Tätigkeitsbericht

Datenschutzbeauftragter des Fürstentums Liechtenstein

2006

Inhaltsverzeichnis

1. Vorwort **3**
2. Allgemeines und Prioritäten **5**
3. Information **6**
3.1. Information der Öffentlichkeit durch den Datenschutzbeauftragten 6
3.2. Informationspflichten von Dateninhabern 8
4. Beratung **9**
4.1. Unterstützung von privaten Personen und Behörden durch allgemeine Orientierungen und Beratungen 9
4.2. Stellungnahmen zu Datenschutzfragen in hängigen Verfahren vor Rechtsmittelbehörden – Rechtsprechung zum Datenschutzgesetz 11
4.3. Begutachtung der Gleichwertigkeit des ausländischen Datenschutzes 11
4.4. Stellungnahme zu Vorlagen und Erlassen 11
4.5. Projektbegleitung 13
5. Aufsicht **15**
5.1. Aufsicht über Behörden 15
5.1.1. Datenschutzwidrige Bearbeitungen 15
5.1.1.1. Datenbanken 15
5.1.1.2. Anderes 16
5.1.2. Gesetzliche Grundlagen 17
5.2. Abklärungen und Empfehlungen im Privatrechtsbereich 17
6. Register der Datensammlungen **19**
7. Internationales **20**
7.1. Art. 29 Arbeitsgruppe der Richtlinie 95/46/EG 20
7.2. Vereinigung der Schweizerischen Datenschutzbeauftragten 22
7.3. Europarat 23
7.4. Europäische Datenschutzkonferenz 24
7.5. Internationale Datenschutzkonferenz 24
8. Personelles und Organisatorisches **25**
9. Ausblick **26**
Anhang **27**

1. Vorwort

Der 4. Tätigkeitsbericht liegt hiermit vor. Dieser Tätigkeitsbericht des Datenschutzbeauftragten (DSB) soll die Öffentlichkeit über die Tätigkeiten des vergangenen Jahres informieren und damit auch dazu beitragen, dass das Bewusstsein zum Datenschutz gestärkt wird.

Einer der Schwerpunkte des vergangenen Jahres bestand wie im Vorjahr in der Information der Öffentlichkeit zu verschiedenen Themen: Auf der Internet-Seite wurden Schulungsunterlagen zum Datenschutz verfügbar gemacht oder auch Tipps gegeben wie in den Ferien möglichst wenige Datenspuren hinterlassen werden können. Die Technik entwickelt sich rasant. Damit sind auch Möglichkeiten gegeben, leichter Datenbearbeitungen vornehmen zu können und Daten zu verknüpfen. In diesem technischen Bereich wurden Informationen zu den Bereichen Suchmaschinen auf dem Internet, Telefonieren mit Internet-Technologie (VoIP), Phishing-Mails oder auch Dokumenten-Managementsysteme (DMS) auf der Internet-Seite verfügbar gemacht. Weiters wurden neben den Richtlinien für die Bearbeitung von Personendaten durch Behörden Richtlinien über technische und organisatorische Massnahmen erstellt, welche das Datenschutzgesetz (DSG) fordert (siehe dazu unten, 3.1.).

Die Anfragen, welche an die Stabsstelle für Datenschutz (SDS) gerichtet werden, zeigen nach wie vor ein sehr breites Spektrum auf. So kommt es immer wieder vor, dass nach den zulässigen Bedingungen der Errichtung von Familienstammbüchern, der Internet- und Emailüberwachung des Arbeitnehmers am Arbeitsplatz, der Auslagerung von Datenbearbeitungen, der Datenbekanntgabe ins Ausland oder der Veröffentlichung von Personendaten auf dem Internet gefragt wird. Weitere Fragen beziehen sich etwa auf den Gesundheitsbereich, auf Werbung oder Spam oder darauf, ob das Datenschutzgesetz (DSG) auch verstorbene Personen schützt (siehe dazu unten, 4.1.). Das Berichtsjahr war auch geprägt durch verschiedene wichtige gesetzgeberische Vorhaben. Hierzu erfolgten Stellungnahmen unter anderem zur Änderung des Bankengesetzes, des Invalidenversicherungsgesetzes, des Heimatschriftengesetzes, des Polizeigesetzes oder des Krankenversicherungsgesetzes. Auch das Datenschutzgesetz wäre in verschiedenen Punkten anzupassen (siehe dazu unten, 4.4.).

Im Aufsichtsbereich ist unter anderem zu erwähnen, dass die Zentrale Personenverwaltung (ZPV) als eine zentral geführte Datenbank der Landesverwaltung nach wie vor Probleme aufweist. Die Zunahme von Installationen der Videoüberwachung ist auch in Liechtenstein festzustellen. Dabei geht es vor allem um das vermehrte Bedürfnis von Behörden, eine Videoüberwachung einzurichten. Eine Einrichtung von Webcams kann einer Videoüberwachung im Prinzip gleich gestellt werden. Der Zugriff von U.S. Behörden auf Daten im Rahmen internationaler Bankzahlungen (SWIFT-Affäre) ist in ganz Europa ein Thema. Und damit auch in Liechtenstein (siehe dazu unten, 5.).

Dieser Zugriff der U.S. Behörden auf Bankzahlungsdaten stellt auch den Schwerpunkt der Datenschutzarbeitsgruppe in Brüssel im internationalen Bereich dar. Weiters zu nennen ist etwa das Thema «Whistle Blowing». Im Rahmen der Vereinigung der Schweizerischen Datenschutzbeauftragten wurden unter anderem die auch in Liechtenstein wichtigen Themen «Vertrauensarzt – Wie vertrauenswürdig ist der Vertrauensarzt?» und «Gesundheitskarte: Patientendossier im Portemonnaie?» thematisiert (siehe dazu unten, 7.).

Das DSG ist am 1. August 2007 fünf Jahre in Kraft. In dieser Zeit konnte Einiges erreicht werden. Doch gilt es nach wie vor, das Bewusstsein für den Schutz der Privatsphäre zu stärken. Der Datenschutz wird ab und zu missverstanden oder gar missbraucht. Die Gefahren für den Schutz der Privatsphäre bei der Bearbeitung von Daten bei Kreditanträgen wie auch auf dem Internet bilden einen Teil der Bewusstseinsbildung für die Zukunft. Das Internet hat zu revolutionären Veränderungen in der Gesellschaft geführt. Diese Änderungen sind aber nicht nur von Vorteil für die betroffenen Personen. Besonders beunruhigend ist die Entwicklung zum Identitätsdiebstahl. Nach einer im März veröffentlichten Studie betreffen 93 % der Internetangriffe normale Heimanwender. Das Internet ist ein Spiegel des Lebens. Es enthält somit richtige wie auch falsche oder gar verleumderische Angaben. Ein vorsichtiger Umgang mit Personendaten auf dem Internet ist auch deshalb angezeigt, da unrichtige Angaben nicht gelöscht werden können.

Die automatisierte Bearbeitung von Daten ist alltäglich geworden, bringt aber neben Vorteilen auch Gefahren für die Privatsphäre mit sich. Es wird wichtig sein, im Rahmen von ver-

schiedenen Informatikvorhaben, bei denen die SDS beteiligt ist, weiterhin auf die Bedeutung der Privatsphäre hinzuweisen. Die automatisierte Datenbearbeitung ist auch im Gesundheitswesen ein Thema, das Aufmerksamkeit verdient. Die bisherige Praxis hat gezeigt, dass nach wie vor ein Bedürfnis für den rechtmässigen Umgang mit medizinischen Daten im Allgemeinen besteht. Deshalb wird es wichtig sein, Richtlinien unter anderem zu diesem Thema wie auch zu den Rahmenbedingungen der Datenbearbeitung durch private Personen abzuschliessen.

Mit dem neuen Polizeigesetz wurde ein indirektes Auskunftsrecht geschaffen, welches an den DSB zu richten ist. Dies setzt eine verstärkte Zusammenarbeit mir der Polizei voraus, bindet aber auch Ressourcen für die Auskunftserteilung wie Erfahrungen im benachbarten Ausland gezeigt haben. Dazu wirft auch ein möglicher Beitritt Liechtensteins zum Schengener Übereinkommen seine Schatten voraus.

Insgesamt gilt es, ein Gleichgewicht zwischen dem Recht auf Achtung der Privatsphäre und entgegen gesetzten Interessen zu finden. Um dieses Ziel zu erreichen ist ein entsprechendes Bewusstsein in der breiten Öffentlichkeit wie auch bei den Daten bearbeitenden Stellen und Personen ein wichtiges Element.

Vaduz, im Juni 2007

Dr. Philipp Mittelberger
Datenschutzbeauftragter

2. Allgemeines und Prioritäten

Im letzten Tätigkeitsbericht wurden folgende Prioritäten für 2006 festgelegt:

- Schaffung von Informationen über den Datenschutz allgemein;
- Schaffung von Informationen über die Rechte nach dem DSG;
- öffentliche Veranstaltung zum Datenschutz;
- allgemeine Informationsbroschüre;
- Tätigkeiten aufgrund eines möglichen Beitritts Liechtensteins zu den Abkommen von Schengen und Dublin.

Dazu waren noch verschiedene Pendenzen aus dem Vorjahr zu erledigen.

- Abschluss von Informationsmaterial bezüglich der Bedingungen für die Bearbeitung von Personendaten durch Behörden;
- Informationen für die Bearbeitung durch Private;
- die Arbeiten an einer gesetzlichen Grundlage für die ZPV;
- Schaffung eines Bearbeitungsreglements zur ZPV;
- die Überprüfung der richtigen Umsetzung der Zugriffsbewilligung auf Felder der Personenübersichtsmaske der ZPV.

Nicht vollendet werden konnten im Berichtsjahr: die allgemeinen *Informationen* für die Datenbearbeitung durch *private Personen*, die Mitarbeit zu einer *gesetzlichen Grundlage zur ZPV* sowie ein Bearbeitungsreglement zur ZPV. Diese Arbeiten werden 2007 abzuschliessen sein. Ein Beitritt Liechtensteins zu den Abkommen von *Schengen / Dublin* steht nicht in naher Zukunft bevor. Deshalb werden diesbezügliche Vorbereitungsaktivitäten noch zu erfolgen haben.

3. Information

Eine wichtige gesetzliche Aufgabe des DSB besteht in der Schaffung und Verbesserung eines **Datenschutzbewusstseins** der Bevölkerung und der Dateninhaber, also derjenigen Behörden und Personen, welche Daten bearbeiten.

3.1. INFORMATION DER ÖFFENTLICHKEIT DURCH DEN DATENSCHUTZBEAUFTRAGTEN

Die **Internetseite** der SDS ist die Plattform, die über aktuelle und/oder wichtige Themen informiert. Diese betrafen folgende Themenbereiche:

- *Telefonieren mit Internettechnologie (VoIP)*[1] wird zunehmend zu einem ernsthaften Konkurrenten der klassischen leitungsverbundenen Telefonie. Im Unterschied zur klassischen Telefonie wird für die Übertragung der Sprachdaten keine eigene Leitung speziell für diesen Dienst eingesetzt, sondern das Internet dient als Kommunikationsplattform. Daten und Sprache nutzen die gleichen Leitungen. Somit übertragen sich die Sicherheitsprobleme der Datennetzwerke auf die IP-Telefonie. Ohne zusätzliche Massnahmen kann keine qualitätsgesicherte Übertragung sichergestellt werden.[2] Es ist notwendig, das Kommunikationsgeheimnis auch bei der Internet-Telefonie zu wahren. Hierfür müssen angemessene technische und organisatorische Massnahmen definiert werden, um eine sichere und datenschutzfreundliche Nutzung solcher Dienste zu ermöglichen.[3] Dazu sollten die Betreiber ihre Kunden über die Gefahren und Einschränkungen gegenüber der klassischen Telefonie informieren.
- Die Bearbeitung von Personendaten ist auch vor und während der *Ferien* oft gegeben: Die automatisierte Datenbearbeitung ist mittlerweile die Regel. Leider kommt es immer wieder zu so genannten Identitätsdiebstählen. Damit im Ausland, wo vielleicht nicht der gleiche Datenschutz besteht wie in Liechtenstein, möglichst wenige elektronische Spuren hinterlassen werden, bietet es sich an, mit der Freigabe der eigenen Daten sparsam umzugehen.
- Bei *Spionprogrammen* handelt es sich um ein leistungsstarkes System zur heimlichen Überwachung des Verhaltens von Benutzern an Computern. Ausser der Aufzeichnung von eingehenden und ausgehenden E-Mails ist auch eine Aufzeichnung von Bildschirminhalten, Tastaturschlägen oder besuchten Web-Seiten möglich.[4] Spionprogramme dienen oft dem Indentitätsdiebstahl oder auch etwa der unerlaubten Leistungs- und Verhaltenskontrolle des Arbeitnehmers.
- Anliegen eines *Lernprogramms zur Datensicherheit*[5] ist die Stärkung des Bewusstseins zur sicheren Nutzung von Daten und Dokumenten bei der Benutzung des Computers. So ziehen zum Beispiel unbeaufsichtigte Arbeitsplätze und Computer neugierige Blicke an und können zum Datenmissbrauch einladen. Disketten und andere portable Datenträger werden zur leichten Beute für Informationsdiebe. Das Programm soll zum sicheren Umgang mit Personendaten anregen.
- *Suchmaschinen auf dem Internet* sind ein Schlüssel und damit ein unverzichtbares Werkzeug zu Informationen geworden, welche sich auf dem Internet befinden. Anbieter von Suchmaschinen haben die Möglichkeit, detaillierte Interessenprofile ihrer Nutzer aufzuzeichnen. Wichtig in diesem Zusammenhang ist aus Datenschutzsicht, dass die Anbieter von Suchmaschinen die Nutzer zum Vornherein in transparenter Weise über die Datenbearbeitung informieren[6] und die Suchmaschinen datenschutzfreundlich einrichten.
- *«Hooliganismus, Fussball-WM und Datenschutz»* war das Thema der Frühjahrstagung der Schweizerischen Datenschutzbeauftragten.[7] Dabei wurden die Themen Hooligan-Datenbank, Videoüberwachung und auch personifizierte Tickets behandelt.
- Die Dokumentation zur Durchführung einer *landesverwaltungsinternen Schulung* zum Datenschutz enthält einen

[1] VOIP bedeutet Voice-Over-IP und ist ein Sprachtelefonie-Dienst auf der Basis von Internetstandards. Solche Dienste werden meist auch als IP-Telefonie oder Internet-Telefonie bezeichnet. Dies bedingt eine Integration von Sprache und Daten in ein gemeinsames Netzwerk.

