Tätigkeitsbericht

Datenschutzbeauftragter des Fürstentums Liechtenstein

2007

Inhaltsverzeichnis

1. Vorwort **3**
2. Allgemeines und Pendenzen **5**
3. Information **6**
3.1. Information der Öffentlichkeit durch den Datenschutzbeauftragten 6
3.2. Informationspflichten von Dateninhabern 8
4. Beratung **10**
4.1. Unterstützung von privaten Personen und Behörden durch allgemeine Orientierungen und Beratungen 10
4.2. Stellungnahmen zu Datenschutzfragen in hängigen Verfahren vor Rechtsmittelbehörden – Rechtsprechung zum Datenschutzgesetz 13
4.3. Begutachtung der Gleichwertigkeit des ausländischen Datenschutzes 13
4.4. Stellungnahme zu Vorlagen und Erlassen 13
4.5. Projektbegleitung 16
5. Aufsicht **18**
5.1. Aufsicht über Behörden 18
5.1.1. Datenschutzwidrige Bearbeitungen 18
5.1.1.1. Datenbanken 18
5.1.1.2. Anderes 18
5.1.2. Gesetzliche Grundlagen 18
5.2. Abklärungen und Empfehlungen im Privatrechtsbereich 19
6. Register der Datensammlungen **22**
7. Internationales **23**
7.1. Artikel-29-Arbeitsgruppe der Richtlinie 95/46/EG 23
7.2. Vereinigung der Schweizerischen Datenschutzbeauftragten 25
7.3. Europarat 25
7.4. Europäische Datenschutzkonferenz 25
7.5. Internationale Datenschutzkonferenz 26
8. Personelles und Organisatorisches **27**
9. Ausblick **27**
Anhang **28**

1. Vorwort

Der 5. 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.

Im letzter Zeit haben europaweit einige gravierende Verletzungen des Datenschutzrechts Schlagzeilen in den Medien gemacht. Erinnert sei zum Beispiel an den wiederholten Verlust von Tausenden teilweise sehr sensibler Daten in Grossbritannien[1] oder an das neue und sehr umstrittene Gesetz in Deutschland zur Vorratsdatenspeicherung im Bereich der Telekommunikation, gegen das eine Verfassungsbeschwerde mit nicht weniger als 34 000 Beschwerdeführern einging.[2] Diese Aufzählung liesse sich – leider – noch beliebig fortsetzen. In Liechtenstein zeigte die so genannte Steueraffäre mit einem Schlag die Wichtigkeit des Schutzes der Privatsphäre auf. Dazu kam bekanntermassen der Erpressungsversuch bei einer Bank, wo es auch um Kundendaten ging. Wenn der DSB auch nicht direkt mit diesen Angelegenheiten zu tun hat(te) – das Stichwort «Privatsphäre», das mit dem Begriff des Datenschutzes weitgehend deckungsgleich ist, erhielt mit einem Schlag eine Bedeutung, die vorher in diesem Ausmass unausgesprochen war.

Diese Fälle wie die Tätigkeiten des DSB im Jahr 2007 sollen die Öffentlichkeit weiter für Anliegen der Privatsphäre sensibilisieren.

Genannt seien an dieser Stelle nur einige der wichtigsten Aktivitäten, welche im Bericht zusammen mit weiteren Tätigkeiten vertieft dargestellt werden: Nach wie vor ist es ein wichtiges Anliegen des DSB, die Öffentlichkeit über wichtige und aktuelle Themen zu informieren. Dies geschieht insbesondere über die Internetseite; so wurde über die Wichtigkeit eines starken Passwortes oder über datenschutzfördernde Technologien (Privacy Enhancing Technologies, PETs) informiert. Zudem wurden auch Richtlinien zum Thema Videoüberwachung erlassen wie auch über den Umgang mit unerwünschter Werbung und insbesondere mit Spam (siehe unten, 3.1.). Die Anfragen, welche an die SDS gerichtet werden, zeigen nach wie vor ein sehr breites Spektrum auf. Neben Fragen, welche das Verhältnis Arbeitgeber/Arbeitnehmer betreffen und immer wieder gestellt werden, ging es z.B. um die datenschutzkonforme Veröffentlichung von Gerichtsurteilen, die Versendung amtlicher Unterlagen an Mitglieder von Kommissionen nach Hause, die Einrichtung von Webcams, die Frage, ob E-Mails zu verschlüsseln sind, oder um die namentliche Bekanntgabe einer Personengruppe, damit diese persönlich eingeladen werden können (siehe dazu unten, 4.1.). Das Berichtsjahr war auch geprägt durch wichtige gesetzgeberische Vorhaben. Hierzu erfolgten Stellungnahmen unter anderem zur Abänderung des Sanitätsgesetzes, des Heimatschriftengesetzes, des Gesetzes über das betriebliche Mobilitätsmanagement in der Landesverwaltung oder des Informationsweiterverwendungsgesetzes (siehe dazu unten, 4.4.). Auch im Rahmen des Projekts Integriertes Case Management, welches durch den Sozialfonds, zwei Krankenkassen und die Invalidenversicherung (IV) initiiert wurde, waren der DSB wie auch die Liechtensteinische Ärztekammer involviert (siehe dazu unten, 4.5.).

