ähnlich wie die Vorlage des Bundesrates zu einem Bundesgesetz über die Öffentlichkeit der Verwaltung (BGÖ) eine Interessenabwägung zulässt und erfordert. Artikel 62 HMG ist denn auch nicht als spezialgesetzliche Zugangsregelung im Sinne von Art. 4 BGÖ zu betrachten. Bei einer Einführung des Öffentlichkeitsprinzips im Sinne der bundesrätlichen Vorlage wäre der Heilmittelbereich deshalb nicht vom Geltungsbereich des BGÖ ausgeschlossen.»

Alle Unterlagen aus den Zulassungsdossiers sind amtliche Dokumente nach Art. 5 Abs. 1 BGÖ und unterliegen damit grundsätzlich dem Öffentlichkeitsprinzip. Eine mögliche Beschränkung des Zugangs ist einzig nach Massgabe der gesetzlichen Bestimmungen von Art. 7-9 BGÖ möglich.

4. Amtliche Dokumente können sowohl Personendaten als auch Informationen enthalten, die unter Ausnahmebestimmungen nach Art. 7 BGÖ (z.B. Berufs-, Geschäfts- oder Fabrikationsgeheimnisse) fallen können. Aus verfahrensökonomischen Gründen ist vorgängig zu prüfen, ob eine Ausnahmebestimmung greift, und erst dann die Frage der Personendaten zu klären.

5. Art. 7 Abs. 1 Bst. g BGÖ ermöglicht eine teilweise oder vollständige Verweigerung des Zugangs, sofern dadurch Berufs-, Geschäfts- oder Fabrikationsgeheimnisse offenbart werden können.

   Swissmedic verfügt aufgrund des gesetzlich vorgeschriebenen Zulassungsverfahrens für Arzneimittelprodukte von C, D und E über eine grosse Menge von Informationen. Nicht sämtliche Informationen, die sich in Zulassungsdossiers befinden, weisen zwangsläufig Geheimnischarakter auf. Dieser fehlt beispielsweise bei jenen Informationen, die von einem Unternehmen selber oder von einer anderen (auch ausländischen) Behörde (z.B. Bewilligungs- und Zulassungsbehörden der EU oder der USA) bereits allgemein zugänglich gemacht worden sind. Hier besteht kein tatsächliches Missbrauchs- oder Schadensrisiko, weshalb die entsprechenden Informationen immer zugänglich gemacht werden müssen.

   Die in Art. 7 Abs. 1 Bst. g BGÖ festgehaltene Ausnahmeklausel schützt nur Geschäftsinformationen von C, D und E, die tatsächlich Geheimnischarakter aufweisen und an denen ein legitimes Geheimhaltungsinteresse besteht, weil ein Bekanntwerden dieser Informationen zu Wettbewerbsverzerrungen führen und darüber hinaus zur Folge haben könnte, dass dem Geheimnisherrn ein wesentlicher Marktvorteil gegenüber seinen Konkurrenten verloren ginge. In der Korrespondenz mit C, D und E (insbesondere im Schreiben vom 17. November 2009) legte Swissmedic dar, in welchem Umfang einzelne Passagen aufgrund des Geschäfts- oder Fabrikationsgeheimnisses geschwärzt werden sollten.

   Gemäss Art. 12 Abs. 1 VBGÖ prüft der Beauftragte die Rechtmässigkeit und die Angemessenheit der Beurteilung des Zugangsgesuch durch die Behörde. Er kann damit im Schlichtungsverfahren einerseits prüfen, ob die Bearbeitung des Zugangsgesuchs durch die Behörde rechtmässig erfolgt ist. Anderseits kann er in jenen Bereichen, in denen das Öffentlichkeitsgesetz der Behörde bei der Bearbeitung eines Zugangsgesuchs einen gewissen Ermessenspielsraum verleiht (z.B. Art der Einsichtnahme in die amtlichen Dokumente), prüfen, ob die von der Behörde gewählte

Lösung auf die Umstände des jeweiligen Falls abgestimmt und angemessen ist. Insgesamt beurteilt der Beauftragte das Vorgehen und Einschätzung von Swissmedic in Bezug auf das Vorliegen von Fabrikations- und Geschäftsgeheimnissen in den Zulassungsdossiers als rechtmässig und angemessen.

6. Soweit Informationen betreffend C, D und E nicht unter das Geschäfts- oder Fabrikationsgeheimnis subsumiert werden können, bestimmt sich der Schutz ihrer Personendaten nach Art. 9 BGÖ.

   Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 Bst. a des Bundesgesetzes über den Datenschutz, DSG, *SR* 235.1). Amtliche Dokumente, die Personendaten enthalten, sind nach Möglichkeit vor der Einsichtnahme zu anonymisieren (Art. 9 Abs. 1 BGÖ). Ist eine Anonymisierung nicht möglich, so beurteilt sich der Zugang nach den Vorschriften über die Bekanntgabe von Personendaten durch Bundesorgane (Art. 9 Abs. 2 BGÖ i.V.m. Art. 19 DSG). Art. 19 Abs. 1*bis* DSG ermöglicht es den Bundesbehörden, gestützt auf das Öffentlichkeitsgesetz Personendaten bekannt zu geben, wenn diese im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen und an deren Bekanntgabe ein überwiegendes öffentliches Interesse besteht. Diese Bestimmung stellt eine Koordinationsnorm zu Art. 7 Abs. 2 BGÖ dar, der vorsieht, dass der Zugang zu amtlichen Dokumenten beschränkt wird, wenn durch seine Gewährung die Privatsphäre Dritter beeinträchtigt werden könnte. Ausnahmsweise muss deren Privatsphäre einem überwiegenden Interesse der Öffentlichkeit am Zugang zu den Dokumenten weichen.

7. Bei den zu beurteilenden Dokumenten können bestimmte Personendaten in den Zulassungsdossiers anonymisiert werden. Swissmedic hat die entsprechenden Anonymisierungen zu Recht vorgenommen.

8. Im Gegensatz dazu ist eine Anonymisierung in Bezug auf Angaben zu C, D und E nicht möglich. In diesem Fall muss eine Interessenabwägung gemäss Art. 7 Abs. 2 BGÖ vorgenommen werden. Im Rahmen der Umsetzung der mit A und B in der Schlichtungsverhandlung vereinbarten Einigung hat Swissmedic entsprechend den Vorgaben von Art. 11 BGÖ eine Anhörung der Betroffenen durchgeführt. Swissmedic informierte die Betroffenen nebst allgemeiner Ausführungen und Erklärungen über das Öffentlichkeitsgesetz. In Bezug auf das konkrete Zugangsgesuch erklärte das Institut seine Absicht, den Zugang grundsätzlich zu gewähren. Gleichzeitig stellte Swissmedic den Betroffenen die fraglichen Dokumente zu und markierte jene Passagen, die es zu schwärzen beabsichtigte. Weiter räumte das Institut den Betroffenen gesetzeskonform die Möglichkeit ein, sich in einer Stellungnahme zum Vorschlag zu äussern (so genannte Anhörung). Aufgrund der Stellungnahmen

der Betroffenen überprüfte Swissmedic erneut seine Einschätzung betreffend die teilweise Zugangsgewährung und nahm in einigen Fällen Korrekturen vor. Entsprechend Art. 11 Abs. 2 BGÖ informierte Swissmedic die Betroffenen mit Schreiben vom 17. November 2009 über das Ergebnis der Anhörung und teilte ihnen mit, dass es im Rahmen der Verhältnismässigkeit und nach Einzelfallabwägung zum Schluss gekommen sei, dass der Beeinträchtigung der Privatsphäre «ein überwiegendes Interesse der öffentlichen Gesundheit (vgl. Art. 6 Abs. 2 Bst. c [recte b] VBGÖ) und ein allgemeines Informationsinteresse gemäss BGÖ an der Einsichtnahme in ein Zulassungsdossier bzw. dessen Bearbeitung durch die Zulassungs- und Aufsichtsbehörde gegenüber [stehen].» Aufgrund dessen hielt Swissmedic an der teilweisen Zugangsgewährung zu den Zulassungsdossiers fest.

Der Beauftragte beurteilt die Einschätzung von Swissmedic in Bezug auf das Vorliegen des öffentlichen Interesses am Zugang zu Teilen der Zulassungsdossiers (Art. 7 Abs. 2 BGÖ, Art. 9 Abs. 2 BGÖ i.V.m. Art. 19 Abs. 1bis DSG) als rechtmässig.

9. Der zu beurteilende Fall zeichnet sich einerseits durch den grossen Umfang der zu beurteilenden Dokumente (ca. 250 Seiten) und anderseits durch die Komplexität der Materie aus. Dabei hat Swissmedic sowohl die Interessen der Betroffenen (hinsichtlich Geschäfts- und Fabrikationsgeheimnisse ebenso wie Schutz der Privatsphäre) als auch das öffentliche Interesse am Zugang zu amtlichen Dokumenten adäquat berücksichtigt. In Anwendung des Verhältnismässigkeitsprinzips gelangte Swissmedic zum Schluss, einen teilweisen Zugang zu den Zulassungsdossiers zu gewähren, und begründete den betroffenen Pharmaunternehmen sein Entscheid, insbesondere im Schreiben vom 17. November 2009. Abschliessend stellt der Beauftragte fest, dass Swissmedic im Verlaufe des Verfahrens, insbesondere seit den beiden Schlichtungsverhandlungen, der Transparenz und der Umsetzung des Öffentlichkeitsgesetzes einen hohen Stellenwert eingeräumt hat.