[2] Dies bedeutet, dass das Abhören von Gesprächen und Denial-of-Service-Angriffe (z.B. durch mehrmaliges Versenden von Klingelrundrufen an mehrere Teilnehmer gleichzeitig) mit bereits existierender Software, wie z.B. Paket-Sniffern, durchgeführt werden können. Ein weiteres Problem ist die Möglichkeit, Identitäten zu fälschen und damit Phishing oder Spamming zu vereinfachen. Es gibt auch zahlreiche Skripte/Programme für Angriffsmöglichkeiten wie für das Suchen von VoIP-Geräten oder das Umleiten der Sprachdaten.

[3] Dies verlangt Verschlüsselungsverfahren für die IP-Telefonie. Sicherheits- und Datenschutzmängel, die die verwendeten Protokolle oder die genutzte Software mit sich bringen, müssen möglichst schnell behoben werden. Weiters sollte darauf geachtet werden, dass offene und standardisierte Lösungen (Protokolle, Algorithmen) eingesetzt werden. Um eine datenschutzfreundliche Nutzung der IP-Telefonie zu erreichen, müssen auf den Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten angemessene Sicherheitsmassnahmen bereitgestellt werden.

[4] Ein Beispiel von Spionprogrammen stellen so genannte Content Scanners dar. Ein Content Scanner ist eine Software, welche die gesendeten und/oder empfangenen E-Mails nach bestimmten vordefinierten Stichwörtern auswertet und entsprechend reagiert (z. B. Sperrung, Löschung, Kopie an Systemadministrator oder gar an Vorgesetzten).

[5] Vgl. *http://www.datenschutz.ch/wbt/sicherheit; vgl. auch unten, 3.2.*

[6] Vgl. dazu Tätigkeitsbericht 2005, 3.2.

[7] Vgl. unten, 7.2.

theoretischen Teil über die Anwendung des Gesetzes bei der Arbeit durch Behörden wie auch einen praktischen Teil zu aktuellen Fällen in Liechtenstein.

- Der Europäische Gerichtshof (EuGH) kam in einem Urteil zum Schluss, dass das Abkommen zwischen der EU und der USA zum *Transfer von Flugpassagierdaten* illegal ist. Dies gilt auch für Transfers in Bezug auf liechtensteinische Flugpassagiere.[8]
- *Dokumentenmanagementsysteme (DMS)* dienen der Einführung des «papierlosen Büros». Mit dem DMS werden vorhandene Dateien (Dokumente, Bilder etc.) elektronisch verwaltet und bearbeitet. Mit einer solchen umfassenden elektronischen Bearbeitung besteht auch die Möglichkeit der erleichterten Suche und Verknüpfung von Dateien. Damit stellen sich Gefahren für die Privatsphäre.[9]

Ausführlichere Informationen zu diesen Themenbereichen sind auf der Internetseite[10] verfügbar.

Das DSG ist naturgemäss abstrakt gehalten und auch die Datenschutzverordnung (DSV) gibt nur wenig konkrete Anhaltspunkte für die Handhabung des Datenschutzes in der Praxis. Deshalb erschien es sinnvoll, aufgrund von entsprechenden Informationen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) *Richtlinien für die Bearbeitung von Personendaten durch Behörden*[11] heraus zu geben. Damit soll den Behörden entsprechende Leitplanken gesetzt werden, die einer konkreten Handhabung des Gesetzes dienlich sind. Dasselbe wurde zum Thema technische und organisatorische Massnahmen gemacht, da das DSG wie auch die DSV mehr oder weniger detailliert *technische und organisatorische Massnahmen*[12] zur Datensicherheit verlangen.

Richtlinien zur Bearbeitung von medizinischen Daten wie auch ein *Kommentar zu den Bestimmungen der DSV* konnten nicht abgeschlossen werden. Dies wird 2007 nachzuholen sein.

In einer **Pressemitteilung** wurde auf die Problematik von so genannten *Phishing-Mails* hingewiesen. Dabei geht es darum, dass insbesondere beim Online-Banking, bei Internet-Auktionen oder Versandhäusern auf eine betrügerische Art und Weise vertrauliche Zugangsdaten (wie Passwort, Kontonummer, PIN, Kreditkartennummern, usw.) vor allem durch offiziell wirkende E-Mails abgefangen werden. Solche E-Mails sind oft als Sicherheitsupdates, Checks und dergleichen getarnt und machen auf den ersten Blick einen vertrauenswürdigen Eindruck. Bei diesen Phising-Mails[13] geht es um eine Art des *Identitätsdiebstahls*. Phishing stellt ein zunehmendes Problem dar. Obwohl es in Liechtenstein noch keine bekannten (Schaden) Fälle gab, war es dem DSB ein Anliegen auf dieses Problem öffentlich hinzuweisen, damit Schadenereignisse möglichst vermieden werden können. Bei E-Mails, mit denen ein Benutzer um die Angabe von vertraulichen Zugangsdaten gebeten wird, ist somit Vorsicht angebracht. Es kann ausgeschlossen werden, dass diese ehrlich gemeint sind. Es bietet sich an, den angeblichen Absender einer E-Mail auf diese Problematik hinzuweisen, damit das betroffene Unternehmen seine Kunden darüber informieren kann. Weiters sollten im E-Mail angegebene Links auf eine Internetseite nicht benutzt werden, da diese zu einer falschen Internetseite führen können. Die Einführung von *Tarmed* war nach wie vor[14] ein wichtiges Thema. Der DSB wurde hierzu bei den datenschutzrelevanten Aspekten beigezogen und äusserte sich dazu öffentlich unter anderem in einer Pressemitteilung. Dabei unterbreitete der DSB Vorschläge wie die datenschutzrechtliche Situation im Bereich der sozialen Krankenversicherung auf Gesetzesebene verbessert werden könnte. Insbesondere der Vorschlag der Angleichung der rechtlichen Stellung des Vertrauensarztes an die gesetzliche Lage in der Schweiz wurde sowohl durch den Krankenkassenverband als auch durch die Ärztekammer begrüsst. Dieser wie auch andere Vorschläge wurden später durch die Regierung in einem Vernehmlassungsbericht zur Änderung des Krankenversicherungsgesetzes[15] aufgenommen.

Die **Medien** gelangten im Vergleich zum Vorjahr erneut vermehrt an die SDS. Dabei ging es um Themen wie die Einführung der *Videoüberwachung* in der Fussgängerzone in Vaduz.[16] Der Zugriff von US Behörden auf Daten von internationalen Banktransfers *(SWIFT-Affäre)*[17] war Anfang des Jahres nebst

[8] Vgl. unten, 7.1.
[9] Vgl. dazu unten, 4.5., und Tätigkeitsbericht 2005, 4.5.
[10] *www.sds.llv.li*
[11] *http://www.llv.li/pdf-llv-sds-richtlinien_zur_bearbeitung_von_personendaten_durch_behoerden.pdf*
[12] *http://www.llv.li/leitfaden_technische_und_org_massnahmen_fl_a.pdf*
[13] Phishing ist ein Kunstwort, das aus den Wörtern Passwort und Fishing entstand.
[14] Vgl. Tätigkeitsbericht 2005, 4.1.
[15] Vgl. dazu unten, 4.4.
[16] Vgl. unten, 5.1.1.2.
[17] Vgl. unten, 5.2. und 7.1.

Tarmed ein weiterer datenschutzrechtlicher Brennpunkt. Auch Fragen zu Themen allgemeiner Art bestanden wie zum Entscheid der österreichischen Datenschutzkommission, wonach keine *Autohalterdaten* mehr an liechtensteinische Behörden bekannt gegeben werden dürfen oder zur Pressemitteilung zu *Phishing*.

Die Einwilligung der betroffenen Person steht gerade bei der Datenbearbeitung durch private Personen im Vordergrund. Dabei geht es auch um die gültige Einwilligung in eine vertragliche Beziehung. Aufgrund der Wichtigkeit der Einwilligung in der Praxis veröffentlichte der DSB in der Liechtensteinischen Juristenzeitung (LJZ) einen **Aufsatz** zum Thema *«Die Einwilligung als zentrales Element des Datenschutzrechts»*.[18] Dabei geht es unter anderem darum, dass von einer gültigen Einwilligung nur dann ausgegangen werden kann, wenn die betroffene Person weiss, worauf sich die Einwilligung bezieht *(informierte Einwilligung)*. Das Kriterium der informierten Einwilligung ist insbesondere im Vertragsrecht sehr wichtig und so sind auch und insbesondere Allgemeine Geschäftsbedingungen entsprechend zu formulieren. Der Begriff der Einwilligung in Liechtenstein unterscheidet sich vom Begriff der Einwilligung in der Schweiz. Da etliche in Liechtenstein tätigen Banken und Versicherungen auch in der Schweiz tätig sind, dürften die Allgemeinen Geschäftsbedingungen, welche ihren Ursprung in der Schweiz haben, nicht so für Liechtenstein übernommen werden wie sie sind. Eine ausführlichere Information dürfte notwendig sein. Wichtig ist auch der Begriff der *freien Einwilligung*. Das heisst, dass eine Einwilligung, welche in einem Abhängigkeitsverhältnis gegeben wird, nur bedingt oder gar nicht gültig ist. Denn gerade im Arbeitsverhältnis ist der Arbeitgeber in einer stärkeren Position, so dass nicht immer davon ausgegangen werden kann, dass der Arbeitnehmer eine gültige Einwilligung zu einer Frage gegeben hat.

Schliesslich besteht auf der Internetseite die Möglichkeit, über einen *Newsletter* über Entwicklungen zum Datenschutz auf dem Laufenden gehalten zu werden.

3.2. INFORMATIONSPFLICHTEN VON DATENINHABERN

Ein Grundpfeiler des Datenschutzes besteht darin, dass die betroffene Person darüber Kenntnis hat, wer was wann über sie weiss (Recht auf informationelle Selbstbestimmung). Dies bedeutet, dass die Daten bearbeitende Person oder Behörde die betroffene Person über den Sinn und den Zweck der stattfindenden Datenbearbeitung vorgängig zu informieren hat,[19] damit die betroffene Person ihre gesetzlich garantierten Rechte (Einwilligungs- bzw. Widerspruchs-, Sperr- und Löschrecht) in Anspruch nehmen kann.
Hierzu gab es verschiedene Tätigkeiten. Die wichtigsten betrafen die folgenden: Bei der geplanten *Videoüberwachung* in der Fussgängerzone in Vaduz wie auch bei der Installierung von Webcams sind Hinweistafeln aufzustellen, damit die betroffenen Personen über die Datenbearbeitung informiert sind und ihr Verhalten darauf einstellen können. Dies hat zum Vorteil, dass Sachbeschädigungen verhindert oder zumindest deren Anzahl verringert werden sollten.[20] Bei der *SWIFT*[21]*-Affäre* geht es um den möglichen Zugriff von US-Behörden auf Daten internationaler Zahlungsanweisungen. Dabei fordern die Datenschutzbehörden vor allem im EWR-Raum, dass die Kunden über diese Tatsachen durch die Banken informiert werden.[22] Bei der Schaffung der *Auslagerung der Datenbearbeitung durch Banken ins Ausland* im Rahmen der Revision des Bankengesetzes war eine vorherige Information der Kunden bereits im Vernehmlassungsbericht vorgesehen. Im Rahmen der *Revision des Invalidenversicherungsgesetzes* (IVG) wurde ein Früherfassungssystem neu eingeführt, bei dem der betroffene Versicherte vor einer Meldung an die IV-Anstalt informiert werden muss. Auch bei der *Revision des Krankenversicherungsgesetzes* (KVG) ist vorgesehen, dass die Kassen die Versicherten besser über die Datenbearbeitung informieren müssen.[23] Bei der Benutzung von *Suchmaschinen auf dem Internet*[24] sammeln die Betreiber der Suchmaschine detaillierte Angaben über die Benutzer. Diese Betreiber sollten die Benutzer umfänglich über die stattfindende Datenbearbeitung informieren.[25] Ebenfalls zu informieren ist bei der Einrichtung von *Lesebestätigungen* bei der Versendung von elektronischer Post.[26]

[18] www.llv.li/pdf-llv-li-die_einwilligung_als_zentrales_element_des_datenschutzrechts.pdf
[19] Vgl. Art. 5 DSG, Tätigkeitsbericht 2004 und Tätigkeitsbericht 2005, je 3.2.
[20] Vgl. Tätigkeitsbericht 2004, 5.2. und 7.1. sowie Tätigkeitsbericht 2005, 5.1.1.2.
[21] SWIFT steht für Society for Worldwide Interbank Financial Telecommunication
[22] Vgl. unten, 5.2. und 7.1.
[23] Vgl. zum IVG und KVG unten, 4.4.
[24] Vgl. oben, 3.1.
[25] Vgl. auch Tätigkeitsbericht 2005, 3.2., zur Notwendigkeit von Datenschutzhinweisen auf Internetseiten.
[26] Vgl. dazu unten, 7.1.

4. Beratung

4.1. UNTERSTÜTZUNG VON PRIVATEN PERSONEN UND BEHÖRDEN DURCH ALLGEMEINE ORIENTIERUNGEN UND BERATUNGEN

Die Anzahl der Anfragen an die SDS nahm gemäss der **Anfragenstatistik**[27] ab. Während nach wie vor Behörden am Meisten Anfragen stellten und die Anzahl der Medien leicht zunahm, war bei Fragen internationaler Art ein starker Rückgang zu verzeichnen. Dies kann damit erklärt werden, dass der DSB inzwischen sowohl für die Europäische als auch die Internationale Konferenz[28] zugelassen wurde.