Im Aufsichtsbereich wurde vor allem die Frage, ob die flächendeckende Videoüberwachung in der Fussgängerzone in Vaduz verhältnismässig ist, der Datenschutzkommission zur Entscheidung vorgelegt (dazu unten, 5.1.1.2.). Bei den meisten der eingegangenen Beschwerden aus dem Privatrechtsbereich ging es entweder um den Erhalt von Werbung in der Form von schriftlichen Postsendungen, E-Mail oder Fax wie auch um Fragen im Verhältnis Arbeitnehmer/Arbeitgeber (siehe dazu unten, 5.2.). Weite Kreise der Landesverwaltung arbeiten mit einer Nummer. Diese Personenidentifizierungsnummer, welche ein ganzes Leben lang für eine Person gilt, verfügt bis heute über keine rechtliche Grundlage (siehe dazu unten, 5.1.2.). Im internationalen Bereich ist insbesondere zu erwähnen, dass ein Dokument zum wichtigen Begriff der Personendaten erstellt wurde, wie auch im Zusammenhang mit dem ebenfalls in Liechtenstein wichtigen Binnenmarkt Informationssystem (IMI). Last but not least wurden Entwicklungen in der Schweiz in Bezug auf einen Beitritt zu den Abkommen von Schengen und Dublin verfolgt (siehe dazu unten, 7.).

[1] Ein Pressebericht der deutschen Zeitung «Der Tagesspiegel», der exemplarisch für eine Vielzahl von Berichterstattungen zu diesem Thema genannt werden kann, ist abzurufen unter: http://www.tagesspiegel.de/politik/international/Grossbritannien;art123,2459399.

[2] Vgl. *http://www.vorratsdatenspeicherung.de/content/view/51/70/*.

Die kürzlich ergangene Entscheidung der Datenschutzkommission, wonach die flächendeckende Videoüberwachung in der Fussgängerzone in Vaduz auf das notwendige Mass zu reduzieren ist, ist nicht nur für den Einzelfall und der wohl auch in Liechtenstein zunehmenden Tendenz des Ausbaus der Videoüberwachung wichtig. Die Entscheidung nimmt die Argumente des DSB auf, wonach staatliche Eingriffe in das Recht auf Privatsphäre auf Grund der Verfassung verhältnismässig sein müssen. So gesehen bekommt diese Entscheidung eine Bedeutung, welche weit über die Videoüberwachung hinaus reicht.

Der Schutz der Privatsphäre bekommt insbesondere im Zusammenhang mit dem anstehenden Beitritt Liechtensteins zu den Abkommen von Schengen und Dublin einen neuen Stellenwert. Der Landtag wird sich noch im Juni mit einer Vorlage zur Änderung des Datenschutzgesetzes (DSG) befassen, welche im Rahmen dieses Beitritts zu sehen ist. Da das Schengener Informationssystem (SIS) Millionen von Personendaten umfasst, muss der Datenschutz dementsprechend Bedeutung finden.

Der Einsatz für die Belange des Datenschutzes wäre ohne die aktive Unterstützung der Regierung und der Landesverwaltung nicht möglich. Deshalb möchte ich an dieser Stelle den Regierungsmitgliedern und -mitarbeitern sowie Kollegen in der Landesverwaltung meinen Dank für die gute Zusammenarbeit aussprechen. Aber auch allen anderen, die mit Anregungen, Anfragen oder Beschwerden dazu beigetragen haben, dass die Belange des Schutzes der Privatsphäre berücksichtigt und oft auch verbessert werden können, gilt mein aufrichtiger Dank.

Ich wünsche Ihnen eine anregende Lektüre.