   Der Beauftragte beurteilt das von Swissmedic gewählte Vorgehen auf die Umstände des Einzelfalls abgestimmt. Die konkrete Beurteilung betreffend die teilweise Zugangsgewährung erfolgte in angemessener Art und Weise.

III. Aufgrund dieser Erwägungen empfiehlt der Datenschutz- und Öffentlichkeitsbeauftragte:

1. Swissmedic gewährt den teilweisen Zugang zu den Zulassungsdossiers der Arzneimittelprodukte von C, D und E gemäss seiner Stellungnahme vom 17. November 2009.

2. *Swissmedic erl*ässt eine Verfügung nach Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG, SR 172.021), wenn es in Abweichung von Ziffer 1 den Zugang nicht gewähren will.

   Swissmedic erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung (Art. 15 Abs. 3 BGÖ).

3. Die Antragstellenden können innerhalb von 10 Tagen nach Erhalt dieser Empfehlung bei Swissmedic den Erlass einer Verfügung nach Art. 5 VwVG verlangen, wenn sie mit der Empfehlung nicht einverstanden sind (Art. 15 Abs. 1 BGÖ).

4. Gegen die Verfügung können die Antragstellenden beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

5. In Analogie zu Art. 22a VwVG stehen gesetzliche Fristen, die nach Tagen bestimmt sind, vom siebten Tag vor Ostern bis und mit dem siebten Tag nach Ostern still. Der Fristenlauf beginnt somit am 12. April 2010.

6. Diese Empfehlung wird veröffentlicht. Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten wird der Name der Antragstellenden anonymisiert (Art. 13 Abs. 3 VBGÖ).

7. Die Empfehlung wird eröffnet:

   - A (Empfehlung auf Deutsch und Übersetzung auf Französisch)
   - B (Empfehlung auf Deutsch und Übersetzung auf Französisch)
   - C
   - D
   - E
   - Swissmedic (Empfehlung auf Deutsch und Übersetzung auf Französisch)

     Hallerstrasse 7

     Postfach

     3000 Bern 9

Hanspeter Thür

4.2.4 Empfehlung an das Bundesamt für Justiz: «Loterie Romande»

(Siehe Abschnitt 4.2.4 im französischen Teil des Berichts)

4.2.5 Empfehlung an das Departement für Verteidigung, Bevölkerungsschutz und Sport: «Islamistische Imame»

Bern, den 21. Oktober 2010

Empfehlung

gemäss

Art. 14 des
Bundesgesetzes über das
Öffentlichkeitsprinzip der Verwaltung

zu den Schlichtungsanträgen von

(Antragsteller A)

(Antragsteller B)

gegen

Eidgenössisches Departement
für Verteidigung, Bevölkerungsschutz und Sport

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ, SR 152.3) reichten der Antragsteller A (Journalist) am 2. November 2009 und der Antragsteller B (Journalist) am 5. November 2009 beim Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) ein Gesuch um Zugang zu einem Bericht vom 29. Januar 2008 mit dem Titel «Islamistische Imame» ein. Der Bericht wurde vom Stab des Sicherheitsausschusses (Stab SiA) für den Sicherheitsausschuss des Bundesrates (SiA) erstellt[1]. Der *SiA* setzt sich aus den Departementsvorsteherinnen und Departementsvorstehern des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA), des Eidgenössischen Justiz- und Polizeidepartements (EJPD) und des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) zusammen. Vorsitzender des SiA ist der Chef des VBS. Der *Stab SiA* ist dem Chef des VBS unterstellt und dem Generalsekretariat des VBS administrativ zugeordnet.

2. Das VBS lehnte die beiden Zugangsgesuche mit Schreiben vom 11. November 2009 ab. Es begründete dies damit, dass der Bericht mit dem Titel «Islamistische Imame» gestützt auf die Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung ISchV; SR 510.411) als vertraulich klassifiziert sei. Die Kenntnisnahme von vertraulich klassifizierten Informationen durch Unberechtigte könne den Landesinteressen Schaden zufügen. Weiter führte das VBS aus, dass gemäss Art. 7 Abs. 1 BGÖ «der Zugang zu amtlichen Dokumenten verweigert werden [kann], wenn durch seine Gewährung *die innere oder äussere Sicherheit der Schweiz gefährdet werden kann (Bst. c) oder die aussenpolitischen Interessen oder die internationalen Beziehungen der Schweiz beeinträchtigt werden können (Bst. d).*»

3. Am 11. November 2009 veröffentlichte die Weltwoche ein Interview mit dem Departementschef des VBS. Auf die Frage, ob die Studie (gemeint ist der Bericht) so brisant sei, dass sie unter Verschluss gehalten werden müsse, antwortete er: «Ich habe keine politische Brisanz erkannt, als ich sie übers letzte Wochenende gelesen

[1] s. http://www.vbs.admin.ch/internet/vbs/de/home/departement/organisation/stabsia.html mit Factsheet: Aufgaben und Zuständigkeiten des Sicherheitsausschusses des Bundesrats (SiA), des Stabes SiA und der Lenkungsgruppe Sicherheit

habe. Es ist ein 08/15-Bericht. Es steht nichts darin, was nicht bereits in den Medien abgehandelt wurde.»[2] Am 9. Dezember 2009 publizierte die Weltwoche einen Artikel[3] über den Bericht sowie einen Auszug daraus[4].

4. Die Antragsteller reichten am 12. respektive am 13. November 2009 beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) jeweils einen Schlichtungsantrag ein. Gestützt auf Art. 20 BGÖ forderte der Beauftragte daraufhin das VBS auf, ihm den Bericht zuzustellen und die Zugangsverweigerung für jede Textpassage detailliert zu begründen.

5. Am 4. Dezember 2009 verwies das VBS in einer Stellungnahme zuhanden des Beauftragten erneut auf die Klassifizierung des Berichts sowie auf die Tatsache, dass sich sowohl die Koordinationsstelle für den Informationsschutz im Bund (Art. 20 ISchV) wie auch der Urheber des Berichts, der Stab SiA, «aus Gründen der Wahrung der inneren und äusseren Sicherheit der Schweiz sowie ihrer aussenpolitischen Interessen und internationalen Beziehungen […] ausdrücklich gegen eine Entklassifizierung und damit Freigabe des Berichts geäussert [haben].» Das VBS hielt weiter fest, eine Freigabe des Berichts würde früher oder später dazu führen, dass nur einzelne Teile davon gelesen oder insbesondere von der Presse publiziert würden. «Solche Auszüge könnten isoliert betrachtet aber ein völlig falsches Bild über den tatsächlichen Inhalt des Berichts bzw. dessen wesentlichen und eigentlichen Aussagen vermitteln […]. Nebst konkreter Namen […], die zwar grundsätzlich geschwärzt werden könnten, sind an mehreren Stellen einigermassen konkrete […] bis ganz präzise […] Rückschlüsse möglich. Auch hier gilt, dass eine blosse Teilveröffentlichung den Kerngehalt des Berichts verfälschen würde.» Durch eine lediglich lückenhafte Kenntnisnahme des Berichts durch Unberechtigte könne nicht ausgeschlossen werden, dass den Landesinteressen Schaden im Sinne von Art. 6 Abs. 1 Bst. c ISchV zugefügt werden könne. Der Zugang sei daher wegen einer möglichen Gefährdung der inneren und äusseren Sicherheit der Schweiz (Art. 7 Abs. 1 Bst. c BGÖ) und der potentiellen Beeinträchtigung der aussenpolitischen Interessen oder der internationalen Beziehungen der Schweiz (Art. 7 Abs. 1 Bst. d BGÖ) zu verweigern. Im Weiteren vertrat das VBS angesichts der eben angenommenen Minarett-Initiative die Ansicht, dass eine Herausgabe des Berichts mit erhöhter Zurückhaltung zu prüfen sei, «damit die bereits ‚aufgeheizte' Stimmung – gerade auch in den Medien – nicht noch zusätzlich gereizt wird.»

[2] http://www.weltwoche.ch/ausgaben/2009-46/artikel-2009-46-5000-mann-sind-einsatzbereit.html
[3] http://www.weltwoche.ch/ausgaben/2009-50/artikel-2009-50-imame-moschee-als-dunkelkammer.html
[4] http://www.weltwoche.ch/ausgaben/2009-50/artikel-2009-50-dokument-studie-islamistische-imame.html

6. Am 23. September 2010 führte der Beauftragte eine Schlichtungsverhandlung mit zwei Vertretern des VBS und den beiden Antragstellern durch. Das VBS hielt an seiner Position, einer vollumfänglichen Verweigerung, fest und begründete dies gegenüber den Antragstellern. Dabei verwies das VBS auch auf die ablehnenden Stellungnahmen des Bundesrates zu zwei parlamentarischen Vorstössen, in denen ebenfalls die Veröffentlichung des entsprechenden Berichts verlangt worden war.