Eine Darstellung sämtlicher Anfragen sowie Antworten würden den Rahmen dieses Berichtes sprengen. Erwähnt sei an dieser Stelle immerhin das **breite Spektrum** derselben: Neben verschiedenen Anfragen zur Möglichkeit der *Datenbekanntgabe ins Ausland*[29] wurde verschiedentlich nach den datenschutzrechtlichen Bedingungen der Veröffentlichung von Daten auf Internetseiten, der Installation von *Videokameras* im privaten wie im öffentlichen Bereich, in Bezug auf *Werbung*[30], *Spam*[31] sowie auf in Gemeinden vorhandene oder geplante *Familienstammbücher* gestellt. Weiters war der DSB vermehrt mit der Frage befasst, wie *Geheimhaltungserklärungen* im Fall des Outsourcings von Datenbearbeitungen zu gestalten sind. Neben weiteren Fragen wie der Bekanntgabe von *Stimmbürgern* durch die Gemeinden ging es auch darum, inwiefern der Datenschutz für *verstorbene Personen* gilt. Auf Grund des Bedürfnisses in der Praxis sind 2007 die Informationen zu Datentransfers ins Ausland zu vertiefen und eine Vorlage für eine Geheimhaltungserklärung zu schaffen. Auch die Bearbeitung bzw. Veröffentlichung von Personendaten auf dem Internet wird zu vertiefen sein. An dieser Stelle kann immerhin festgestellt werden, dass sich bei einer Veröffentlichung von Daten auf dem Internet Fragen zur Verhältnismässigkeit und zur Zweckgebundenheit der Bearbeitung stellen.[32]

Erwähnt seien an dieser Stelle folgende Anfragen:
Eine Person fragte nach, ob es nötig sei, dass in einem konkreten Edikt des Landesgerichts zu *Unterhaltsvorschusssachen* die Angaben in Bezug auf die betroffene Mutter und Kinder so genau sein müssen.[33] In Unterhaltsvorschussverfahren geht es darum, dass der unterhaltspflichtige Elternteil den geschuldeten Unterhalt nicht bezahlt, weil er z. B. unbekannt weggezogen ist. In diesem Fall kann vom Land die Zahlung eines Unterhaltsvorschusses beantragt werden, der dann vom unterhaltspflichtigen Elternteil zurückzuzahlen ist, wenn er / sie wieder greifbar oder zahlungsfähig ist. In einer solchen Situation sind die Daten der betroffenen Unterhaltsgläubiger verständlicher Weise besonders sensibel zu behandeln. Obwohl das DSG unter anderem auf hängige Zivilverfahren nicht anwendbar ist, machte der DSB von seiner Kompetenz Gebrauch, Behörden auch in solchen Fällen zu beraten.[34] Daraufhin nahm das Landgericht von der bisherigen Praxis Abstand, in den Edikten von Unterhaltsvorschusssachen Angaben zum betreffenden Elternteil und zum Geburtsdatum der Kinder zu machen.[35]

An einer Besprechung zur Installation von *Videokameras* durch die Gemeinde Schaan ging es darum, dass bei der Primarschule öfters Fahrräder von Schülern beschädigt und zum Teil Bremskabel durchgeschnitten werden. Deshalb fragte die Gemeindepolizei an, ob und unter welchen Umständen die Installierung einer Videokamera bei den Fahrradständern möglich sei. Obwohl eine genügende rechtliche Grundlage für die Gemeinden zu bezweifeln ist, wies der DSB darauf hin, dass zuerst weniger weitgehende Mittel geprüft werden müssen. Um eine Verhältnismässigkeit zu erreichen, wies der DSB auf die Umstände einer rechtlich zulässigen Videoüberwachung hin: Dabei ist mit einer Hinweistafel auf die statt findende Videoüberwachung hinzuweisen. Dies hat den Vorteil, dass somit wahrscheinlich Sachbeschädigungen vermieden werden können. Weiters ist sicher zu stellen, dass die Speicherdauer sowie die Zugriffe auf die aufgenommenen Bilder auf das notwendige Mass reduziert werden. Durch die Gemeindepolizei wurden noch weitere Sachverhalte vorgetragen, zu denen eine Videoüberwachung möglicherweise eine Lösung sei. Der DSB nahm dies zur Kenntnis und stellte fest, dass eine Videoüberwachung auch zu einer örtlichen Verlagerung des Problems führen könne (Beispiel: Vandalismus).

[27] Vgl. Anhang.
[28] Vgl. unten, 7.4. und 7.5.
[29] Vgl. *http://www.llv.li/amtsstellen/llv-sds-spezialthemen-datentransfer_ins_ausland.htm*
[30] Vgl. *http://www.llv.li/amtsstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-adresshandel.htm*
[31] Vgl. unten, 5.2.
[32] Vgl. Art. 4 DSG.
[33] Angegeben wird Name, Geburtsdatum und genaue Wohnadresse der Mutter und der Kinder.
[34] Art. 32 Abs. 2 DSG.
[35] In § 117 der Zivilprozessordnung ist nämlich nicht davon die Rede, dass die Kindesmutter und die Geburtsdaten in einem solchen Edikt genau genannt werden muss. Die Rede ist lediglich davon, dass die Bestellung des Kurators, dessen Name und Wohnort und eine kurze Angabe des Inhaltes des zuzustellenden Schriftstückes nebst der Bezeichnung des Prozessgerichts und der Streitsache durch Edikt bekannt zu machen sind.

Das Landesspital gelangte mit einer Anfrage an die SDS, unter welchen Bedingungen ein *Vertrauensarzt* Daten an die Verwaltung einer Krankenkasse weiter geben darf. Hintergrund der Anfrage war ein Fall, in dem angeblich ein Vertrauensarzt detaillierte medizinische Angaben an die Verwaltung der Kasse weiter gegeben hatte. Der DSB hielt in seiner Stellungnahme fest, dass Sinn und Zweck der Institution des Vertrauensarztes eine Filterfunktion zwischen dem behandelnden Arzt einerseits und der Verwaltung der Krankenkasse andererseits ist. Diese Filterfunktion wird im Gesetz insbesondere dadurch belegt, dass der Vertrauensarzt die Persönlichkeitsrechte des Patienten zu bewahren hat. Praxisfragen um die Institution des Vertrauensarztes werden immer wieder thematisiert.[36]

Die Motorfahrzeugkontrolle (MFK) gelangte an die SDS mit der Frage, ob *Motorfahrzeughalterdaten* in einem Abrufverfahren den *Gemeindepolizisten* zur Verfügung gestellt werden können. Hintergrund war der Wunsch des Bürgermeisteramtes von Vaduz, elektronisch Halterdaten einsehen zu können, um Falschparker einfacher und zeitsparender ermitteln zu können. Die MFK machte einen Vorschlag, wie dies konkret umgesetzt werden könne, damit die Datensicherheit weiterhin gewährleistet ist. Der DSB machte darauf aufmerksam, dass nach dem Wortlaut des Strassenverkehrsgesetzes (SVG)[37] die Polizeiorgane Einsicht in die Registereinträge für die Kontrolle der Verkehrszulassung, die Identifikation des Halters und seines Versicherers sowie die Fahndung nehmen können. Der DSB stellte fest, dass diese Bestimmung sich von der Rezeptionsvorlage der Schweizerischen SVG[38] unterscheidet. Während in der schweizerischen Fassung von einem Abrufverfahren die Rede ist, heisst es im liechtensteinischen Gesetz nur, dass diese Organe Einsicht nehmen können. Von einer elektronischen Einsichtnahme ist nicht die Rede, wenigstens nicht im Gesetzesartikel selbst.[39] Der DSB sprach sich jedoch nicht dagegen aus, dass die Gemeindepolizeien auf diese Halterdaten zugreifen können, regte jedoch an, dass das SVG dementsprechend angepasst wird. Der Zugriff wurde allen Gemeindepolizeien des Landes gewährt, obwohl es sicher unter den Gemeinden erhebliche Unterschiede in Bezug auf Falschparker gibt.

Immer wieder wenden sich Personen an die SDS mit der Frage, ob und inwiefern eine *Internet- und E-Mail-Überwachung des Arbeitnehmers am Arbeitsplatz* möglich ist. Die Frage ist sehr brisant, geht es doch darum, dass den berechtigten Ansprüchen des Arbeitgebers auf Produktivität des Unternehmens die ebenfalls berechtigten Ansprüche des Arbeitnehmers auf Achtung seiner Privatsphäre entgegenstehen. Die Sektion Informatik der ehemaligen Gewerbe- und Wirtschaftskammer trat ebenfalls an die SDS heran und bat um Auskunft zu diesem Thema. Der DSB verwies auf die bestehenden Richtlinien zum Thema «Internet- und E-Mailüberwachung des Arbeitnehmers am Arbeitsplatz».[40] Auch für Informatikunternehmen ist es sehr wichtig über die gesetzlichen Möglichkeiten informiert zu werden, da meist Informatikfirmen entsprechende Auswertungen wahrnehmen.

Die *automatisierte Bearbeitung* von Personendaten ist auch in der *Landesverwaltung* die Regel. Diesbezüglich stellt die ZPV[41] das Hauptinstrument dar. In verschiedenen Ämtern gibt es Datenbanken, welche hauptsächlich amtsintern geführt werden und teils mit der ZPV zusammen hängen. Es war dem DSB ein Anliegen, mit der Arbeit solcher Datenbanken in der Praxis vertraut zu werden. Deshalb konnte im Berichtsjahr die Funktionsweise und die Arbeit in der Praxis in Bezug auf die Datenbank der MFK, der Landeskasse, der Staatsanwaltschaft und des Landgerichtes, der Abteilung Arbeitslosenversicherung beim Amt für Volkswirtschaft, des Gewerberegisters sowie des Landesarchivs aufgenommen werden. Zudem erfolgte eine Vorführung der Datenbearbeitung beim Zivilstandsamt, beim Ausländer- und Passamt und beim Amt für Volkswirtschaft Fachbereich Statistik.

[36] Vgl. oben, 3.2. und unten, 4.4. und 7.2.
[37] Vgl. Art. 99 b Abs. 3 Bst. a.
[38] Art. 104 a Abs. 5 Bst. d
[39] Wohl aber in den Materialien zu dieser Bestimmung.
[40] *http://www.llv.li/pdf-llv-sds-richtlinien_ueber_internet-_und_e-mail-ueberwachung_am_arbei_04_oktober_05.pdf*
[41] Vgl. Tätigkeitsbericht 2004, 5.1.1.1., Tätigkeitsbericht 2005, 5.1.1.1. und unten 5.1.1.1.

4.2. STELLUNGNAHMEN ZU DATENSCHUTZFRAGEN IN HÄNGIGEN VERFAHREN VOR RECHTSMITTELBEHÖRDEN – RECHTSPRECHUNG ZUM DATENSCHUTZGESETZ

Im Berichtsjahr erfolgten keine Anfragen an die SDS zu Datenschutzfragen in hängigen Verfahren durch entscheidende Organe oder Rechtsmittelbehörden, obwohl das DSG diese Möglichkeit ausdrücklich vorsieht.[42]

4.3 BEGUTACHTUNG DER GLEICHWERTIGKEIT DES AUSLÄNDISCHEN DATENSCHUTZES

Im Berichtsjahr erfolgte keine Untersuchung einer ausländischen Datenschutzgesetzgebung in Bezug auf die Frage, ob sie als gleichwertig angesehen werden kann. In Bezug auf die USA waren der Transfer von *PNR-Daten* wie auch der Zugriff von U.S. Behörden auf Daten von internationalen Geldüberweisungen (*SWIFT*) ein Thema.[43]

4.4. STELLUNGNAHME ZU VORLAGEN UND ERLASSEN

Auszugsweise soll an dieser Stelle auf folgende Stellungnahmen zu Gesetzesänderungen im Einzelnen eingegangen werden:

In der Stellungnahme zum Vernehmlassungsbericht betreffend die **Änderung des Gesetzes über die Banken und Finanzgesellschaften** ging es aus datenschutzrechtlicher Sicht hauptsächlich um die Einführung der Möglichkeit für Bankinstitute, bestimmte Tätigkeiten an Dritte auszulagern, welche sich im Ausland befinden. In Bezug auf die gesetzliche Regelung zur Datenbearbeitung im Ausland wäre es aus Sicht des DSB zu bevorzugen gewesen, die Vorgaben des DSG[44] explizit und vollumfänglich im neuen Gesetzestext einzubauen. Hierauf wurde jedoch mit dem Hinweis darauf verzichtet, dass es keiner gesonderten Regelung im Bankengesetz bzw. in deren Verordnung bedürfe, da sie sowieso gelte. Es war zu begrüssen, dass die Gesetzesänderung bei einer Auslagerung ins Ausland eine vorherige Information der Bankkunden vorsieht. Diese ist notwendig, damit die betroffenen Bankkunden eine gültige Einwilligung zu einer Datenbearbeitung nach Art. 16 DSG geben können.[45]

Die Arbeiten zur **Revision des Heimatschriftengesetzes** (HSchrG) zur *Einführung des biometrischen Reisepasses* wurden fortgesetzt.[46] Biometrie ist zwar im Pass nicht völlig neu. Neu sollen aber biometrische Merkmale auf einem Chip gespeichert werden, der im Reisepass integriert ist. Nach den Empfehlungen der Internationalen Zivilluftfahrt-Organisation (ICAO) müssen auf diesem Chip ein aufgenommenes Gesichtsfeld und ab Ende 2008 auch die Fingerabdrücke abgespeichert werden. Dementsprechend sieht die Neuregelung des HSchrG die Aufnahme von Grösse, Unterschrift und neu des digitalen Gesichtsfelds als biometrische Daten vor. Die Aufnahme von Fingerabdrücken bleibt vorbehalten.[47] Von der zusätzlichen Einführung der in Liechtenstein in der Praxis vorkommenden Personenidentifikationsnummer (PEID) wurde auf Empfehlung des DSB Abstand genommen, da es für diese Nummer noch keine gesetzliche Grundlage gibt. Bei biometrischen Daten handelt es sich um einzigartige Merkmale, die eines besonderen Schutzes bedürfen.[48] Mit der neuen Bestimmung, wonach die auf dem Chip gespeicherten Daten durch angemessene technische und organisatorische Massnahmen zu sichern sind, sollte jedoch ein ausreichender Schutz gewährleistet sein. Eine zentrale Speicherung der Daten sollte dagegen aus datenschutzrechtlicher Sicht nicht erfolgen.