   Auszug aus der Antwort des Bundesrates zur Interpellation 09.4315 Schlüer Ulrich[5]: «Der Bundesrat lehnt eine Veröffentlichung des vom Stab des Sicherheitsausschusses des Bundesrates für den Sicherheitsausschuss erstellten und klassifizierten Berichtes vom 29. Januar 2008 mit dem Titel «Islamistische Imame» ab. Der Bericht ist ausschliesslich für die sicherheitspolitischen Entscheidungsträger bestimmt und enthält Informationen aus nachrichtendienstlichen Quellen. Deren Preisgabe wäre mit dem für eine seriöse nachrichtendienstliche Arbeit unerlässlichen Schutz dieser Quellen nicht vereinbar. Zudem würde mit einer Veröffentlichung die mutmasslich begangene Amtsgeheimnisverletzung nachträglich gerechtfertigt. Schliesslich entsprechen die zu Beginn des Jahres 2008 gemachten Aussagen teilweise nicht mehr dem aktuellen Erkenntnisstand.»

   Auszug aus der Antwort des Bundesrates zur Motion 09.4319 Baumann J. Alexander[6]: «Der Bundesrat lehnt eine Veröffentlichung dieses klassifizierten Berichtes ab. Der Bericht ist ausschliesslich für die sicherheitspolitischen Entscheidungsträger bestimmt und enthält Informationen aus nachrichtendienstlichen Quellen. Mit einer Veröffentlichung würde eine mutmassliche Amtsgeheimnisverletzung nachträglich gerechtfertigt. Ferner entsprechen die Aussagen teilweise nicht mehr dem aktuellen Erkenntnisstand.»

   Die Antragsteller schätzten nach eigenen Angaben insgesamt den Informationsaustausch mit dem VBS ebenso wie die erhaltenen Ausführungen. Sie hielten indessen an ihrer Forderung nach einem zumindest teilweisen Zugang zum Bericht fest. Die Beteiligten konnten sich daher nicht über die Zugänglichkeit des besagten Berichts einigen.

7. Im Anschluss an die Schlichtungsverhandlung trafen sich der Beauftragte und die Vertreter des VBS ohne die Antragsteller zu einer offenen Diskussion über den Inhalt des Berichts. Dabei gab der Beauftragte seine Einschätzung betreffend die Zugänglichkeit des Berichts bekannt und präsentierte einen Vorschlag für eine teilweise Zugangsgewährung (s. nachfolgende Ausführungen). Dieser Vorschlag sollte den zuständigen Stellen im VBS unterbreitet werden. Am 29. September 2010 teilte das VBS dem Beauftragten telefonisch mit, dass es an seiner ursprünglichen Position festhalte und es folglich den Vorschlag des Beauftragten ablehne, ohne dass neue Argumente angeführt wurden.

[5] Interpellation 09.4315 Schlüer Ulrich «Wie setzt der Bundesrat die Minarettverbots-Initiative um?»
[6] Motion 09.4319 Baumann J. Alexander «Integrative Toleranz von islamistischen Imamen»;

II. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zieht in Erwägung:

A. Schlichtungsverfahren und Empfehlung gemäss Art. 14 BGÖ

1. Gemäss Art. 13 BGÖ kann eine Person einen Schlichtungsantrag beim Beauftragten einreichen, wenn die Behörde den Zugang zu amtlichen Dokumenten einschränkt, aufschiebt oder verweigert, oder wenn die Behörde innert der vom Gesetz vorgeschriebenen Frist keine Stellungnahme abgibt.

   Der Beauftragte wird nicht von Amtes wegen, sondern nur auf Grund eines schriftlichen Schlichtungsantrags tätig[7]. Berechtigt, einen Schlichtungsantrag einzureichen, ist jede Person, die an einem Gesuchsverfahren um Zugang zu amtlichen Dokumenten teilgenommen hat. Für den Schlichtungsantrag genügt einfache Schriftlichkeit. Aus dem Begehren muss hervorgehen, dass sich der Beauftragte mit der Sache befassen soll. Der Schlichtungsantrag muss innert 20 Tagen nach Empfang der Stellungnahme der Behörde schriftlich eingereicht werden.

2. Die Antragsteller haben ein Zugangsgesuch nach Art. 10 BGÖ beim VBS eingereicht und eine ablehnende Antwort erhalten. Als Teilnehmer an einem vorangegangenen Gesuchsverfahren sind sie zur Einreichung ihrer Schlichtungsanträge berechtigt. Die Schlichtungsanträge wurden formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Empfang der Stellungnahme der Behörde) beim Beauftragten eingereicht.

3. Das Schlichtungsverfahren kann auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten stattfinden. Die Festlegung des Verfahrens im Detail obliegt alleine dem Beauftragten[8].

   Kommt keine Einigung zu Stande oder besteht keine Aussicht auf eine einvernehmliche Lösung, ist der Beauftragte gemäss Art. 14 BGÖ gehalten, aufgrund seiner Beurteilung der Angelegenheit eine Empfehlung abzugeben.

B. Sachlicher Geltungsbereich

1. Der Bericht mit dem Titel «Islamistische Imame» wurde vom Stab SiA erstellt, einer Verwaltungseinheit der zentralen Bundesverwaltung. Beim Bericht handelt sich um ein amtliches Dokument im Sinne von Art. 5 BGÖ. Das VBS hat von Beginn weg anerkannt, dass dieser Bericht grundsätzlich in den Geltungsbereich des Öffentlichkeitsgesetzes fällt und hat keine Spezialbestimmung gemäss Art. 4 BGÖ geltend gemacht. Das VBS wies explizit darauf hin, dass der Bericht für den SiA erstellt worden ist.

[7] BBl 2003 2023
[8] BBl 2003 2024

Zentral in der Anwendung des Öffentlichkeitsgesetzes ist jedoch nicht der Adressat eines Dokuments, sondern das Kriterium des amtlichen Dokuments (Art. 5 BGÖ) sowie allenfalls jenes des Erstellers (Art. 10 Abs. 1 BGÖ)[9]. Weiter unterliegt der Gesamtbundesrat als Kollegialbehörde nicht dem Öffentlichkeitsgesetz. Dies gilt jedoch nicht für einen Vorsteher eines Departements oder für einzelne Ausschüsse des Bundesrates.

2. Das VBS argumentierte, eine Teilveröffentlichung würde den Kerngehalt des Berichts verfälschen, weil allenfalls nur Auszüge von der Presse publiziert würden. Hierzu muss erstens festgehalten werden, dass Behörden nie kontrollieren können, wie und in welchem Umfang von ihr veröffentlichte Informationen weiterverwendet werden. Zweitens kann der Argumentation des VBS mit mindestens gleicher Berechtigung entgegen gehalten werden, dass erst ein (inhaltlich möglichst weitgehendes) Zugänglichmachen des Berichts es der Öffentlichkeit erlaubt, sich ein *eigenes und differenziertes* Bild einerseits über den konkreten Inhalt und andererseits über die Tätigkeit des Stabs SiA zu machen. An dieser Stelle sei erneut daran erinnert, dass der Grundsatz der Öffentlichkeit die *demokratische Kontrolle* über das Verwaltungshandeln nicht nur sicherstellen, sondern erst ermöglichen und darüber hinaus zur *Glaubwürdigkeit* staatlichen Verwaltungshandelns beitragen soll[10]. Dies ergibt sich im Übrigen deutlich aus dem Zweckartikel des Öffentlichkeitsgesetzes, gemäss dem die Transparenz über den Auftrag, die Organisation und die Tätigkeit der Verwaltung gefördert werden soll (Art. 1 BGÖ). In letzter Konsequenz soll verhindert werden, dass innerhalb der Verwaltung Geheimbereiche entstehen können. Auch wenn der Stab SiA mit sicherheitspolitischen Aufgaben betraut ist, heisst dies nicht, dass jedes seiner Dokumente dem Öffentlichkeitsprinzip entzogen ist.

3. Das VBS verweigerte den Zugang zum Bericht mit Verweis auf seine Klassifizierung (vertraulich) in Verbindung mit den Ausnahmegründen der Gefährdung der inneren oder äusseren Sicherheit der Schweiz (Art. 7 Abs. 1 Bst. c BGÖ) und der Beeinträchtigung der aussenpolitischen Interessen oder der internationalen Beziehungen der Schweiz (Art. 7 Abs. 1 Bst. d BGÖ).

4. Als *Klassifizierung* wird der Vorgang bezeichnet, bei welchem die Behörde eine konkrete Information dem Klassifizierungskatalog (Art. 8 ISchV) entsprechend beurteilt und mit dem Klassifizierungsvermerk formell kennzeichnet (Art. 3 Bst. f ISchV). Entsprechend dem Grad der Schutzwürdigkeit von Informationen werden drei Klassifizierungsstufen unterschieden: «geheim» (Art. 5 ISchV), «vertraulich»

[9] Dem Adressaten kommt ein gewisse Relevanz bei einem von einem Dritten der Verwaltung mitgeteilten Dokument («Hauptadressat» in Art. 10 Abs. 1 BGÖ; in casu handelt es sich jedoch um ein von einer Verwaltungseinheit erstelltes Dokument) sowie in Bezug auf ein fertig gestelltes Dokument (s. Art. 1 Abs. 2 Bst. b VBGÖ) zu.
[10] BBl 2003 1973

(Art. 6 ISchV) oder «intern» (Art. 7 ISchV). Die Umschreibung der Klassifizierungsstufen orientiert sich stark am Wortlaut der Ausnahmebestimmungen von Art. 7 BGÖ und muss denn auch «im Lichte dieser Bestimmungen»[11] ausgelegt werden.

5. Die Tatsache, dass ein amtliches Dokument klassifiziert ist, mag ein gewichtiges Element in der Beurteilung des Zugangsgesuches darstellen, *alleine aufgrund der Klassifizierung darf der Zugang aber nicht verweigert werden*[12]. Bezieht sich nämlich ein Zugangsgesuch auf ein klassifiziertes Dokument, muss gemäss Art. 11 Abs. 5 der Verordnung über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsverordnung VBGÖ, SR 152.31) geprüft werden, ob dieses entklassifiziert werden kann. Gemäss Art. 13 Abs. 3 ISchV wiederum prüft die zuständige Stelle, unabhängig von einem allfälligen Klassifizierungsvermerk, ob der Zugang nach Öffentlichkeitsgesetz zu gewähren, zu beschränken, aufzuschieben oder zu verweigern ist. Bei der Prüfung der Frage, ob die Klassifizierung überhaupt noch gerechtfertigt ist, muss die zuständige Stelle u.a. auch abklären, ob sämtliche Teile eines Dokuments noch zurückbehalten werden müssen, um den mittels Klassifizierung angestrebten Schutz bestimmter Interessen sicherzustellen. Ergibt die Prüfung, dass die Klassifzierung nicht mehr gerechtfertigt ist, muss das Dokument (als ganzes oder in Teilen) entklassifiziert und der Zugang gewährt werden[13]. Mit anderen Worten führt die Koordination des Öffentlichkeitsgesetzes und der Informationsschutzverordnung dazu, dass im Rahmen der Beurteilung eines Zugangsgesuchs nur Klassifizierungen von Informationen gerechtfertigt sind, soweit eine Ausnahmebestimmung nach Art. 7 Abs. 1 BGÖ oder einer der Sonderfälle von Art. 8 Abs. 1-4 BGÖ vorliegt.

6. Der zu beurteilende Bericht wurde als *vertraulich* klassifiziert. Gemäss Art. 6 ISchV kann die Kenntnisnahme der klassifizierten Informationen durch Unberechtigte den Landesinteressen Schaden zufügen, insbesondere wenn das Bekanntwerden die Sicherheit der Bevölkerung (Art. 6 Abs. 1 Bst. c ISchV) sowie die aussenpolitischen Interessen oder internationalen Beziehungen der Schweiz (Art. 6 Abs. 1 Bst. f ISchV) beeinträchtigen kann. Wie oben ausgeführt, müssen diese Umschreibungen im Lichte der Ausnahmeklauseln des Öffentlichkeitsgesetzes, vorliegend Art. 7 Abs. 1 Bst. c und d BGÖ, interpretiert werden. Dabei muss auch geprüft werden, ob – und im welchem Umfang – die Klassifizierungstufe «vertraulich» in Bezug auf den zu beurteilenden Bericht noch gerechtfertigt ist.

[11] Brunner, Die neue Informationsschutzverordnung des Bundes: Das Öffentlichkeitsprinzip am Scheideweg? Ziff. 2, in: medialex 1/08

[12] Handkommentar zum BGÖ, Art. 4 Rz 30; Handkommentar zum BGÖ, Art. 12 RZ 8; Bundesamt für Justiz, «Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen» Ziffer 4.3 (Stand 25. Februar 2010)

[13] BBl 2003 2006

Im Weiteren gilt es daher zu prüfen, ob die Voraussetzungen für die Beschränkung des Zugangs nach Art. 7 Abs. 1 Bst. c und d BGÖ gegeben sind.

7. Ausgangspunkt für die Prüfung der Zugänglichkeit ist gemäss Öffentlichkeitsgesetz das *konkrete amtliche Dokument*, d.h. vorliegend der Bericht mit dem Titel «Islamistische Imame». Es geht also *nicht um eine generelle Qualifikation der Zugänglichkeit* von Dokumenten und Informationen des Stab SiA oder des Nachrichtendienstes des Bundes (NDB).

8. Ob eine Ausnahme gemäss Art. 7 Abs. 1 BGÖ gegeben ist, hängt *nicht* von einer Abwägung der Interessen der Verwaltung an der Geheimhaltung und des Interesses des Gesuchstellers auf Zugang ab. Der Gesetzgeber hat diese Interessenabwägung bereits vorweggenommen, indem er in Art. 7 Abs. 1 BGÖ *abschliessend* die Fälle der überwiegenden öffentlichen oder privaten Interessen aufgezählt hat, welche das öffentliche Interesse auf Zugang überwiegen[14]. Eine solche Abwägung darf die Behörde nur im Fall von Art. 7 Abs. 2 BGÖ vornehmen, falls ein Dokument Personendaten enthält, die nicht anonymisiert werden können[15]. Der im Öffentlichkeitsgesetz verankerte Schutzmechanismus von Geheimhaltungsinteressen beruht nach Art. 7 Abs. 1 BGÖ *einzig auf dem Bestehen oder Nichtbestehen eines Schadensrisikos*. Dabei müssen kumulativ folgende zwei Bedingungen vorliegen: Erstens muss das von der Behörde geltend gemachte Interesse durch die Offenlegung *erheblich beeinträchtigt* werden, und zweitens muss ein *ernsthaftes* Risiko bestehen, dass die Beeinträchtigung eintritt[16]. Ist eine Beeinträchtigung lediglich denkbar oder im Bereich des Möglichen, darf der Zugang nicht verweigert werden. Damit die Ausnahme wirksam wird, muss der Schaden «nach dem üblichen Lauf der Dinge» mit hoher Wahrscheinlichkeit eintreten. Im Zweifelsfall ist der Zugang zu gewähren[17].

9. Falls ein amtliches Dokument aus der Sicht der Behörde Informationen enthält, deren Bekanntwerden ein Schadensrisiko beinhaltet, bedeutet das nicht, dass das ganze Dokument oder bestimmte Informationen daraus unbesehen als Ausnahmefall nach Art. 7 BGÖ zu betrachten sind. Die Behörde ist verpflichtet, bei jeder Gesucherteilung das Verhältnismässigkeitsgebot[18] zu beachten. Es verlangt im

[14] Bertil Cottier/Rainer J. Schweizer/Nina Widmer, in: Brunner/Mader, (Hrsg.), Handkommentar zum BGÖ, Art. 7 Rz. 5
[15] Art. 7 Abs. 2 BGÖ, Art. 9 BGÖ und Art. 6 VBGÖ
[16] Bertil Cottier/Rainer J. Schweizer/Nina Widmer, in: Brunner/Mader, (Hrsg.), Handkommentar zum BGÖ, Art. 7 Rz 4
[17] Bertil Cottier/Rainer J. Schweizer/Nina Widmer, in: Brunner/Mader, (Hrsg.), Handkommentar zum BGÖ, Art. 7 Rz 4.; BBl 2003 2009, Empfehlung vom 29. August 2008, Ziffer II.B.4;sowie Stephan C. Brunner, Interessenabwägung im Vordergrund, digma 4/2004, S. 162
[18] Urteil des Bundesverwaltungsgerichtes vom 15. September 2009, A-3631/2009, Erw.2.6, Erw. 3.4.1, Erw. 3.5.1 und Erw. 4.; BGE 133 II 209 Erw. 2.3.3

Falle einer Beschränkung, immer die mildeste mögliche Variante zu wählen[19]. Die Behörde hat demnach durch Güterabwägung zu prüfen, ob anstelle einer vollkommenen Verweigerung das amtliche Dokument *teilweise zugänglich* gemacht werden kann, oder ob allenfalls ein Aufschub in Frage kommt.