In der Vorlage zum **Invalidenversicherungsgesetz (IVG)** soll ein System der *Früherfassung* neu eingeführt werden. Dieses soll es ermöglichen, das Bestehen einer Arbeitsunfähigkeit frühzeitig zu melden. Zweck der frühzeitigen Meldung ist, dass der Eintritt einer Invalidität mittels rechtzeitiger Massnahmen vermieden werden kann. Als meldeberechtigt sind verschiedene Personengruppen vorgesehen. Bei einer Meldung durch Dritte sind diese verpflichtet, die versicherte Person vorher über die bevorstehende Meldung zu informieren. Um Versicherten, die bei der Früherfassung gemeldet sind oder die Leistungen beziehen, den Zugang zu geeigneten Eingliederungsmassnahmen

[42] Vgl. Art. 32 Abs. 1 Bst. b DSG.
[43] Vgl. je unten, 7.1.
[44] Art. 19 Abs. 3 DSG regelt die Dokumentationspflichten: «Zum Zwecke der Beweissicherung sind die datenschutzrelevanten Elemente des Vertrags und die Anforderungen in Bezug auf Massnahmen nach Abs. 1 und 2 schriftlich oder in einer anderen Form zu dokumentieren.»
[45] Vgl. dazu oben, 3.2.
[46] Vgl. hierzu Tätigkeitsbericht 2005, 4.4 und 7.1
[47] Art. 16 HSchrG.
[48] Vgl. Tätigkeitsbericht 2005, 4.4. und 7.1. und Tätigkeitsbericht 2004, 7.1.

zu erleichtern, wurde weiters die rechtliche Grundlage für eine *inter-institutionelle Zusammenarbeit (IIZ)* geschaffen. Nach Ansicht des DSB waren die dortigen Begriffe der «öffentlichen Verwaltungsbehörden» und die Zweckangabe «zur Abklärung im Allgemeinen» zu ungenau formuliert und es wurde vorgeschlagen, dass beide Formulierungen im Gesetz genau definiert werden sollten, welchen Behörden unter welchen Bedingungen die IIZ möglich sein soll. Diese erfordert den Austausch von Daten, die in der Regel besonders schützenswert sind (insbesondere Angaben über die Gesundheit). Ein entsprechender Informationsaustausch unterliegt nach dem DSG besonderen Vorgaben und steht zum Teil auch der in Spezialgesetzen verankerten Schweigepflicht entgegen. Um diesen Widerspruch zu vermeiden, sollte nach Vorschlag des DSB eine Entbindung von der Schweigepflicht unter bestimmten Bedingungen erfolgen, die abschliessend im Gesetz geregelt werden sollten. Die Umsetzung der IIZ in der Praxis wird sehr wichtig sein. Es ist klar, dass es zu Missbräuchen im Zusammenhang von Sozialbezügen nicht kommen darf. Demgemäss sollte auch der Datenschutz seinen Teil dazu beitragen, dass Daten dort fliessen können, wo dies angezeigt und nötig ist. Der DSB zeigte stets seine Bereitschaft bei der Umsetzung der IIZ in die Praxis mitzuwirken. Dies gilt unverändert.

Die Stellungnahme zum Vernehmlassungsbericht über die Änderung des **Krankenversicherungsgesetzes** war positiv, da sich die Vernehmlassungsvorlage auf eine Initiative der SDS stützte. Es geht im Wesentlichen um die Umsetzungen von Forderungen einer unabhängigen Expertenkommission, welche in der Schweiz einen Bericht zur Stärkung des Datenschutzes im Sozialversicherungsbereich erstellt hatte.[49] Daneben soll auch die Stellung des *Vertrauensarztes*[50] gestärkt werden. Dazu wird eine *gestufte Bekanntgabe* durch Leistungserbringer an die Krankenkassen gesetzlich vorgesehen. Auch sollen die Krankenkassen besser über ihre Datenbearbeitungen *informieren*, insbesondere in Bezug auf die internen Datenflüsse.

Der DSB war im Berichtsjahr verstärkt in die Ausarbeitung der Vorlage zur **Revision des Polizeigesetzes** eingebunden, die als einen Schwerpunkt die Aufnahme von Erfordernissen des Datenschutzes beinhaltet. Im Vergleich zum geltenden Polizeigesetz von 1989 sollen zur Effizienzsteigerung auch neue Techniken der automatisierten Datenbearbeitung verankert werden. Bei der Schaffung und Ausarbeitung dieser und weiterer erforderlichen Bestimmungen geht es vor allem um einen Ausgleich zwischen dem Schutz der Bürgerrechte im Rahmen des geltenden DSG (Recht auf informationelle Selbstbestimmung) auf der einen Seite und auf der anderen Seite um die Besonderheiten der Polizeiarbeit, die mitunter eine Abweichung von den allgemeinen datenschutzrechtlichen Grundsätzen erfordern.[51] Die endgültige Vorlage zur Revision des Polizeigesetzes lag zum 31.12.2006 noch nicht vor, so dass im folgenden Jahr der Bericht hierüber fortgesetzt wird.

Obwohl das **DSG** bereits einmal revidiert worden war[52] zeigten sich weiterhin Probleme in der Praxis. Der DSB gelang mit verschiedenen Anliegen an das zuständige Ressort. Bei diesen Anliegen ging es um Folgendes: Das DSG sieht verschiedentlich vor,[53] dass Daten bearbeitet bzw. bekannt gegeben werden dürfen, wenn unter anderem die *betroffene Person* die Daten *selbst* allgemein zugänglich gemacht hat. Auch in Bezug auf Daten, welche durch Behörden veröffentlicht wurden, besteht nach dem aktuellen DSG keine Möglichkeit der Datenbearbeitung durch Privatpersonen. Somit dürfen insbesondere Angaben aus Massenmedien wie Zeitungen und Radio, Lexika, Adress- und Telefonverzeichnisse, Daten auf Internetseiten oder Angaben aus öffentlich zugänglichen Registern[54] eigentlich nicht bearbeitet werden. Da das DSG in diesem Punkt zu eng gefasst ist, wurde beim Ressort angeregt, die relevanten Bestimmungen zu lockern. Weiters machte der DSB darauf aufmerksam, dass eine Ratifizierung des *Zusatzprotokolls zum Datenschutzabkommen des Europarats* wünschenswert wäre. Dieses hat den grenzüberschreitenden Datenverkehr sowie eine Stärkung der Datenschutzbehörde zum Ziel. Ausserdem wurde das *Bundesgesetz über den Datenschutz in der Schweiz* im Jahr 2006 revidiert. Verschiedene Bestimmungen dieser Revision sind sehr sinnvoll und deren Übernahme in Liechtenstein wäre angezeigt. Dabei geht es unter anderem um die Einrichtung eines *betrieblichen Datenschutzbeauftragten*, welcher bereits in 14 europäischen Ländern besteht. Ausserdem sollte die Möglichkeit der *Zertifizierung* nach der neuen Fassung des schweizerischen Gesetzes übernommen werden. Die Praxis zeigt zu-

[49] *http://www.llv.li/amtsstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-gesundheit.html*
[50] Vgl. zum Vertrauensarzt auch oben, 4.1 und unten, 7.2.
[51] Vgl. auch Tätigkeitsbericht 2005, 4.4., zur Staatsschutzverordnung.
[52] Vgl. LGBl. 2004 Nr. 174 und Tätigkeitsbericht 2004, 4.4.
[53] Vgl. Art. 17 und 23.
[54] Vgl. Spiros Simitis, Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., Baden-Baden 2003, Randnummer 189 ff zu § 28.

dem, dass in Liechtenstein naturgemäss sehr viele *Datentransfers ins Ausland* vorkommen. Die Datenschutzrichtlinie sieht in Art. 25 und 26 Regelungen vor, zu denen es in Liechtenstein Unterschiede gibt. Die Praxis hat sich aber soweit wie möglich nach der Richtlinie zu richten. Insbesondere da die Art. 29 Arbeitsgruppe ein Dokument zur Auslegung von Art. 26 der Richtlinie angenommen hat[55] wären konkrete Anhaltspunkte für die Praxis gegeben. Somit wäre eine Übernahme von Art. 25 und 26 der Richtlinie wünschenswert. Ausserdem wäre es wünschenswert, wenn der DSB nicht (nur) der Regierung periodisch Bericht erstatten müsste,[56] sondern auch dem Landtag. Damit fände eine jährliche Diskussion im Landtag über die Tätigkeiten im Bereich des Datenschutzes statt.

Des weiteren wurde noch zu folgenden Vorhaben in verschiedenen Stadien des Gesetzgebungsverfahrens Stellung bezogen:

Berufsbildungsgesetz, Energieeffizienzgesetz, Finanzkonglomeratsgesetz, Kinder- und Jugendgesetz, Marktmissbrauchsgesetz, Pensionsfondsgesetz, Pensionsversicherungsgesetz, Personen- und Gesellschaftsrecht, Prospektgesetz, Rechtsanwalts-, Treuhänder-, Patentanwalts- und Wirtschaftsprüfergesetz, Richterdienstgesetz, Sachenrecht, Sanitätsgesetz, Schulgesetz, Staatspersonalgesetz, Strafvollzugsgesetz, Strassenverkehrsgesetz, Transplantationsgesetz, gesetzliche Grundlage für die Zentrale Personenverwaltung der Landesverwaltung (ZPV), Sammelpaket in Bezug auf die Anpassung verschiedener Gesetze an das DSG,[57] eine Regierungsvereinbarung zwischen Liechtenstein und der Schweiz betreffend das Strassenverkehrsregister sowie eine Übernahme des Notenaustausches zwischen der Schweiz und den USA über den Transfer von Flugpassagierdaten.

4.5. PROJEKTBEGLEITUNG

Das Projekt **elektronisches Gesundheitsnetz (eGN)** ging in eine zweite Phase. Nach der ersten Phase, in der es um die Vorbereitung der praktischen Seite der Krankenversicherungskarte ging, geht es nun darum, dass zusätzlich zu den administrativen Daten auch Gesundheitsdaten bearbeitet werden könnten. Dazu erschien es nötig, die entsprechenden Gesundheitsdaten vorerst zu definieren.

Die Landespolizei (LP) hat zur Effizienzsteigerung ihrer Arbeitsabläufe ein neues Werkzeug (Software-Tool) eingeführt, mit welchem die Abfrage in den **polizeilichen Datenbanken** über eine einzige Abfragemaske mit der Selektion der im Einzelfall notwendigen und erforderlichen Applikationen getätigt werden kann. In diesem Zusammenhang fragte die LP die SDS an, ob die Anbindung der ZPV sowie der Fahrzeughalter- und Führerausweisapplikation der MFK (Bistrada) im Rahmen der bestehenden Zugriffsberechtigungen an dieses neue Werkzeug möglich sei, damit eine weitere Effizienzsteigerung erreicht werden könne. Der DSB war der Ansicht, dass sich bei der Verwendung von Datenbanken, welche nicht für die polizeiliche Arbeit geschaffen wurden (wie der ZPV) sich Fragen zur Zweckgebundenheit und Verhältnismässigkeit der Bearbeitung der Daten stellen. Die Erstellung einer internen Weisung zur Datenbearbeitung durch die Polizei stellt einen wichtigen Schritt dar, um die Verhältnismässigkeit der Bearbeitung zu erreichen. Der Forderung nach Anpassung der internen Weisung kam die LP nach. Ebenfalls forderte der DSB die Schaffung einer rechtlichen Grundlage für diese Verknüpfungsmöglichkeit. Auch diese Forderung des DSB wurde aufgenommen.

Unter der Leitung des Amtes für Personal und Organisation wurde ein Prototyping von **ECM**[58] im Ausländer- und Passamt gestartet. Ziel dieses Vorprojektes ist es, eine abschliessende Aussage darüber machen zu können, ob und wie ein ECM-System verwaltungsweit eingeführt werden kann. Die Phase des Prototypings wurde im Hintergrund begleitet. Insgesamt muss beachtet werden, dass die Anforderungen an das Vorprojekt auf die ganze Verwaltung ausgerichtet sein soll und unter Beachtung der notwendigen gesetzlichen, technischen und organisatorischen Massnahmen.

Die durch die Regierung eingesetzte Arbeitsgruppe zum Thema **«Public Key Infrastructure» (PKI)** setzte ihre Arbeit fort. Der DSB nahm zu einem Entwurf eines Schlussberichts an die Regierung ausführlich Stellung. In einer ersten Phase wird die PKI, welche zur eindeutigen elektronischen Feststellung der Identität eines Kunden gebraucht wird, beim Grundbuch- und Öffentlichkeitsregisteramt (GBOERA) eingesetzt. PKI soll aber noch breiter eingesetzt werden, damit eine vertrauliche, gesicherte und rechtlich verbindliche Kommunikation zwischen den

[55] Arbeitspapier über eine gemeinsame Auslegung des Art. 26 Abs. 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, WP 114.
[56] Vgl. Art. 31 Abs. 1 DSG.
[57] Vgl. zu letzteren beiden unten, 5.1.2.
[58] Enterprise Content Management (ECM) oder auch Dokumentenmanagement-System (DMS); vgl. dazu auch oben, 3.1. und Tätigkeitsbericht 2005, 4.5.

Kunden und der Verwaltung sowie innerhalb von Behörden statt finden kann. Ein Kernelement solcher Anwendungen ist die Benutzung einer personenbezogenen Kennziffer. Liechtenstein kennt eine solche Kennziffer (PEID) schon seit Jahren. Sie wird im Rahmen ZPV gebraucht.[59] Für die Benutzung einer solchen Nummer fehlt in Liechtenstein nach wie vor eine rechtliche Grundlage. Eine solche sollte dringend geschaffen werden. Als datenschutzfreundlich gilt dabei die Lösung, welche in Österreich verwendet wird. Dabei geht es um bereichsspezifische Kennzahlen.[60]

[59] Vgl. unten, 5.1.1.1.