10. Der Bericht enthält u.a. allgemeine Ausführungen zur Rolle von Imamen, zu Problemen mit islamistischen Imamen, Auflistungen der gesetzlichen Einreisebestimmungen in die Schweiz, Bedingungen für den Erhalt einer Arbeitsbewilligung in der Schweiz etc. Dabei handelt es sich durchwegs um Informationen, die auch *in öffentlich zugänglichen Quellen* (Internet, Bücher, Statistiken, Medien etc.) oder in Gesetzen zu finden sind. Eine Offenlegung dieser allgemeinen – und in keiner Art und Weise vertraulichen – Informationen kann daher nicht zu einer Gefährdung der inneren oder äusseren Sicherheit des Landes respektive zu einer Beeinträchtigung der aussenpolitischen Interessen oder der internationalen Beziehungen der Schweiz führen. Mit anderen Worten ist nach Ansicht des Beauftragten bereits die Erheblichkeit der Gefährdung respektive der Beeinträchtigung nicht geben. Damit fehlt – selbstredend – auch das vom Gesetzgeber geforderte Element des ernsthaften Schadensrisikos im Falle einer Zugangsgewährung. Eine Kenntnisname dieser Informationen durch Unberechtigte kann den Landesinteressen folglich auch keinen Schaden zufügen (Art. 7 ISchV) und eine Klassifizierung ist damit nicht gerechtfertigt.

    Nach Einschätzung des Beauftragten hat ein Bekanntwerden dieser Inhalte des Berichts keinerlei ernsthaftes Schadensrisiko zur Folge. Es resultiert daraus keine ernsthafte Gefährdung der inneren oder äusseren Sicherheit der Schweiz oder keine ernsthafte Beeinträchtigung der aussenpolitischen Interessen oder der internationalen Beziehungen.

11. Der Bericht beinhaltet jedoch auch Passagen, deren Bekanntwerden ein ernsthaftes Risiko für die innere und äussere Sicherheit des Landes zur Folge haben könnte. Gemeint sind Einschätzungen und Analysen des NDB (insbesondere jene des ehemaligen Dienstes für Analyse und Prävention DAP). Diese Passagen fallen unbestreitbar in den Geltungsbereich von Art. 7 Abs. 1 Bst. c BGÖ und dürfen nicht zugänglich gemacht werden. Das VBS hat es im Schlichtungsverfahren aber versäumt darzulegen, welche Passagen – auch zum Schutz nachrichtendienstlicher Quellen – nicht zugänglich gemacht werden dürfen.

    Nach Ansicht des Beauftragten sind folgende Passagen zu schwärzen:
    1. S. 6; Absatz 2, Satz 3 «Selon …»
    2. S. 13, Ziffer 4.1, sofern die Informationen aus nachrichtendienstlichen Quellen stammen.

[19] Bundesamt für Justiz, Leitfaden Gesuchsbeurteilung und Checkliste, Ziffer 2.4

12. Die im Bericht zitierten Namen von Privaten sowie die erwähnten Beispiele in der Schweiz und Europa sind ebenfalls abzudecken. Dies ist zum einen aus Gründen des Schutzes der Privatsphäre (Art. 9 Abs. 1 BGÖ) gerechtfertigt, zum andern aus Gründen der Sicherheit des Landes und der aussenpolitischen Beziehungen geboten (Art. 7 Abs. 1 Bst. c und d BGÖ).

    Folgende Passagen sind zu schwärzen:
    1. S. 7f. «Exemples européens»
    2. S. 8f. «Exemples suisses»
    3. S. 10, zweitletzter Absatz, Text in der Klammer «(ex.: la …)», sofern darüber zu dem erwähnten Zeitpunkt nicht bereits in den Medien berichtet worden ist.

13. Auf Seite 17 sind die Optionen Nr. 1.-4. für das weitere Vorgehen sind – mangels vorgebrachter Argumente des VBS und angesichts der bereits verstrichenen Termine – vollumfänglich zugänglich zu machen. Diese Optionen tangieren weder die Sicherheit des Landes noch aussenpolitische Interessen oder internationale Beziehungen der Schweiz. Zudem könnte das Argument der zielkonformen Durchführung von behördlichen Massnahmen (Art. 7 Abs. 1 Bst. b BGÖ) nicht mehr als Ausnahmeklausel herbeigezogen werden, da die vorgeschlagenen Massnahmen aufgrund der festgesetzten Fristen zum heutigen Zeitpunkt bereits umgesetzt sein müssen. Gestützt auf Art. 7 Abs. 1 Bst. d (Aussenpolitik) kann hingegen die Option Nr. 5. betreffend Visumerteilung kann abgedeckt werden.

14. Sofern der Bericht Informationen enthält, die auf Ersuchen des Stab SiA von anderen Verwaltungseinheiten des Bundes ausgearbeitet worden sind und die tatsächlich Ausnahmequalität gemäss Art. 7 Abs. 1 BGÖ aufweisen, hört der Stab SiA die betroffenen Stellen vor der teilweisen Zugangsgewährung an (Art. 11 VBGÖ).

15. Zusammenfassend hält der Beauftragte fest, dass der Bericht mit dem Titel «Islamistische Imame» über weite Strecken zugänglich zu machen ist. Die Einschätzungen und Aussagen des NDB können abgedeckt werden ebenso wie die Option Nr. 5 auf Seite 17. Weiter sind die Personendaten zum Schutz der Privatsphäre der Betroffenen zu schwärzen.

III. Aufgrund dieser Erwägungen empfiehlt der Datenschutz- und Öffentlichkeitsbeauftragte:

1. Das VBS gewährt einen teilweisen Zugang zum Bericht mit dem Titel «Islamistische Imame» entsprechend den Ausführungen unter Ziffer II.

2. Das VBS erlässt eine Verfügung nach Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG, SR 172.021), wenn es in Abweichung von Ziffer 1 den teilweisen Zugang nicht gewähren will.

   Das VBS erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung (Art. 15 Abs. 3 BGÖ).

3. Die Antragsteller können innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim VBS den Erlass einer Verfügung nach Art. 5 VwVG verlangen, wenn sie mit der Empfehlung nicht einverstanden sind (Art. 15 Abs. 1 BGÖ).

4. Gegen die Verfügung können die Antragsteller beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

5. Diese Empfehlung wird veröffentlicht. Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten wird der Name der Antragsteller anonymisiert (Art. 13 Abs. 3 VBGÖ).

6. Die Empfehlung wird eröffnet:

   - A
   - B
   - Eidg. Departement für Verteidigung,
     Bevölkerungsschutz und Sport

     3003 Bern

Jean-Philippe Walter

4.2.6 Empfehlung an das Bundesamt für Landwirtschaft: «Vom EVD eingesetzte Arbeitsgruppe»

Bern, 23. Dezember 2010

Empfehlung

gemäss

Art. 14 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung

zum Schlichtungsantrag von

X
(Antragstellerin)

gegen

Bundesamt für Landwirtschaft

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Die Antragstellerin (Journalistin) hat am 9. Mai 2009 beim Bundesamt für Landwirtschaft (BLW), gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz BGÖ, SR 152.3), ein Gesuch um Zugang zu Dokumenten der *Arbeitsgruppe Begleitmassnahmen Freihandelsabkommen* (nachfolgend Arbeitsgruppe) gestellt. Darin begehrte sie Einsicht in eine von der Arbeitsgruppe erstellte «Liste mit mehr als 100 Vorschlägen» sowie in eine «reduzierte Liste mit ca. 80 Vorschlägen».

Die Arbeitsgruppe steht im Zusammenhang mit dem Beschluss des Bundesrats vom 14. März 2008 für ein Verhandlungsmandat mit der EU betreffend der gegenseitigen Öffnung der Agrar- und Lebensmittelmärkte. Der Bundesrat beauftragte das Eidgenössische Volkswirtschafts-departement (EVD), in Zusammenarbeit mit dem Eidgenössischen Finanzdepartement (EFD) und unter Beizug einer Arbeitsgruppe konkrete Begleitmassnahmen und entsprechende gesetzliche Grundlagen auszuarbeiten. Das EVD setzte ein eine Arbeitsgruppe aus Vertretern der betroffenen Kreise ein mit dem Auftrag, dem Departement konkrete Vorschläge für Begleitmassnahmen vorzulegen. Mit der Leitung der Arbeitsgruppe wurde der Direktor des Bundesamtes für Landwirtschaft (BLW) beauftragt. Das Sekretariat führte das BLW[1]. Gemäss Medienmitteilung[2] gehörten der Arbeitsgruppe Vertreter von 15 Organisationen aus dem Agrar- und Lebensmittelbereich, zwei Vertreter der Kantone sowie Wissenschaftsexperten an.

2. Das BLW wies am 20. Mai 2009 die Einsicht der Antragstellerin in die verlangten Dokumente ab und begründete dies u.a. wie folgt: «Die Arbeitsgruppe setzt sich aus verschiedenen Vertretern von Privatorganisationen sowie zwei Vertretern von Kantonen zusammen. Die Arbeitsgruppe gehört somit nicht der Bundesverwaltung an und kann auch keine Erlasse oder erstinstanzliche Verfügungen erlassen. Sie untersteht folglich nicht dem BGÖ». Zudem hielt das BLW fest, das Gesuch könne auch nicht gutgeheissen werden, weil das Dokument nicht in seiner definitiven Fassung vorliege.

3. Die Antragsstellerin reichte am 2. Juni 2009 beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) einen Schlichtungsantrag ein.