[60] Die bereichsspezifischen Kennzahlen bauen zwar auf eine einzige Kennzahl hin, werden aber so umgewandelt, dass je nach Bereich eine andere Kennzahl verwendet wird, welche aber mit der Stammzahl zusammenhängt. Damit wird verhindert, dass der Bürger auf eine einzige von vielen Stellen verwendete Nummer reduziert wird.

5. Aufsicht

5.1. AUFSICHT ÜBER BEHÖRDEN

5.1.1. DATENSCHUTZWIDRIGE BEARBEITUNGEN

5.1.1.1. DATENBANKEN

Wie schon früher berichtet,[61] stellen sich zur **ZPV** datenschutzrechtliche Fragen. Generell ist aufgrund der Beschaffenheit der ZPV eine *verhältnismässige Datenbearbeitung* nach wie vor nicht möglich:[62] Für die Amtsstellen, welche über einen Zugriff auf die so genannten globalen Daten haben, ist ein Zugriff auf Daten der *gesamten Bevölkerung* und nicht nur auf Daten ihrer Kunden möglich. Dazu können entweder auf *sämtliche Vergangenheitsdaten* zugegriffen werden oder ein solcher Zugriff wird überhaupt nicht gegeben. Eine Einschränkung des Zugriffs auf eine gewisse Dauer ist nicht möglich. Auch dies ist als unverhältnismässig zu beurteilen.[63] Ausserdem fordert die DSV, dass eine *Leseprotokollierung* bei automatisierten Bearbeitungen stattfinden muss, wenn die präventiven Massnahmen des eingesetzten Systems den Datenschutz nicht gewährleisten können. Aufgrund der nicht gegebenen Verhältnismässigkeit im Rahmen der ZPV muss davon ausgegangen werden, dass eine Protokollierung nötig ist. Um dieser Anforderung zu entsprechen, werden neu bei der sogenannten Personenübersichtsmaske der ZPV nicht nur die Benutzeranmeldungen und die Mutationen auf die einzelnen Felder *protokolliert*, sondern auch der Zugriff auf die Fotos in der ZPV.[64] Eine solche Protokollierung von blossen Zugriffen stellt zwar einen Mehraufwand an die technische und organisatorische Umsetzung dar, der jedoch aus Sicht des Datenschutzes nötig ist. Und schliesslich ist aufgrund der Konstellation der ZPV eine *Löschung* von Daten nicht möglich. Dies widerspricht ebenfalls dem Verhältnismässigkeitsprinzip, wonach Daten nur solange aufzubewahren sind, wie sie benötigt werden. Der Umstand, dass Daten oder genauer gesagt die so genannten globalen Daten nicht gelöscht werden, führt dazu, dass in dieser Datenbank Angaben von Personen enthalten sind, die schon längst gestorben sind und sicher nicht mehr für alle Amtsstellen, welche Zugriff auf diese Daten haben, relevant sind. Die Nichtlöschung von diesen Daten führt zu einem Datenberg, welcher nicht gebraucht wird. Die genannten Punkte konnten im Berichtsjahr nicht abschliessend gelöst werden und sind somit 2007 weiter zu behandeln.

Die Überprüfung der Umsetzung der ZPV-Anträge hinsichtlich Zugriffsberechtigungen der Personenübersichtsmaske wurde weiter behandelt.[65] Alle im Berichtsjahr vorhandenen Anträge wurden analysiert. Dabei wurden Diskrepanzen im System festgestellt. Diese Analyse-Dokumente wurden dem Amt für Personal und Organisation zur Erledigung weitergeleitet.

Nachdem im letzten Jahr ein Schreiben für ein einziges Amt erstellt wurde, wurde im Berichtsjahr die Notwendigkeit erkannt, dass ein ähnliches Schreiben zur ZPV an alle anwendenden Ämter notwendig ist.[66] Dieses Informationsschreiben der von der Regierung zur Sicherstellung des Datenschutzes eingesetzten Arbeitsgruppe informiert die Ämter vor allem darüber, dass die Daten durch die Eigentümer zu deren eigenen Zwecken erfasst werden und sich dadurch bei den anwendenden Amtsstellen Diskrepanzen ergeben können. Vor allem der Grad der Aktualität der Daten in der ZPV richtet sich deshalb in erster Linie nach den Bedürfnissen des jeweiligen erfassenden Amtes. Somit bestehen zwischen den Bedürfnissen der erfassenden und der zugreifenden Amtsstellen regelmässig Differenzen. Mit diesem Schreiben konnte ein bestimmtes Mass an Sensibilisierung der Benutzer bezüglich des Verwendungszweckes gegenüber dem Erfassungszweck erreicht werden. Es wurde auch auf den Umstand hingewiesen, dass die ZPV zum Teil doppelte als auch falsche Einträge enthält.

[61] Vgl. Tätigkeitsbericht 2005, 5.1.1., Tätigkeitsbericht 2004, 5.1.1. und Tätigkeitsbericht 2003, 4.1.2.
[62] Vgl. Tätigkeitsbericht 2005, 5.1.1.1.
[63] Vgl. Tätigkeitsbericht 2005, 5.1.1.1.
[64] Ein Protokollierungsdatensatz einer solchen Abfrage auf das Feld Foto besteht aus den Feldern Benutzerkürzel, Datum und Zeit der Datenabfrage sowie der PEID der Person auf dem Foto. Weiters musste geregelt werden, wie mit den Protokollierungsdateien umgegangen werden muss.
[65] Siehe dazu auch Tätigkeitsbericht 2005, 5.1.1.1. Die Verteilung der Zugriffsberechtigung wird in der Praxis dahingehend überprüft, ob die Berechtigungen richtig umgesetzt wurden. Diese aufwändige Arbeit wurde mit einer Aushilfskraft angegangen, konnte jedoch letztes Jahr nicht abgeschlossen werden.
[66] Siehe dazu auch Tätigkeitsbericht 2005, 5.1.1.1.

Art. 21 DSV verlangt ein *Bearbeitungsreglement*, falls eine automatisierte Datensammlung besonders schützenswerte Daten oder Persönlichkeitsprofile beinhaltet oder durch mehrere Behörden benutzt wird, was bei der ZPV der Fall ist. Ein solches Bearbeitungsreglement regelt die organisatorischen und technischen Massnahmen zur datenschutzkonformen Bearbeitung der Daten. Das Bearbeitungsreglement informiert über die für den Datenschutz und die Datensicherheit verantwortlichen Organe, über die Herkunft der Daten und die Zwecke, für welche sie regelmässig bekannt gegeben werden sowie auch das Verfahren für die Erteilung der Zugriffsberechtigungen. Mit der Erstellung eines Entwurfs eines Bearbeitungsreglements zur ZPV konnte viel Erfahrung gesammelt werden, welche an verschiedene Stellen weiter gegeben werden konnte. Zu erwähnen ist schliesslich, dass die Bearbeitungsreglemente der Krankenkassen nach wie vor nicht abgeschlossen wurden. Auch verschiedene weitere Behörden verfügen noch über kein Bearbeitungsreglement, obwohl ein solches für verschiedene Datenbanken nötig wäre.

Die ZPV selbst umfasst mehrere Datensammlungen. Diese Datensammlungen stammen insbesondere von den Dateneigentümern selbst, aber auch von anderen Amtsstellen, welche eine Fachanwendung führen. Diese Datensammlungen hängen in der ZPV zusammen. Damit stellt die ZPV als Ganzes, d.h. unabhängig von den einzelnen Lösungen, eine logische Datensammlung dar. Deshalb muss diese Datensammlung beim DSB registriert werden. Diese Anmeldung der Datensammlung ZPV als Ganzes wurde vorbereitet und den betroffenen Dateneigentümern zur Kommentierung zur Verfügung gestellt.

5.1.1.2. ANDERES

In einer Schule war eine **Webcam** insbesondere im Eingangsbereich und im Bereich der Caféteria vorhanden. Auf Beschwerde einer betroffenen Person wies der DSB darauf hin, dass die Installation einer Webcam mit einer Videoüberwachung vergleichbar ist, womit verschiedene Massnahmen zu treffen sind (insbesondere ist eine Hinweistafel anzubringen, welche auf diese quasi Videoüberwachung hinweist).[67] Daraufhin wurde die in Frage stehende Webcam deinstalliert.

Eine private Person fragte ausserdem nach der Rechtmässigkeit einer im Malbun installierten **Webcam**, welche über eine Zoommöglichkeit verfügte. Mit dieser Zoommöglichkeit der Webcam konnte das Aufnahmefeld auf einzelne Häuser und sich davor befindende Parkplätze fokussiert werden. Damit war es grundsätzlich möglich, dass gewisse Verhaltensweisen von Bewohnern weltweit zur Schau gestellt werden. Der DSB machte den Betreiber der Webcam darauf aufmerksam. Die Antwort lautete dahin gehend, dass der Zoom bereits reduziert worden war, so dass es sich nun um eine Grenzfrage handeln dürfte. Der DSB stimmte dem zu. Dennoch wies er darauf hin, dass eine weitere Reduzierung des Zoomes wünschenswert wäre. Dem kam der Betreiber der Webcam nach.

Im Spätsommer des Berichtsjahres wurde bekannt, dass der Gemeinderat Vaduz beschlossen hatte, im Fussballstadion, aber auch in der Fussgängerzone eine **Videoüberwachung** einzuführen. Das betreffende Gemeinderatsprotokoll nahm zwar Bezug auf den Datenschutz. Zur Begründung der Einführung der Videoüberwachung wurde aufgeführt, dass auch in unserem Land das Aggressionspotenzial und Sachbeschädigungen zunehmen, dass Überfälle auf Einkaufszentren, Tankstellenshops und Geschäfte in Besorgnis erregendem Ausmass zugenommen haben, dass in letzter Zeit immer häufiger festgestellt werden musste, dass Randalierer bei privatem und öffentlichem Eigentum Schaden verursachen und dass die Geschäfte im Städtle in den letzten Jahren ebenfalls mit kriminellen Vorfällen konfrontiert wurden. Das entsprechende Gemeinderatsprotokoll nahm nur Bezug auf den Zugriff und die Sicherheit der Daten. Jedoch wurde nicht auf die Notwendigkeit der Videoüberwachung oder die Frage der Überprüfung von alternativen Massnahmen eingegangen. Da das Gemeinderatsprotokoll einerseits auf allgemeine Entwicklungen im Land und nicht im Städtle abgefasst war und auch der Teil bezüglich des Datenschutzes nicht alle Fragen beantwortete, gelangte der DSB an das Bürgermeisteramt und fragte insbesondere, ob weniger weit gehende Massnahmen als eine Videoüberwachung geprüft worden waren; weiters wurde insbesondere nach der Anzahl von festgestellten Sachbeschädigungen in der Fussgängerzone gefragt. Schliesslich machte der DSB die Gemeinde Vaduz darauf aufmerksam, dass es bei der Installierung einer Videoüberwachung durch eine Gemeinde nicht nur um einen Eingriff in die Privatsphäre geht, sondern dass auch die Bewegungsfreiheit und Versammlungsfreiheit der Bürger betroffen ist. Somit stellen sich verfassungsrechtliche Fragen. In einem Schreiben wurden die entsprechenden Anforderungen an Grundrechtseingriffe nach der Rechtssprechung des

[67] Vgl. Tätigkeitsbericht 2004, 7.1., zu allgemeinen Regeln der Videoüberwachung.

Staatsgerichtshofs dargestellt. Danach braucht es eine *gesetzliche Grundlage*. An einer genügenden Grundlage fehlt es derzeit noch. Das *öffentliche Interesse* kann zwar als gegeben betrachtet werden, da es um eine Verhinderung von Sachbeschädigungen geht. Die meisten offenen Punkte ergaben sich im Zusammenhang mit der *Verhältnismässigkeit* einer staatlichen Massnahme, welche für einen Eingriff in Grundrechte gegeben sein muss. Weiters wurde darauf aufmerksam gemacht, dass eine Datenbearbeitung nach Treu und Glauben, welche das DSG erfordert[68] nur dann gegeben ist, wenn die Videoüberwachung klar sichtbar statt findet und mit *Hinweistafeln* auf diese Überwachung hingewiesen wird. Weiters sind Aufnahmefelder der Kameras so zu gestalten, dass das notwendige Mass nicht überschritten wird. Zudem wurde zur *Datensicherheit* danach gefragt, durch wen und wie lange ein Zugriff auf die Bilder möglich ist und ob dies nur im Fall eines Schadenereignisses der Fall ist. Das Bürgermeisteramt antwortete auf dieses Schreiben in dem Sinn, dass das Gemeindegesetz eine entsprechende Grundlage enthalte.[69] Weiters wurde nur die Frage nach der Datensicherheit beantwortet. Die anderen Fragen wurden nicht abschliessend beantwortet. Anlässlich einer Besichtigung konnte die Videoüberwachungsanlage betrachtet werden. Dabei stellte sich heraus, dass insgesamt zwölf Kameras installiert wurden. Neben einer Besichtigung der Kameras und einer Erklärung ihrer Funktionsweise und der Einrichtung des Bildfeldes wurden auch die Sicherheitsmassnahmen vorgestellt. Der Forderung nach der Anbringung von Hinweistafeln in der Nähe der Kameras oder zumindest bei den Eingangsbereichen zur Fussgängerzone wurde durch die Gemeinde nachgekommen. Die meisten der erwähnten Fragen blieben aber bis Jahresende unbeantwortet.