4. Auf Ersuchen des Beauftragten übermittelte ihm das BLW am 22. Juni 2009 seine Stellungnahme. Die von der Antragsstellerin verlangten Dokumente reichte es jedoch nicht ein. Es hielt an seiner Einschätzung fest, wonach die Arbeitsgruppe nicht der Bundesverwaltung angehöre und damit nicht dem Öffentlichkeitsgesetz unterstehe. Weiter argumentierte das BLW: «Der Zugang zum FactSheet könnte auch nicht gewährt werden, wenn das betroffene Fact-Sheet ein amtliches Dokument gemäss BGÖ wäre. Gemäss Artikel 5 Absatz 3 Buchstabe b BGÖ besteht kein Anspruch auf Zugang zu einem Dokument, das noch nicht fertig gestellt ist. […] Die Arbeitsgruppe Begleitmassnahmen hat ihre Beratungen noch nicht abgeschlossen […], jedoch [wird] Anfang Juli 2009 die Schlussversion ihres Berichtes vorliegen. Anschliessend wird er dem EVD übergeben und veröffentlicht […].»

[1] Bericht Begleitmassnahmen zu einem Freihandelsabkommen im Agrar- und Lebensmittelbereich, S. 4
[2] Medienmitteilung vom 8. April 2008: Einsetzung der Arbeitsgruppe Begleitmassnahmen

5. Der Beauftragte verlangte am 25. Juni 2009 vom BLW die Zustellung der relevanten Dokumente und die Mitteilung, an welchem Datum der Arbeitsgruppenbericht veröffentlicht werde.

6. Das BLW teilte am 1. Juli 2009 mit der Bericht inkl. Factsheet werde im Internet am 8. Juli 2009 publiziert[3]. Am gleichen Tag übermittelte das BLW dem Beauftragten u.a. den ersten Berichtsentwurf (inkl. Factsheet) zum veröffentlichten Bericht.

7. Die Antragsstellerin erklärte am 11. Juli 2009 auf Anfragen des BLW hin, ihr Begehren um Einsicht in die vollständige Liste der Vorschläge sei nach wie vor hängig.

8. Am 22. Juli 2009 sandte das BLW dem Beauftragten u. a. das Begleitschreiben des BLW zum Bericht der Arbeitsgruppe sowie den Berichtsentwurf inkl. Anhang zu.

9. Nach telefonischer Nachfrage des Beauftragten beim BLW, ob die Liste mit 250 Vorschlägen existiere, übermittelte dieses am 28. Juli 2009 das Dokument «AG Begleitmassnahmen FHAL Synoptische Darstellung der Vorschläge» (nachfolgend Dokument Synopsis), die Einladung zur 2. Sitzung sowie die E-Mail vom 2. Oktober 2008. Gleichentags übermittelte das BLW zusätzlich das Protokoll der Arbeitsgruppe vom 12. Juni 2009 und teilte mit, «die AG [hat] klar festgehalten, dass sie keine Zwischenergebnisse ihrer Arbeit veröffentlichen will.»

10. Am 21. September 2010 lud der Beauftragte die Antragstellerin und das BLW zu einer Schlichtungssitzung ein. In der Folge teilte das BLW dem Beauftragten und der Antragsstellerin am 5. Oktober 2010 u.a. mit: «Einerseits haben wir Ihnen bereits am 22. Juni 2009 alle unsere Standpunkte erklärt und andererseits sehen wir uns an den Beschluss der Arbeitsgruppe Begleitmassnahmen vom 12. Juni 2009, in welcher die Arbeitsgruppe klar festgehalten hat, dass sie keine Zwischenergebnisse ihrer Arbeit veröffentlichen will, gebunden. Das Protokoll dieses Beschlusses haben wir Ihnen mit E-Mail vom 22. Juli 2009 [recte 28. Juli 2009] weitergeleitet. Ausserdem sind die politischen Diskussionen betreffend dem Freihandelsabkommen Schweiz-EU und somit auch betreffend der Begleitmassnahmen noch nicht abgeschlossen, weshalb die Zwischenergebnisse der Arbeitsgruppe Begleitmassnahmen auch nicht zugänglich gemacht werden können.»

11. Der Beauftragte führte am 2. November 2010 mit dem BLW ein Einzelgespräch, in welchen die konkreten Dokumente und deren Inhalte diskutiert wurden. In der Schlichtungssitzung vom 25. November 2010 einigten sich die Antragstellerin und das BLW dahingehend, dass das Zugangsgesuch betreffend Einsicht in das Factsheet mit 70 Vorschlägen durch deren Publikation am 8. Juli 2009 gegenstandslos geworden ist. In Bezug auf die Einsicht in die Sammlung der rund 250 Vorschläge konnte keine Einigung erzielt werden. Das BLW hielt an seiner Position der

[3] Bericht Begleitmassnahmen zu einem Freihandelsabkommen im Agrar- und Lebensmittelbereich

Zugangsverweigerung fest, während die Antragstellerin erklärte, sie sei lediglich an den eingereichten Vorschlägen interessiert, nicht aber daran, von wem welche Vorschläge eingereicht worden waren. Aufgrund der Nichteinigung in dieser Frage erlässt der Beauftragte eine Empfehlung.

12. Im Anschluss an diese Sitzung forderte der Beauftragte das BLW auf, ihm die Einsetzungsverfügung betreffend Arbeitsgruppe zuzustellen sowie zu erläutern, wie es zu deren Einsetzung gekommen ist. Das BLW teilte am 7. Dezember 2010 mit: «1. Das Eidgenössische Volkswirtschaftsdepartement EVD, d. h. die damalige Departementsvorsteherin, hat das BLW, d.h. den Direktor, im Hinblick auf ein allfälliges Freihandelsabkommen zwischen der Schweiz und der EU im Agrar- und Lebensmittelbereich oder eines möglichen WTO-Abschlusses mündlich beauftragt, alle aus ihrer Sicht wichtigen Organisationen der Land- und Ernährungswirtschaft und zwei Kantone einzuladen, ein gemeinsames Konzept für konkrete Massnahmen auszuarbeiten, mit denen die Betroffenen, insbesondere die Landwirte, beim Übergang in die neue Marktsituation unterstützt werden können. Das BLW lud in der Folge die durch die Departementsvorsteherin bestimmten Organisationen der Land- und Ernährungswirtschaft und zwei Kantone ein, Vertreter für eine Arbeitsgruppe zu bezeichnen, die ein solches Konzept erarbeitet. Eine Entlöhnung für diese Tätigkeit war nicht vorgesehen. 2. Nachdem die eingeladenen Organisationen und Kantone Vertreter bezeichnet hatten, organisierte das BLW die Treffen der Arbeitsgruppe und machte die Sekretariatsarbeiten. Entscheidungsbefugnis kam keinem Vertreter des BLW zu.»

   Ergänzend argumentierte das BLW: [D]ie Tatsache, dass die Dokumente der Arbeitsgruppe durch das BLW erstellt worden sind, ändert nichts daran, dass diese Dokumente der Arbeitsgruppe zuzurechnen sind und somit nicht dem BGÖ unterliegen.» [Weiter sei …]«zu berücksichtigen, dass das Dokument mit den 250 Vorschlägen einzig zum persönlichen Gebrauch der Arbeitsgruppenmitglieder bestimmt war. Es diente der Arbeitsgruppe als Hilfsmittel für die Erstellung des Arbeitsgruppenberichts. Dieses Dokument kann deshalb aus diesem Grund kein Dokument im Sinne des BGÖ sein. Schliesslich gibt es keinen sachlichen Grund, weshalb die Arbeitsgruppe anders behandelt werden sollte als andere Fachexperten, die einen Bericht oder Gutachten zuhanden der Bundesverwaltung erstellen. Ein Rechtsgutachter muss beispielsweise auch nicht damit rechnen, dass die Öffentlichkeit Zugang zu seinen Vorentwürfen und seinem Brainstorming erhält.» Zudem hielt das BLW fest, dass die Mitglieder der Arbeitsgruppe aufgrund des unter

Ziffer I. 9 erwähnten Beschlusses der Arbeitsgruppe darauf Vertrauen konnten, dass das Dokument nicht veröffentlicht werde. Seine Bekanntgabe, so das BLW weiter, beeinflusse möglicherweise auch die politische Diskussion über das Freihandelsabkommen Schweiz-EU und die Begleitmassnahmen negativ. Abschliessend erklärte das BLW, das Dokument enthalte eine Vielzahl von Personendaten, die nicht anonymisiert werden können: «Einzelne Branchenkenner können die Vorschläge ohne Weiteres den verschiedenen 15 Organisationen zuordnen. Der Zugang zu diesem Dokument ist somit aus Datenschutzgründen zu verweigern.

II. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zieht in Erwägung:

A. Schlichtungsverfahren und Empfehlung gemäss Art. 14 BGÖ

1. Gemäss Art. 13 BGÖ kann eine Person einen Schlichtungsantrag beim Beauftragten einreichen, wenn die Behörde den Zugang zu amtlichen Dokumenten einschränkt, aufschiebt oder verweigert, oder wenn die Behörde innert der vom Gesetz vorgeschriebenen Frist keine Stellungnahme abgibt.

   Der Beauftragte wird nicht von Amtes wegen, sondern nur auf Grund eines schriftlichen Schlichtungsantrags tätig.[4] Berechtigt, einen Schlichtungsantrag einzureichen, ist jede Person, die an einem Gesuchsverfahren um Zugang zu amtlichen Dokumenten teilgenommen hat. Für den Schlichtungsantrag genügt einfache Schriftlichkeit. Aus dem Begehren muss hervorgehen, dass sich der Beauftragte mit der Sache befassen soll. Der Schlichtungsantrag muss innert 20 Tagen nach Empfang der Stellungnahme der Behörde schriftlich eingereicht werden.

2. Die Antragstellerin hat ein Zugangsgesuch nach Art. 10 BGÖ beim BLW eingereicht und eine ablehnende Antwort erhalten. Als Teilnehmerin an einem vorangegangenen Gesuchsverfahren ist sie zur Einreichung eines Schlichtungsantrags berechtigt. Der Schlichtungsantrag wurde formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Empfang der Stellungnahme der Behörde) beim Beauftragten eingereicht.

3. Das Schlichtungsverfahren kann auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten stattfinden. Die Festlegung des Verfahrens im Detail obliegt alleine dem Beauftragten[5].

   Kommt keine Einigung zu Stande oder besteht keine Aussicht auf eine einvernehmliche Lösung, ist der Beauftragte gemäss Art. 14 BGÖ gehalten, aufgrund seiner Beurteilung der Angelegenheit eine Empfehlung abzugeben.

[4] BBl 2003 2023
[5] BBl 2003 2024

B. Sachlicher Geltungsbereich

1. Das Öffentlichkeitsgesetz gilt in erster Linie für die Bundesverwaltung (Art. 2 Abs. 1 Bst. a BGÖ), es findet aber ebenso Anwendung auf Expertenkommissionen, Arbeitsgruppen und andere Ad-hoc-Kommissionen, die von der Verwaltung für bestimmte Aufgaben eingesetzt werden[6].

   1.1 Entgegen der Ansicht des BLW ist für die Anwendbarkeit des Öffentlichkeitsgesetzes nicht massgeblich, ob sich eine Arbeitsgruppe aus Verwaltungsexternen, Verwaltungsinternen oder aus Vertretern beider Bereiche zusammensetzt. Wesentlich ist einzig, ob die Arbeitsgruppe von der Bundesverwaltung für eine bestimmte Aufgabe eingesetzt wurde. Dabei ist unerheblich, ob die Arbeitsgruppe eine beratende oder entscheidende Funktion hatte oder ob ihre Mitglieder ihr Fachwissen der Verwaltung unentgeltlich oder gegen Bezahlung zur Verfügung gestellt haben.

   Die hier zu beurteilende Arbeitsgruppe ist ein vom EVD eingesetztes Gremium, welches den Auftrag hatte, unter der Leitung des BLW Begleitmassnahmen hinsichtlich eines allfälligen Freihandelsabkommens im Agrar- und Lebensmittelbereich zu erarbeiten. Die Mitglieder dieser Arbeitsgruppe, d.h. die darin vertretenen Organisationen sowie die beiden Kantonsvertreter, sind gemäss Angaben des BLW von der Departementsvorsteherin explizit aufgrund ihres Expertenwissens ausgewählt worden. Als Branchenvertreter und Betroffene konnten sie direkt Einfluss auf mögliche Begleitmassnahmen nehmen, indem sie für das EVD nach dessen Vorgaben den entsprechenden Bericht und das Factsheet erstellten.

   Demzufolge ist die vom EVD angeordnete Arbeitsgruppe der Bundesverwaltung im Sinne von Art. 2 Abs. 1 Bst. a BGÖ zuzurechnen.

2. Die Arbeitsgruppe hat an ihrer Sitzung vom 12. Juni 2010 – nachdem sie Kenntnis vom Eingang eines Zugangsgesuches bekommen hatte – beschlossen, keine Zwischenergebnisse zu veröffentlichen. Mit Verweis auf diesen Entscheid begründete das BLW seine Zugangsverweigerung und hielt fest, es sei daran gebunden. Die Arbeitsgruppe dürfe darauf vertrauen, dass keine Zwischenergebnisse veröffentlicht werden. Schliesslich werde nur der definitive Bericht die Meinung der Arbeitsgruppe zeigen.

   2.1 In diesem Zusammenhang ist klar festzuhalten, dass dem Transparenzprinzip unterliegenden Stellen (Departemente, Bundesämter, alle Arbeits- und Expertengruppen, Gutachter etc.) *nicht in eigener Kompetenz* entscheiden können, von

[6] Empfehlung vom 12. Februar 2010: BAG / Interessenerklärungen von Kommissionsmitgliedern (EKIF), Bundesamt für Justiz, Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen, Ziffer 2. 4 (Stand 25. Februar 2010)

ihnen erstellte Dokumente vom Öffentlichkeitsgesetz auszuschliessen. Vielmehr muss bei einem konkreten Zugangsgesuch nach den Vorgaben dieses Gesetzes jeweils geprüft werden, ob ein amtliches Dokument vorliegt (Art. 5 BGÖ) und ob allenfalls einer der gesetzlichen Ausnahmegründe (Art. 7 BGÖ und Art. 8 BGÖ) die Vermutung des Dokumentenzugangs umzustossen vermag.

Die von der Arbeitsgruppe erstellten Dokumente sind nach Vorgaben des Öffentlichkeitsgesetzes zu beurteilen.

3. Das BLW macht geltend, dass das Dokument Synopsis einerseits nicht fertig gestellt (Art. 5 Abs. 3 Bst. b BGÖ) und andererseits zum persönlichen Gebrauch bestimmt sei (Art. 5 Abs. 3 Bst. c BGÖ).

3.1 Nach Art. 5 BGÖ liegt ein amtliches Dokument vor, wenn folgende drei Voraussetzungen kumulativ erfüllt sind: Die Information muss auf einem beliebigen Informationsträger aufgezeichnet sein (Art. 5 Abs. 1 Bst. a BGÖ); sie muss sich im Besitz einer Behörde befinden (Art. 5 Abs. 1 Bst. b BGÖ), und sie muss der Erfüllung einer öffentlichen Aufgabe dienen (Art. 5 Abs. 1 Bst. c BGÖ). Nicht als amtlich gelten nach Art. 5 Abs. 3 BGÖ Dokumente, welche durch eine Behörde kommerziell genutzt werden (Bst. a), nicht fertig gestellt (Bst. b) oder zum persönlichen Gebrauch bestimmt sind (Bst. c).

In die Kategorie der Dokumente, die zum persönlichen Gebrauch bestimmt sind (Art. 5 Abs. 3 Bst. c BGÖ), fallen alle Informationen, die dienstlichen Zwecken dienen, deren Benutzung jedoch ausschliesslich dem Autor bzw. der Autorin oder einem eng begrenzten Personenkreis vorbehalten ist (Art. 1 Abs. 3 der Verordnung über das Öffentlichkeitsprinzip der Verwaltung, Öffentlichkeitsverordnung, VBGÖ, SR 152.31): z.B. handschriftliche Notizen, Korrektur-vorschläge, Kurzzusammenfassungen, Gedankenstützen, Sitzungs- und Arbeitsnotizen etc. die als Arbeitsgrundlage oder Arbeitshilfsmittel, die höchstens innerhalb eines Teams oder zwischen Mitarbeiterinnen und Mitarbeitern und Vorgesetzten ausgetauscht werden[7]. Wesentlich ist, ob die zum persönlichen Gebrauch bestimmten Dokumente das Kriterium des Arbeitshilfsmittels erfüllen. Mit anderen Worten muss es sich um Dokumente handeln, die im Rahmen eines Arbeits- und Entwicklungsprozesses entstanden sind[8].

Der im Internet veröffentlichte Bericht der Arbeitsgruppe erläutert den Prozessablauf des Auftrags. Demnach erhielt die Arbeitsgruppe vom BLW den Auftrag, auf die zweite Sitzung vom 8. Oktober 2008 hin konkrete Vorschläge zu Begleitmassnahmen einzureichen. In dieser Sitzung «[präsentierten] die Mitglieder […] diese

[7] Erläuterungen zur Verordnung über das Öffentlichkeitsprinzip der Verwaltung Ziffer 2; Handkommentar BGÖ, Art. 5 RZ 39

[8] Empfehlung vom 3. April 2009: ESTV / Cockpits und Amtsreportings, II. B 7

Vorschläge […] und ihre strategischen Überlegungen. Anschliessend wurde eine erste Diskussion zu den Massnahmen geführt, welche Hinweise gab, wie die rund 250 eingereichten Vorschläge in einem ersten Schritt gruppiert werden können. Das Sekretariat erarbeitete auf der Basis dieser Diskussion eine erste Synthese der Vorschläge und unterbreitete diese den Mitgliedern zur Beurteilung». Aus diesem Bericht und der zugestellten Unterlagen ergibt sich, dass das BLW nicht nur Sekretariatsarbeiten für die Arbeitsgruppe ausführte, sondern vielmehr selber substantiell, materiell und inhaltlich aktiv war. Es sammelte die eingereichten Vorschläge, teilte diese systematisch in sechs Kategorien ein, versah jeden Vorschlag mit drei Bewertungsmöglichkeiten (breite, mittlere und geringe Unterstützung) und forderte die Mitglieder der Arbeitsgruppe auf, jeden Vorschlag entsprechend zu gewichten. Das vom BLW so gestaltete Dokument Synopsis diente daher nicht als Arbeitsgrundlage zum Austausch unter den Arbeitsgruppenmitgliedern zwecks Korrektur, Ergänzung oder Finalisierung, sondern es wurde ihnen zur Bewertung der einzelnen Vorschläge übergeben. Auch enthält das Dokument keinerlei persönliche Notizen, Anmerkungen oder Korrekturen. Das Kriterium des Arbeitshilfsmittels ist also nicht erfüllt. Zudem war das Dokument nie einem eng begrenzten Personenkreis vorbehalten, sondern wurde an die 15 Organisationen sowie die zwei Kantone übergeben.