Im Zusammenhang mit den Diskussionen der Einführung von *Tarmed* wurde die Arbeitsweise von zwei Krankenkassen vor Ort untersucht und aktiv an den Verhandlungen zwischen dem Kassenverband und der Ärztekammer teilgenommen und eine Lösung unterbreitet, wie der Datenschutz im Krankenversicherungsbereich verbessert werden könnte.[70]

5.1.2. GESETZLICHE GRUNDLAGEN

Im Berichtsjahr war der DSB erneut bei der Schaffung einer rechtlichen Grundlage für die ZPV beteiligt. Das Vorhaben konnte noch nicht abgeschlossen werden. Zudem galt es, eine ausdrückliche gesetzliche Grundlage für die Bearbeitung von besonders schützenswerten Daten und Persönlichkeitsprofilen auszuarbeiten, da eine Bearbeitung derselben ohne eine entsprechende Grundlage ab dem 1. August 2007 nicht mehr legal sein wird.[71]

5.2. ABKLÄRUNGEN UND EMPFEHLUNGEN IM PRIVATRECHTSBEREICH

Zwei Privatpersonen wandten sich an die SDS, da sie unerwünscht Werbemails von einer in Liechtenstein tätigen Firma erhalten hatten (**Spam**). Die Abklärungen ergaben, dass diese Firma zwar E-Mail-Adressen einzukaufen pflegt, jedoch entsprechende Sicherungsmassnahmen getroffen hatte. Denn der Verkäufer der Adressen im Ausland hatte die Garantie dafür übernommen, dass die betroffenen Adressaten ihre Einwilligung zum Erhalt von Werbemails gegeben hatten. Da der Verkäufer im Ausland tätig war, war dieser für mögliche Fehler zur Rechenschaft zu ziehen.

In diesem Zusammenhang gab es im Berichtsjahr eine wichtige Gesetzesänderung: Mit dem neuen Kommunikationsgesetz (KomG),[72] welches unter anderem die Datenschutzrichtlinie in der elektronischen Kommunikation umsetzt, wurde ein «Opt-in»-Ansatz eingeführt. Danach ist der Versand von Nachrichten zum Zwecke der Direktwerbung grundsätzlich unzulässig.[73] Eine Ausnahme liegt nur dann vor, wenn der Empfänger den Versand durch vorherige ausdrückliche Einwilligung gestattet hat. Es ist erlaubt, diese Einwilligung einmalig mittels elektronischer Post durch ein entsprechendes Ersuchen einzuholen (Opt-in).[74] In diesem Ersuchen ist in ausdrücklicher, klarer und auffälliger Form darauf hinzuweisen, dass der Empfänger unter anderem berechtigt ist, jede weitere Zusendung von Nachrichten abzulehnen.

[68] Vgl. Art. 4 Abs. 2 DSG.
[69] Angegeben wurde Art. 52 Abs. 4: Danach steht der Gemeindevorsteher der örtlichen Polizei vor und sorgt für Ruhe, Sicherheit und Ordnung. Er trifft die dazu nötigen Anordnungen und verhängt aufgrund gesetzlicher oder ortspolizeilicher Vorschriften Bussen.
[70] Vgl. oben, 4.4.
[71] Vgl. Tätigkeitsbericht 2005, 5.1.2. und Tätigkeitsbericht 2004, 4.4.
[72] Kommunikationsgesetz vom 17. März 2006, LGBl. Nr. 2006 Nr. 91.
[73] Vgl. Art. 50 Abs. 1 KomG.
[74] Vgl. Art. 50 Abs. 2 KomG.

Eine Privatperson wandte sich in einem weiteren Fall der Zusendung unerwünschter Werbung an die SDS. Bei der Klärung des Sachverhaltes stellte sich heraus, dass der Ursprung dieser Werbung auf eine in Liechtenstein tätige Firma zurück zu führen war. Obwohl es widersprüchliche Aussagen dieser Firma bei der Klärung des Sachverhaltes gab, bestanden Anzeichen dafür, dass sie nicht als eigentliche *Adresshandelsfirma*, sondern als Listbroker tätig ist. Listbroker sind als Vermittler tätig und nehmen eine eigentliche Maklerfunktion ein. Listbroker verfügen selbst kaum über Adressen, welche sie vermarkten, sondern führen Wünsche von Listeneigentümern mit Wünschen von Listennutzern zusammen. Es gab nicht genügend Gründe, um die in Frage stehende Firma als Inhaberin einer Datensammlung[75] zu qualifizieren, wodurch sie strengeren Vorschriften unterworfen wäre. Die Tätigkeit als Listbroker entsprach jedoch nicht der bestehenden Gewerbebewilligung. Dies wurde dem für Gewerbebewilligungen zuständigen Amt für Volkswirtschaft mitgeteilt.

Die **Society for Worldwide Interbank Financial Telecommunication (SWIFT)** ist ein weltweit agierender Geldüberweisungsdienst, welcher im Auftrag von 7800 Finanzinstituten (darunter die in Liechtenstein tätigen Banken) internationale Zahlungsanweisungen im Wert von über 7 Billionen Franken täglich übermittelt. SWIFT speichert alle Überweisungsdaten in zwei Rechenzentren, von denen sich eines in der EU, das andere in den USA befindet. Die Zahlungsanweisungen enthalten personenbezogene Daten wie Namen des Zahlungsanweisenden oder des Zahlungsempfängers. Nach den Terrorangriffen vom September 2001 verlangte das U.S. Finanzministerium (UST) von SWIFT Zugang zu den in den USA gespeicherten Daten zur Bekämpfung des Terrorismus.[76] Erst aufgrund von Presseberichten im Sommer erfuhr die Öffentlichkeit erstmals von dieser Angelegenheit, deren Brisanz darin liegt, dass die U.S. Behörden möglicherweise Zugriff auf Geldüberweisungen haben, welche bis anhin als sicher galten.[77] Die Hauptforderung der Datenschutzbehörden vor allem des EWR-Raumes an die nationalen Banken besteht darin, dass die Kunden über die Datenbearbeitung im Rahmen der Nutzung der Dienste von SWIFT informiert werden.[78] Diese Forderungen gelten auch für die in Liechtenstein tätigen Banken. In diesem Zusammenhang fanden daher Sitzungen mit dem Bankenverband und der Finanzmarktaufsicht (FMA) statt. Dabei wurde insbesondere auf die entsprechende Stellungnahme der Art. 29 Arbeitsgruppe[79], aber auch auf eine Stellungnahme des EDÖB[80] hingewiesen. Neben Massnahmen, welche SWIFT selbst zu treffen hat, sind eben auch die liechtensteinischen Banken dazu verpflichtet, ihre Kunden entsprechend zu informieren. Weiters besteht analog zur Schweiz ein formeller Verstoss durch die Banken darin, dass sie die Meldung des Datentransfers in ein Drittland nicht beim DSB angemeldet haben, wie dies durch das Datenschutzgesetz verlangt wird.[81] Da die Forderung an die Banken erst im November des Berichtsjahres gestellt wurde, konnte diese Angelegenheit nicht beendet werden.

[75] Vgl. Art. 3 Abs. 1 Bst. k DSG.
[76] SWIFT gab diesen Anordnungen nach, konnte aber gewisse Einschränkungen aushandeln.
[77] SWIFT unterliegt als in Belgien ansässige Genossenschaft belgischem Datenschutzrecht, das die auch für Liechtenstein verbindliche EU-Datenschutzrichtlinie 95/46/EG umsetzt. Die Finanzinstitute, die sich der Dienstleistungen von SWIFT bedienen, unterliegen den jeweils nationalen Datenschutzvorschriften in den Mitgliedstaaten, in denen sie angesiedelt sind.
[78] Vgl. auch oben, 3.2. und 7.1.
[79] Ausführlich hierzu unter 7.1.
[80] *http://www.llv.li/pdf-llv-zugriff_auf_transaktionsdaten_swift.pdf*
[81] Vgl. Art. 8 DSG.

6. Register der Datensammlungen

An dieser Stelle sei daran erinnert,[82] dass das Register der Datensammlungen das Ziel hat, eine Transparenz zu schaffen, damit insbesondere sichtbar werden soll, über welche Datensammlungen die Behörden verfügen. In das Register werden zwar keine Einzeldaten über die Betroffenen, sondern nur summarische Angaben aufgenommen, welche einen Überblick über die gesamte Datenbearbeitung erlauben. Nähere Angaben können die Betroffenen beim Inhaber der Datensammlung selbst auf Grund des gesetzlichen Auskunftsrechts bekommen.

Im Berichtsjahr wurden weitere Datensammlungen angemeldet. Das Register, welches im Internet veröffentlicht ist, umfasste 522 Datensammlungen.[83] Die Gemeinden und das Zivilstandsamt führen nach dem Heimatschriftengesetz Datensammlungen über Heimatscheine. Diese Anmeldungen waren im Vorjahr nicht erfolgt. Dem wurde auch in diesem Berichtsjahr nicht nachgekommen.

[82] Vgl. Tätigkeitsbericht 2003, 5. oder Tätigkeitsbericht 2004, 4.4.
[83] Vgl. *http://www.llv.li/amtsstellen/llv-sds-register_der_datensammlungen.htm*

7. Internationales

7.1. ART. 29 ARBEITSGRUPPE DER RICHTLINIE 95/46/EG

Das Gremium unabhängiger nationaler Datenschutzbehörden des EWR-Raumes, die so genannte **Art. 29 Arbeitsgruppe**, behandelte auch 2006 Themen internationaler Relevanz, die auch für Liechtenstein Auswirkungen haben werden. In diesem Jahr wurden Dokumente vor allem zu folgenden Themen verabschiedet:

Bezüglich der Bearbeitung von personenbezogenen Daten durch **SWIFT** und die beteiligten Finanzinstitute[84] betont die Art. 29 Arbeitsgruppe, dass auch im Kampf gegen Terrorismus und Kriminalität die Grundrechte gewahrt bleiben müssen. Die Arbeitsgruppe besteht daher auf der Achtung weltweiter Datenschutzprinzipien und kommt unter anderem zu folgenden Schlussfolgerungen: SWIFT und die Auftrag gebenden Finanzinstitute tragen eine *gemeinsame Verantwortung* für die Verarbeitung von personenbezogenen Daten, wenn auch in unterschiedlichem Masse. Die Datenschutz-Richtlinie bzw. die nationalen Datenschutzgesetze sind somit grundsätzlich anwendbar und einzuhalten. Weder SWIFT noch die Finanzinstitute haben die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten *informiert*, wie dies die Richtlinie bzw. die nationalen Gesetze vorschreiben. Die Art. 29 Arbeitsgruppe hält es für unabdingbar, dass die Finanzinstitute im EWR-Raum als professionelle Dienstleister ihre Kunden in Übereinstimmung mit den *Transparenzforderungen* der Richtlinie hinreichend unterrichten, wie deren Daten verarbeitet werden und welche Rechte die Betroffenen haben. Sie haben sie insbesondere auch über die Inanspruchnahme von Dienstleistern wie z.B. den SWIFTNet FIN Service, die umfangreiche Übermittlungen in Länder ohne adäquates Datenschutzniveau durchführen oder über die Möglichkeit eines Zugriffes auf Daten durch U.S. Behörden zu informieren.[85] Darüber hinaus sind auch die Garantien für die Datenübermittlung in ein Drittland, wie sie die Richtlinie vorsieht, und die Grundsätze der *Verhältnismässigkeit* und der *Erforderlichkeit* nicht beachtet worden. Die Art. 29 Arbeitsgruppe fordert SWIFT und die Finanzinstitute auf, unverzüglich Massnahmen zu ergreifen, die die gegenwärtige unrechtmässige Situation beenden.

Die Arbeitsgruppe, welche sich bereits mehrfach mit der künftigen **Vorratsdatenspeicherung von Telekommunikationsdaten** befasst hatte,[86] nahm erneut eine Stellungnahme zu diesem Thema an. Darin wiederholte die Arbeitsgruppe die Bedenken wonach die Bestimmungen der Richtlinie für alle europäischen Bürger und deren Privatsphäre weit reichende Konsequenzen auf den Alltag der Bürger in Europa haben. Denn die Entscheidung wonach zur Bekämpfung schwerer Straftaten Daten auf Vorrat gespeichert werden dürfen, stellt ein absolutes Novum mit historischem Ausmass dar. Die Arbeitsgruppe stellt fest, dass in der Richtlinie angemessene und besondere Schutzvorkehrungen fehlen, die bei der Verarbeitung der Verbindungsdaten angezeigt sind. So kann es zu unterschiedlichen Auslegungen und Umsetzungen der Richtlinie kommen. Dies ist jedoch zu verhindern, insbesondere was das Recht auf Vertraulichkeit bei der Nutzung öffentlich zugänglicher elektronischer Kommunikationsdienste betrifft. Deshalb schlägt die Arbeitsgruppe angemessene und besondere Schutzvorkehrungen vor. Diese sollten mindestens Folgendes umfassen: Die Daten dürfen nur für bestimmte Zwecke im Zusammenhang mit schweren Straftaten gespeichert werden. Zugang zu den Daten dürfen nur eigens genannte Strafverfolgungsbehörden erhalten. Und dies nur zum Zwecke der Ermittlung, Feststellung und Verfolgung der in der Richtlinie genannten Straftaten. Es sollten so wenig Daten wie möglich auf Vorrat gespeichert werden. Die auf Vorrat gespeicherten Daten dürfen nicht mittels eines gross angelegten Datenschürfens ausgewertet werden. Der Zugang zu den Daten muss grundsätzlich in jedem Einzelfall von einer Justizbehörde genehmigt werden. Die Auswertung der Daten darf allein zu den vorgesehenen Zwecken statt finden. Die zu speichernden Daten sind von anderen Daten, welche zu geschäftlichen Zwecken gespeichert werden, zu trennen. Schliesslich sind technische und organisatorische Sicherheitsvorkehrungen zu treffen. Die genannte Richtlinie zur Vorratsspeicherung von Daten im Kommunikationsbereich ist grundsätzlich EWR-relevant und wird somit auch von Liechtenstein umzusetzen sein. Dabei werden diese Forderungen wichtige Anhaltspunkte für die Umsetzung darstellen.

In vielen Unternehmen gibt es interne Hotlines, an welche mutmassliche Missstände gemeldet werden können. Solche Hot-

[84] Vgl. oben, 3.2. und 5.2.

[85] Die Art. 29 Arbeitsgruppe vertritt zudem die Auffassung, dass der Mangel an Transparenz sowie an angemessenen und effektiven Kontrollmechanismen beim gesamten Prozess der Übermittlung personenbezogener Daten in die USA und weiter an das US-Finanzministerium (UST) eine schwere Verletzung der Richtlinie darstellt.

[86] Vgl. Tätigkeitsbericht 2004, 7.1. und Tätigkeitsbericht 2005, 7.1.

lines dienen der Aufdeckung von möglicherweise rechtswidrigen Handlungen. In den USA sieht der so genannte Sarbanes Oxley Act (SOX) vor, dass börsennotierte Unternehmen zur Meldung fragwürdiger Buchhaltungs- und Revisionspraktiken anoyme Meldeverfahren einrichten müssen.[87] Da sich datenschutzrechtliche Fragen zu solchen Hotlines und insbesondere zu den Anforderungen des SOX stellen, nahm die Arbeitsgruppe eine Stellungnahme in Bezug auf interne Verfahren zur Meldung **mutmasslicher Missstände** in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität (**«Whistle Blowing»**) an.[88] Interne Verfahren zur Meldung von Missständen werden in der Regel aus dem Bedürfnis eingerichtet, zuverlässige Grundsätze der Unternehmensführung in den täglichen Betrieb der Unternehmen einzuführen und sind als zusätzlicher Mechanismus für die Beschäftigten gedacht, um Missstände intern über einen bestimmten Kanal zu melden. Sie ergänzen die regulären Informations- und Meldekanäle, wie beispielsweise Arbeitnehmervertretungen, Qualitätskontrollpersonal oder interne Auditoren, die eigens für die Meldung solcher Missstände eingerichtet wurden. Mit solchen Verfahren wird auf gute Grundsätze der Unternehmensführung gebaut, um die angemessene Funktionsweise sicherzustellen. Die Grundsätze oder unternehmensinternen Richtlinien, die in diesem Zusammenhang entwickelt wurden, beziehen sich auf die Verbesserung der Transparenz, Entwicklung solider Rechnungslegungspraktiken und bezwecken damit die Verbesserung des Schutzes der Betroffenen und der finanziellen Stabilität der Märkte.[89] Grundsätzlich werden bei solchen Verfahren zwei Gruppen von Personendaten bearbeitet. Erstens dem Hinweisgeber und zweitens der beschuldigten Person. Die Arbeitsgruppe stellt fest, dass die Frage, ob Verfahren zur Meldung von Missständen anonym oder offen sein soll (d.h. unter Angabe des Namens auf jeden Fall unter vertraulichen Bedingungen) besondere Aufmerksamkeit verdient. Dabei ist Anonymität keine gute Lösung für den Hinweisgeber oder für das Unternehmen. Denn die Beschwerde ist schwerer zu überprüfen, wenn keine Anschlussfragen gestellt werden können. Zudem können anonyme Meldungen dazu führen, dass sich die Menschen auf den Hinweisgeber konzentrieren, vielleicht mit dem Verdacht, dass er oder sie die Beschwerde aus Bosheit vorgebracht hat. Ein Unternehmen läuft zudem die Gefahr, dass eine Kultur anonymer böswilliger Meldungen entsteht, womit das soziale Klima schlechter werden könnte. Aus Datenschutzsicht stellen anonyme Meldungen eine besonderes Problem dar, da Daten nur nach Treu und Glauben erhoben werden dürfen. Somit sollten ausschliesslich mit Namen versehene Meldungen möglich sein. Wichtig ist aber die vertrauliche Behandlung der Identität des Hinweisgebers.[90]

Die **Übermittlung von Passagierdaten** bei Flügen zwischen Europa und den Vereinigten Staaten von Amerika war erneut ein Thema.[91] Das Verfahren vor dem Europäischen Gerichtshof, welches das Europäische Parlament angestrengt hatte, um den Gleichwertigkeitsbeschluss der Europäischen Kommission anzufechten endete damit, dass dieser Gleichwertigkeitsbeschluss aufgehoben wurde. Damit gab es keine Rechtsgrundlage mehr für die Übermittlung von Personendaten in die USA. In zwei Stellungnahmen zeigte sich die Arbeitsgruppe besorgt über den rechtswidrigen Zustand von Datentransfers in die USA und wies auf die dringende Notwendigkeit hin, eine neue Rechtsgrundlage zu schaffen. Sie stellte gleichzeitig verschiedene Anforderungen an eine neue Grundlage. Zudem wurden verschiedene Möglichkeiten dargelegt, wie vorzugehen wäre, wenn bis zum 30. September 2006 keine internationale Lösung gefunden werden könnte.[92] Am 16. Oktober 2006 wurde ein neues Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika geschaffen. Dadurch konnte der rechtslose Zustand vorerst beendet werden.

[87] Unternehmen, die diesen Anforderungen nicht entsprechen, unterliegen strengen Sanktionen und Strafen durch die NASDAQ, NYSE oder SEC (The Security Exchange Commission), welche für die Überwachung und der Anwendung des SOX zuständig ist. Die betroffenen Unternehmen stehen dabei vor der Gefahr, entweder gegen Datenschutzvorschriften zu verstossen oder von U.S. Behörden bestraft zu werden.

[88] Andere Bereiche (z.B. Human Ressources, Gesundheit und Sicherheit am Arbeitsplatz usw.) sind von dieser Stellungnahme explizit ausgeschlossen

[89] Dabei ist es insbesondere für eine börsennotierte Aktiengesellschaft wichtig, dass Berichte über mutmassliche Rechnungslegungsmanipulationen oder fehlerhafte Rechnungslegung den Vorstand erreichen, damit angemessene Folgemassnahmen ergriffen werden können. In diesem Zusammenhang kann der SOX als eine der Massnahmen gesehen werden, die getroffen wurden, um die Stabilität der Finanzmärkte und den Schutz der berechtigten Interessen der Betroffenen sicherzustellen, in dem Regeln festgelegt wurden, die die angemessene Unternehmungsführung gewährleisten.

[90] Weiters ist zu beachten, dass nur die notwendigen Daten bearbeitet werden und spätestens nach zwei Monaten nach Abschluss der Untersuchungen gelöscht werden sollten (anders ist die Situation, wenn ein Verfahren eingeleitet wurde). Wichtig ist weiters, dass die Betroffenen von der Existenz, dem Zweck und der Funktionsweise des Systems, den Empfängern der Meldungen und den Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten unterrichtet werden.

[91] Vgl. oben, 3.1. und Tätigkeitsbericht 2004, 7.1.

[92] Das annullierte Abkommen mit den USA behielt bis zum diesen Datum Gültigkeit.

Im Tätigkeitsjahr begann die Art. 29 Arbeitsgruppe erstmalig **eine gemeinsame und europaweite Überprüfung** eines ganzen Sektors. Man entschied sich für eine Überprüfung der Krankenversicherungen, da gerade der *Krankenversicherungsbereich* einen sehr grossen Teil der Bevölkerung betrifft und da die Krankenversicherungen zudem in besonderem Ausmasse besonders schützenswerte Daten, nämlich Gesundheitsdaten, bearbeiten. Mit dieser Überwachung sollten Erkenntnisse darüber gewonnen werden, wie die Krankenversicherungen in Europa arbeiten. An dieser wichtigen Tätigkeit konnte aus Liechtensteiner Sicht nicht teilgenommen werden, da dazu die notwendigen Ressourcen fehlten. Es ist allerdings zu hoffen, dass bei der nächsten europaweiten Prüfung teilgenommen werden kann.

Eine wesentliche Aufgabe von Internet Service Provider (ISP) ist der Schutz von Netzen und Geräten. Dazu werden unter anderem so genannte **Filterdienste** eingesetzt. Dabei wird mittels Nachrichtenprüfung versucht, Spam (Werbemüll) und Viren zu erkennen und zu beseitigen.[93] Das Scannen von Nachrichten kann als Abfangen von Nachrichten betrachtet werden. Die Arbeitsgruppe nahm zu den Filterdiensten eine Stellungnahme an. Während Filtersysteme zur *Virenerkennung*[94] und eine sogenannte *Spamfilterung*[95] als legitim bewertet werden, werden Filtersysteme zum *Erkennen festgelegter Inhalte* von der Arbeitsgruppe als kritisch eingestuft, da sie nicht eine notwendige technische oder organisatorische Massnahme für die Sicherheit darstellt: Dem E-Mail-Anbieter droht keine Beeinträchtigung bzw. kein Erliegen seines Kommunikationsdienstes aufgrund des in der elektronischen Post enthaltenen Inhalts. Mit solchen Filterverfahren besteht die Gefahr, dass die E-Mail-Anbieter eventuell völlig legale Inhalte sperren. Dies wirft grundsätzliche Fragen auf. Die Arbeitsgruppe ist daher der Ansicht, dass es E-Mail-Anbietern in der Regel untersagt ist, Nachrichten und die damit verbundenen Verkehrsdaten zu filtern, zu speichern oder auf andere Weise abzufangen, um eventuelle festgelegte Inhalte zu ermitteln. Eine neuere Art von Dienstleistung ist der Dienst der *Lesebestätigung*,[96] welcher das Verfolgen der Öffnung / Weiterleitung von elektronischen Post (Beispiel: E-Mail, SMS) ermöglicht. Die Datenverarbeitung bei solchen Diensten geschieht oft ohne Kenntnis des Empfängers der elektronischen Post und somit ohne dessen Einwilligung. Zusammengefasst kann gesagt werden, dass ISPs der Verpflichtung nachkommen müssen, die Betroffenen über die Verarbeitung persönlicher Daten zu *informieren*.[97] ISPs müssen jederzeit Auskunft über die Identität des für die Verarbeitung Verantwortlichen sowie über die Zweckbestimmungen der Datenverarbeitung geben können. Die Daten müssen nach Treu und Glauben und auf rechtmässige sowie transparente Weise bearbeitet werden. Die ISPs müssen die Teilnehmer auch über die Risiken der Verletzung der Netzsicherheit unterrichten. Auch sollten die Nutzer über Massnahmen informiert werden, welche sie selbst zum Schutz der Sicherheit ihrer Kommunikation einsetzen können.

7.2. VEREINIGUNG DER SCHWEIZERISCHEN DATENSCHUTZBEAUFTRAGTEN

Im Rahmen der Frühjahrstagung der Vereinigung der Schweizerischen Datenschutzbeauftragten[98] in Delémont, wurden die grundrechtlichen und datenschutzrechtlichen Aspekte bei der Gewährleistung der **Sicherheit bei Sportveranstaltungen** thematisiert. Dabei wurde die Einführung einer *Hooligan-Datenbank* zur Bekämpfung von Gewalt bei Sportveranstaltungen nur als schwer mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar qualifiziert. Eine ähnliche Datenbank ist im Rahmen der Revision des Polizeigesetzes auch für Liechtenstein vorgesehen. Die getroffenen Sicherheits-

[93] Weitere Zwecke können sein: Suche und Rechtschreibprüfung sowie Weiterleitung, automatische Antwort, Kennzeichnung dringender Nachrichten, Umwandlung eingehender E-Mails in Textnachrichten für Mobiletelefone, automatisches Sichern und Ablegen in Ordnern, Umwandlung von Text-Links in anklickbare Links etc.

[94] Filtersysteme zur Virenerkennung sind gerechtfertigt, da sie eine technische und organisatorische Massnahme zur Erfüllung der Sicherheit darstellen. Mit dieser Massnahme können die Anbieter auch die Erfüllung von Dienstleistungsverträgen mit ihren Kunden sicher stellen, die erwarten, E-Mails mit einem gewissen Mass an Sicherheit zu empfangen oder zu versenden. Jedoch sollte der Anbieter darauf achten, dass die Inhalte der E-Mail-Nachrichten und der beigefügten Anhänge geheim gehalten und nur den vorgesehenen Personen weiter gegeben werden. Wenn ein Scannen auf Viren aufgrund inhaltlicher Überprüfung stattfindet, sollte dies automatisch und nur für diesen Zweck erfolgen.

[95] Auch Spamfilterung kann mit den gleichen Argumenten wie bei der Virenerkennung als legitim bewertet. Ein Problem kann darin bestehen, dass auch «falsche Treffer», d.h. rechtmässige und erwünschte Mitteilungen durch diese Massnahme unerwünscht als Spam eingestuft werden können. Aufgrund dieser und weiterer Tatsachen sollte der Benutzer die Möglichkeit haben, sich gegen das Scannen von Spam zu entscheiden, die als Spam eingestuften Nachrichten zu prüfen sowie zu entscheiden, welche «Art» von Spam ausgefiltert werden soll. Dem Endbenutzer sollten demnach auch Programme angeboten werden, welche auf dem eigenen Computer oder dem Server des Anbieters installiert und benutzerspezifisch konfiguriert werden können.

[96] Dies ermöglicht unter anderem festzustellen, ob, wann und wie oft z.B. verschickte E-Mails vom Empfänger gelesen wurden oder ob die E-Mails weitergeleitet wurden. Weiters kann insbesondere auch festgestellt werden, von welchem E-Mail-Server an welchen Standort die Weiterleitung vollzogen wurde.

[97] Vgl. oben, 3.2.

[98] Seit der Herbsttagung 2006 in Chur führt die Vereinigung den neuen Namen «privatim» (www.privatim.ch)

massnahmen für die Fussballweltmeisterschaft in Deutschland verlangte zwar zweifellos besondere Sicherheitsmassnahmen. Dennoch sind Massnahmen wie *personifizierte Tickets* oder die *Akkreditierung von Angestellten* oder auch die *Videoüberwachung* mit immer mehr Möglichkeiten wie der Gesichtserkennung sehr weit gehende Datenbearbeitungen. Im Hinblick auf die Fussball-Europameisterschaft 2008, welche auch in der Schweiz durchgeführt wird, ist sich die Vereinigung bewusst, dass zusätzliche Sicherheitsmassnahmen zur Verhinderung von Gewaltausschreitungen notwendig sind. Dennoch ist es wichtig, dass auch das geltende Datenschutzrecht eingehalten wird. Die beschriebenen Massnahmen werden zweifelsohne auch für die EM 2008 relevant werden. Dabei können auch Daten von Personen aus Liechtenstein bearbeitet werden, insbesondere was personifizierte Tickets oder die Videoüberwachung angeht.[99]

Anlässlich der Ende Oktober in Chur stattfindenden Herbsttagung wurden aktuelle Fragen des Gesundheitswesens diskutiert. Themen waren einerseits **«Vertrauensarzt: Wie vertrauenswürdig ist der Vertrauensarzt?»** und andererseits **«Gesundheitskarte: Patientendossier im Portemonnaie?»** In Bezug auf das Thema *Vertrauensarzt* wurde auch durch Vertrauensärzte auf verschiedene Missstände hingewiesen. Die bereits seit 2001 vom Bundesamt für Sozialversicherung geforderten[100] und in einer Entscheidung des Bundesgerichts im Jahre 2005[101] übernommenen klaren organisatorischen Anforderungen an die Gewährleistung der Unabhängigkeit der Vertrauensärzte werden demnach in der Praxis oftmals nicht umgesetzt. Diese Missstände in der Praxis bei den Krankenkassen werden durch verschiedene Aussagen – auch von betroffenen Versicherungen – in einem Bericht des Bundesrates aus dem Jahr 2005 erhärtet.[102] Ein Problem für einen Vertrauensarzt bestehe darin, dass er stets im Spannungsfeld zwischen der Verwaltung der Versicherung einerseits und dem behandelnden Arzt und dem Patienten anderseits stehe. Weiters wurden auch mangelnde Ressourcen und Probleme in der internen Organisation thematisiert. Das Thema «Vertrauensarzt» stellt sich auch in Liechtenstein immer wieder.[103] Beunruhigend ist insbesondere der Umstand, dass in der Schweiz Probleme bestehen, obwohl die gesetzliche Stellung des Vertrauensarztes in der Schweiz im Vergleich zu Liechtenstein besser ist.