Demzufolge ist das Dokument Synopsis kein zum persönlichen Gebrauch bestimmtes Dokument.

3.2 Weiter gilt es zu klären, ob das Dokument Synopsis fertig gestellt ist (Art. 5 Abs. 3 Bst. b BGÖ e contrario). Gemäss der Verordnung zum Öffentlichkeitsgesetz gilt ein Dokument dann als fertig gestellt, wenn es vom Ersteller unterzeichnet ist oder dem Adressaten zur Kenntnis- oder Stellungnahme oder als Entscheidungsgrundlage definitiv übergeben (Art.1 Abs. 2 Bst. a und b VBGÖ. Es gilt auch festzuhalten, dass sogar Vor- oder Teilentwürfe eines Dokumentes fertig gestellte Dokumente sein, sofern sie in sich selber abgeschlossen sind[9].

Das Dokument Synopsis wurde auf dem offiziellen Papier des BLW erstellt, trägt die Referenz dreier BLW-Mitarbeitenden und wurde im Dokumentensystem[10] des BLW unter Referenz/Aktenzeichen: 2008-06-18/177/gro/tha/msa abgelegt. Es zeigt den ersten, abgeschlossenen Arbeitsschritt der Arbeitsgruppe, nämlich das Sammeln der Vorschläge. In seiner strukturierten Form und mit den Bewertungsmöglichkeiten ist es im Prozessablauf des EVD-Auftrags als ein in sich abgeschlossenes Dokument zu betrachten. Entscheidend ist, dass es definitiv übergeben wurde

[9] BBl 2003 1999
[10] BBl 2003 1998

und die Adressaten, nämlich die Mitglieder der Arbeitsgruppe, frei entscheiden konnten, wie sie mit dem Dokument weiter verfahren, d.h. wie sie die Vorschläge bewerten und eingrenzen[11].

Das Dokument Synopsis ist ein fertig gestelltes, definitives und damit ein amtliches Dokument im Sinne von Art. 5 BGÖ.

4. Das BLW deutete in seinen Stellungnahmen verschiedene Ausnahmegründe an. Es blieb in seiner Argumentation indes zu allgemein (z. B. «Gefährdung der politischen Diskussion») und begründete im Einzelnen nicht, ob, inwieweit und welche gesetzlichen Ausnahmen nach Art. 7 Abs. 1 BGÖ oder nach Art. 8 BGÖ den Zugang zum Dokument Synopsis ausschliessen[12].

   4.1 Für den Beauftragten ist indes kein Ausnahmegrund für eine Einschränkung des Zugangs ersichtlich. In Bezug auf die vom BLW angedeuteten Ausnahmen gilt es festzuhalten:

   - Die Arbeitsgruppe ist Teil der Bundesverwaltung. Deshalb entfällt die Möglichkeit der Zusicherung der Geheimhaltung gemäss Art. 7 Abs. 1 Bst. h BGÖ.
   - Die Arbeitsgruppe hat den Auftrag des EVD unter der Leitung des BLW erfüllt, und mit der Veröffentlichung ihres Schlussberichts (inkl. des Factsheets mit den 70 Vorschlägen) ist die freie Meinungs- und Willensbildung der Arbeitsgruppe abgeschlossen (Art. 7 Abs. 1 Bst. a BGÖ).
   - Blosse Unannehmlichkeiten, wie etwa allfällige politische Diskussionen, rechtfertigen keine Zugangsverweigerung und stellen per se noch keine wesentliche Beeinträchtigung im Sinne von Art. 7 Abs. 1 Bst. a BGÖ dar[13]:
   - Die Arbeitsgruppe hat mit der Veröffentlichung des Schlussberichts (inkl. des Factsheets) ihre (politischen und administrativen) Entscheide gefällt (Art. 8 Abs. 2 BGÖ).
   - Das Dokument Synopsis enthält keine Positionen, die unmittelbar bevorstehende Verhandlungen gefährden könnten (Art. 8 Abs. 4 BGÖ).

[11] Handkommentar BGÖ, Art 5 RZ 34
[12] Zur Beweislast der Bundesbehörden führt das Bundesverwaltungsgericht aus: «Wird der Zugang zu amtlichen Dokumenten verweigert, so obliegt der Behörde die Beweislast zur Widerlegung der Vermutung des freien Zugangs zu amtlichen Dokumenten, die durch das Öffentlichkeitsgesetz aufgestellt wird, d.h. sie muss beweisen, dass die Ausnahmebedingungen gegeben sind, die in den Art. 7 und 8 BGÖ festgelegt sind […].» (Urteil vom 18. Oktober 2010, Referenz A-3443/2010, Erw. 3.1)
[85] BBl 2003 2007; Handkommentar BGÖ, Art. 7 RZ 15

5. Das BLW führte schliesslich aus, das Dokument Synopsis enthalte Personendaten, die nicht anonymisiert werden könnten. Einzelne Brachenkenner könnten die Vorschläge ohne weiteres den jeweiligen Organisationen zuordnen, weshalb der Zugang zu diesem Dokument zu verweigern sei.

   5.1 Dokumente, die Personendaten enthalten, sind nach Möglichkeit vor der Einsichtnahme zu anonymisieren (Art. 9 Abs. 1 BGÖ). Ist eine Anonymisierung nicht möglich, so beurteilt sich der Zugang nach den Vorschriften über die Bekanntgabe von Personendaten durch Bundesorgane (Art. 9 Abs. 2 BGÖ i.V.m. Art. 19 des Bundesgesetzes über den Datenschutz, DSG, SR 235.1).

   5.2 Vorliegend handelt es sich um Personendaten der in der Arbeitsgruppe vertretenen Organisationen sowie um die Kürzel der drei BLW-Mitarbeiter in der Dokumentenreferenz. Die Antragstellerin hielt in der Schlichtungssitzung wiederholt fest, sie interessiere sich einzig für die eingereichten Vorschläge, nicht jedoch welche der Arbeitsgruppenmitglieder welche Vorschläge eingereicht habe. Das Argument des BLW, wonach trotz Anonymisierung die Vorschläge den Organisationen zugeordnet werden könnten, überzeugt nicht. Deshalb sind die Personendaten zu anonymisieren, d.h. im Dokument Synopsis in der Spalte «Organisation» einzuschwärzen. Die Personendaten der BLW-Mitarbeiter sind nicht zu anonymisieren[14]. Die Personen-daten kantonaler Behördenmitglieder sind nach kantonalen Bestimmungen zu den Öffentlichkeitsgesetzen zu beurteilen

   Die Personendaten in der Spalte «Organisation» sind einzuschwärzen und der Zugang zum Dokument Synopsis ist in dieser Form zu gewähren.

III. Aufgrund dieser Erwägungen empfiehlt der Datenschutz- und Öffentlichkeitsbeauftragte:

1. Das Bundesamt für Landwirtschaft anonymisiert das Dokument Synopsis, indem es dessen Spalte «Organisation» einschwärzt, und gewährt den Zugang zum Dokument Synopsis.
2. Das Bundesamt für Landwirtschaft erlässt eine Verfügung nach Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG, SR 172.021), wenn es in Abweichung von Ziffer 1 den Zugang nicht gewähren will.
3. Das Bundesamt für Landwirtschaft erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung (Art. 15 Abs. 3 BGÖ).

[13] Handkommentar BGÖ, Art. 7 RZ 80 mit weiteren Hinweisen

4. Die Antragstellerin kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Bundesamt für Landwirtschaft den Erlass einer Verfügung nach Art. 5 VwVG verlangen, wenn sie mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

5. Gegen die Verfügung kann die Antragstellerin beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

6. In Analogie zu Art. 22a VwVG stehen gesetzliche Fristen, die nach Tagen bestimmt sind, vom 18. Dezember bis und mit dem 2. Januar still.

7. Diese Empfehlung wird veröffentlicht. Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten wird der Name der Antragstellerin anonymisiert (Art. 13 Abs. 3 VBGÖ).

8. Die Empfehlung wird eröffnet:

   - X
   - Bundesamt für Landwirtschaft

     3000 Bern

Jean-Philippe Walter