Die technologischen Entwicklungen nehmen auch im Gesundheitswesen immer mehr Einzug. Da es sich hier um einen Bereich handelt, in dem höchst sensible Daten bearbeitet werden, ist ein umfassender Schutz derselben unabdingbar. Die Geltung des Arzt- bzw. Patientengeheimnisses ist als wichtiges Element dieser Thematik zu berücksichtigen. Die derzeitige Entwicklung einer Gesundheitskarte, die persönliche Daten des Karteninhabers speichern soll, ist daher unter datenschutzrechtlichen Gesichtspunkten aufmerksam zu verfolgen. In der Schweiz ist diese Gesundheitskarte geplant, in Liechtenstein ist sie bereits in Gebrauch. Allerdings verwaltet die **Gesundheitskarte** in Liechtenstein bislang lediglich rein administrative Daten,[104] die Aufnahme weiterer Daten, nämlich solche über die Gesundheit, ist jedoch geplant[105].

Beide Tagungen waren öffentlich und fanden reges Interesse von Seiten der Medien. Sie sind für alle Interessierten eine Plattform, die nicht nur allein der fachlichen Weiterbildung dient, sondern auch der Stärkung des Informationsaustausches und der Sensibilisierung der Öffentlichkeit für den Datenschutz.

7.3. EUROPARAT

An der jährlich statt findenden Sitzung des Expertenausschusses über den Datenschutz wurde beschlossen, sich mit der Auslegung von verschiedenen gesetzlichen Begriffen zu beschäftigen. Daneben beschloss der Ausschuss die Organisation eines *europäischen Datenschutztages*. Ein solcher Datenschutztag sollte europaweit durchgeführt werden und das Bewusstsein zum Datenschutz stärken. Weiters wurde insbesondere diskutiert, ob man ein Recht auf Datenschutz in das System der Europäischen Menschenrechtskonvention aufnehmen soll. Weiters wurde auch über den Stand der Rati-

[99] Vgl. dazu auch oben, 3.1.
[100] Bericht «Persönlichkeitsschutz in der sozialen und privaten Kranken- und Unfallversicherung»: *http://www.llv.li/amtsstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-gesundheit.htm*
[101] BGE 131 II 413.
[102] Bericht «Regelungslücken im medizinischen Datenschutz in den Sozialversicherungen» unter: *http://www.bsv.admin.ch/aktuell/presse/2005/d/0502230101.pdf*
[103] Vgl. oben, 4.1. und 4.4.
[104] Vgl. Tätigkeitsbericht 2005.
[105] Vgl. oben, 4.5.

fikationen und Unterschriften zum *Zusatzprotokoll zum Datenschutzabkommen* informiert. Dieses wurde bis Ende Dezember 2006 von zwölf Staaten ratifiziert und durch 17 weitere Staaten unterschrieben. Durch Liechtenstein erfolgte noch keine Unterschrift. Das Zusatzprotokoll sieht im Wesentlichen Zweierlei vor: Erstens geht es um eine bessere Regelung von internationalem Datenaustausch und andererseits soll die Stellung der Datenschutzbehörden in ihrer Unabhängigkeit gestärkt werden. Die Schweiz hat dieses Zusatzprotokoll im Jahr 2006 ratifiziert. Dies wäre auch für Liechtenstein sinnvoll.[106]

7.4. EUROPÄISCHE DATENSCHUTZKONFERENZ

An der jährlich stattfindenden Europäischen Datenschutzkonferenz ging es um Themen welche auch in anderen Gremien behandelt wurden wie *RFID*,[107] *Geolokalisierung*,[108] *Whistleblowing*[109] oder *elektronische Gesundheitskarten*.[110] Aber auch mit der Behandlung anderer Themen wie die Bearbeitung von *genetischen Daten*[111] oder die *Wirksamkeit von Datenschutzbehörden* können wichtige neue Erkenntnisse gesammelt werden.

7.5. INTERNATIONALE DATENSCHUTZKONFERENZ

An dieser Konferenz, an der jährlich neben Datenschutzbehörden auch viele Vertreter der Privatwirtschaft teilnehmen, stand die Frage im Zentrum, ob wir uns bereits in einer *Überwachungsgesellschaft* befinden. Anhand einer Studie wurde dargelegt, dass zunehmend wirksamere technische Überwachungsmöglichkeiten im privaten wie auch im öffentlichen Bereich zusammen mit zunehmenden Befugnissen der Sicherheitsbehörden dazu führen, dass die Überwachungsgesellschaft schon sehr nah ist. Die Konferenz ist der Ansicht, dass die Balance zwischen der Sicherheit und der Freiheit in Schieflage gerät, wenn die Tendenz der letzten Jahre zum Ausbau des Sicherheitsapparats fortgesetzt wird.

Verschiedene Resolutionen wurden verabschiedet, darunter die sehr wichtige Initiative «Datenschutz vermitteln und effektiver gestalten» («*London Initiative*»). Sie will den Einsatz der DSB bei der Verteidigung der bürgerlichen Grundrechte international koordinieren, dadurch verstärken und effizienter gestalten. Weiters wurde eine Entschliessung zum Thema *«Datenschutz auf Suchmaschinen»*[112] verabschiedet. Dokumente der Konferenz sind auf dem Internet verfügbar.[113]

[106] Vgl. dazu oben, 4.4.
[107] Vgl. Tätigkeitsbericht 2005, 7.1. und Tätigkeitsbericht 2004, 7.5.
[108] Vgl. Tätigkeitsbericht 2005, 7.1.
[109] Vgl. oben, 7.1.
[110] Vgl. zur Krankenversichertenkarte in Liechtenstein oben, 4.5. und 7.2. sowie Tätigkeitsbericht 2005, 4.5., Tätigkeitsbericht 2004, 4.4. und Tätigkeitsbericht 2003, 3.6.
[111] Genetische Daten sind nicht nur besonders schützenswert, da sie sich auf die Gesundheit beziehen, sondern stellen auch einen Sonderfall dar, da sie nicht nur eine Person, sondern auch auf Familienangehörige betreffen. Genetische Daten sind vor allem für künftige Arbeitgeber und Versicherungen interessant.
[112] Vgl. oben, 3.1.
[113] *http://www.privacyconference2006.co.uk/index.asp?PageID=10*

8. Personelles und Organisatorisches

Die personelle Situation hat sich dank einer befristet angestellten Aushilfe, deren Anstellung auch für 2007 zugesagt wurde, wieder etwas verbessert. Weitere Vorbereitungen zur Verbesserung der Personalsituation waren bei Jahresende noch im Gang.

Die Regierung bezeichnete im Berichtsjahr einen Datenschutzberater beim Amt für Personal und Organisation, beim Ausländer- und Passamt und bei der Landespolizei. Dies kann als eine wichtige Massnahme zur Stärkung des Datenschutzes innerhalb dieser Amtsstellen bezeichnet werden.

9. Ausblick

Die Vorhaben, die für 2006 als prioritär qualifiziert wurden und nicht abgeschlossen werden konnten, sind als Aufgaben für 2007 zu übernehmen. Zusätzlich sind auch neue Tätigkeiten vorzusehen. Es geht insgesamt um Folgendes:

Schaffung von Informationsmaterial

- Richtlinien zur Bearbeitung von medizinischen Daten
- Kommentar zu den Bestimmungen der DSV
- Allgemeine Richtlinien für die Datenbearbeitung durch private Personen
- Vertiefung der Informationen zu Datentransfers ins Ausland
- Information zur Sicherheit von mobilen Endgeräten
- Information zur Datenbearbeitung auf dem Internet
- Bearbeitung von Daten bei Kreditanträgen

Arbeit in Bezug auf die ZPV

- Mitarbeit zu einer gesetzlichen Grundlage zur ZPV
- Bearbeitungsreglement zur ZPV
- Beschaffenheit ZPV[114]

Überwachungsfunktion

- Videoüberwachung
- SWIFT

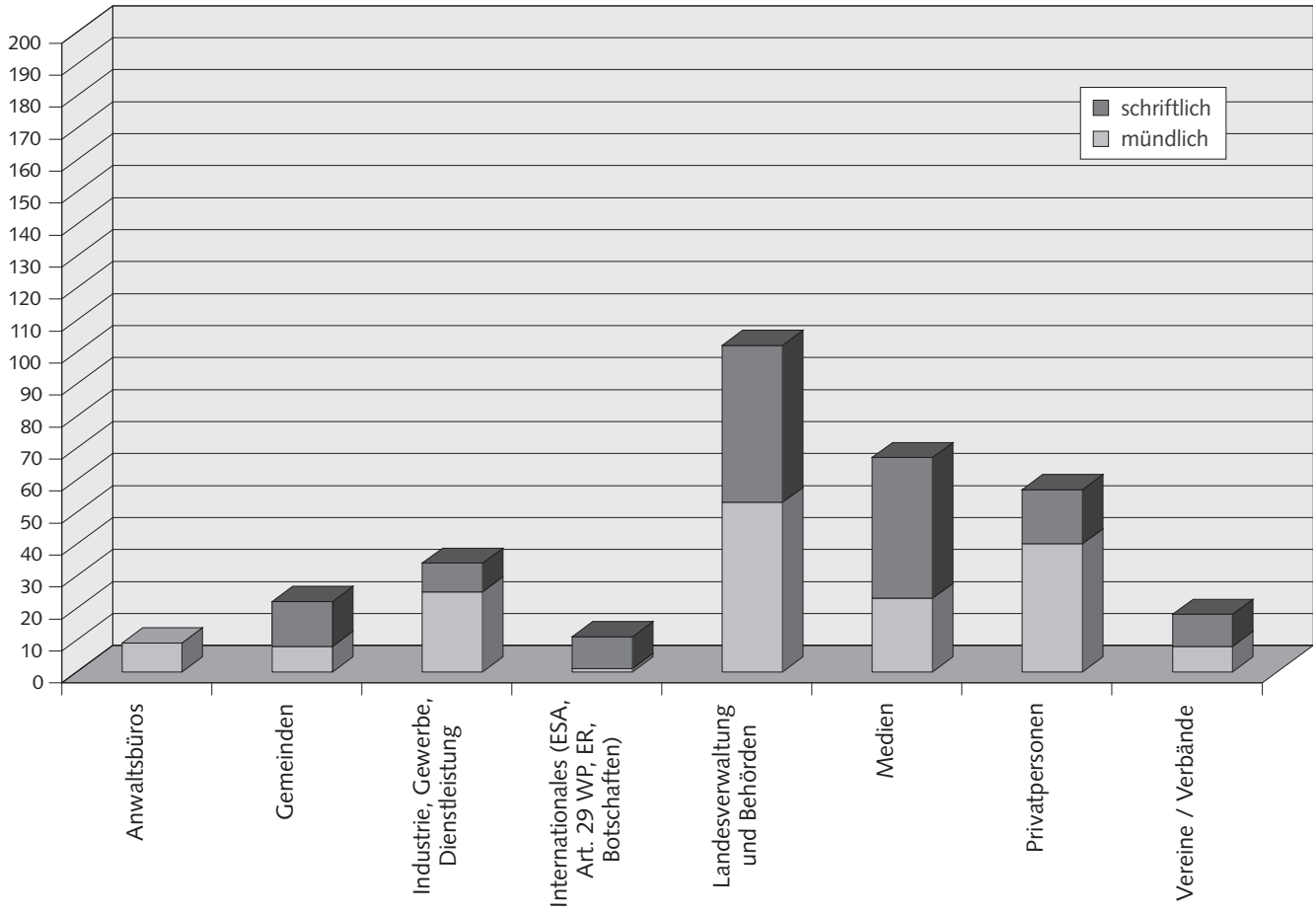
Anderes

- Vorlage für eine Geheimhaltungserklärung
- Vorbereitung eines Beitritts zu Schengen / Dublin

[114] Vgl. dazu oben, 5.1.1.1.

Anhang

ANFRAGEART



GESETZESTHEMEN

	Anwaltsbüros	Gemeinden	Industrie, Gewerbe, Dienstleistung	Internationales	Landesverwaltung und Behörden	Medien	Privatpersonen	Vereine / Verbände	Gesamtergebnis
Anmeldung, Datensammlungen					2				2
Auskunftsrecht					3		3		6
Datenbekanntgabe	1	17	8		45	6	23	7	107
DS Allgemein	1	4	15	9	27	50	28	10	144
Gesetzesvorlagen					21				21
Information der Betroffenen	1		2	1	1				5
Sicherheit		1	2		2	6			11
Übermittlungen ins Ausland	6		6	1	1	4	2		20
Überwachung am Arbeitsplatz			1			1	1	1	4
GESAMTERGEBNIS	**9**	**22**	**34**	**11**	**102**	**67**	**57**	**18**	**320**

Stabsstelle für Datenschutz
Herrengasse 6
FL-9490 Vaduz
Tel. +423 236 60 90
Fax +423 236 60 99
E-Mail: info@sds.llv.li
http://www.sds.llv.li