Vaduz, im Juni 2008

Dr. Philipp Mittelberger
Datenschutzbeauftragter

2. Allgemeines und Pendenzen

Im letzten Tätigkeitsbericht wurden folgende Prioritäten für 2007 festgelegt:

- Allgemeine Informationen für die Datenbearbeitung durch private Personen
- Vertiefung von Informationen zu Datentransfers ins Ausland
- Informationen zur Sicherheit von mobilen Datenträgern
- Information zur Datenbearbeitung auf dem Internet
- Bearbeitung von Daten bei Kreditauskunfteien
- Videoüberwachung
- Swift
- Vorlage für eine Geheimhaltungserklärung

Dazu waren noch verschiedene Pendenzen aus dem Vorjahr zu erledigen, die im Berichtsjahr aus unterschiedlichen Gründen noch nicht vollendet werden konnten:

- Richtlinien zur Bearbeitung von medizinischen Daten
- Kommentar zu den Bestimmungen der DSV
- Arbeiten in Bezug auf die ZPV
- Vorbereitung eines Beitritts zu Schengen / Dublin
- Verschiedene Bearbeitungsreglemente

Nicht vollendet werden konnten im Berichtsjahr: Allgemeine Informationen für die Datenbearbeitung durch private Personen, Informationen zur Sicherheit von mobilen Datenträgern, Information zur Datenbearbeitung auf dem Internet, Bearbeitung von Daten bei Kreditauskunfteien, Vorlage für eine Geheimhaltungserklärung, Richtlinien zur Bearbeitung von medizinischen Daten, Kommentar zu den Bestimmungen der DSV, Arbeiten in Bezug auf die ZPV, Vorbereitung eines Beitritts zu Schengen / Dublin, Bearbeitungsreglemente Krankenkassen.[3]

Einige dieser Vorhaben standen kurz vor einer Fertigstellung; bei anderen war die Stabsstelle für Datenschutz (SDS) auf die Mitarbeit von anderer Seite angewiesen, welche auf sich warten liess. Auf Grund anderer Prioritäten, welche von aussen auf die SDS im Berichtsjahr zukamen, mussten einige der genannten Pendenzen zurück gestellt werden.

[3] Vgl. unten, 9.

3. Information

Eine wichtige gesetzliche Aufgabe des DSB besteht in der Schaffung und Verbesserung des **Datenschutzbewusstseins** der Bevölkerung und der Dateninhaber, also derjenigen Behörden und Personen, welche Daten bearbeiten.[4]

3.1. INFORMATION DER ÖFFENTLICHKEIT DURCH DEN DATENSCHUTZBEAUFTRAGTEN

Die **Internetseite** der SDS[5] ist die Plattform, die über alle wichtigen Themen rund um den Datenschutz informiert wird.

Die Statistik zeigt, dass der Zugriff auf die Webseite weiterhin steigt: Die Anzahl von Zugriffen auf die Internetseite während des Berichtsjahres betrug 54 679 (7 158 unterschiedliche Besucher) im Vergleich zu 50 332 (8 314 unterschiedliche Besucher) Zugriffen im Vorjahr. Daraus ist ein reges Interesse der Bevölkerung an den dort veröffentlichten Themen abzuleiten.

2007 wurde insbesondere über folgende Themenbereiche informiert:

- Datenbearbeitung bei internationalen Zahlungsanweisungen durch Swift und die beteiligten Finanzinstitute.[6]
- *10 Thesen einer datenschutzfreundlichen Informationstechnik:* Der deutsche Bundesbeauftragte für den Datenschutz und die Informationsfreiheit erstellte ein Dokument, in dem aufgezeigt wird, wie Datenschutz und Informationstechnik einhergehen können. Hierzu einige Stichworte im Überblick: Informationstechnik transparent gestalten, Datenschutzanforderungen frühzeitig berücksichtigen, Datenvermeidung und Datensparsamkeit, voreingestellte Sicherheit, Vertraulichkeit der Kommunikation stärken, Datenschutzwerkzeuge.[7]
- *Privacy Enhancing Technologies (PET):* PETs sind technologische Massnahmen, welche in Ergänzung zu rechtlichen Massnahmen den Schutz der Privatsphäre bezwecken. Die Europäische Kommission fördert die Entwicklung durch die Privatindustrie und fordert den Einsatz von PETs auch durch Behörden. Als konkrete Beispiele nennt die Kommission Verschlüsselungsanwendungen, «Platform for Privacy Preferences» (PPP), Programme zur automatischen Datenanonymisierung oder «Cookie Cutters». Angesichts des unumkehrlichen Trends zur automatischen Datenverarbeitung stellt der Einsatz von PETs eine wichtige Massnahme dar, um eine datenschutzkonforme Bearbeitung zu ermöglichen.[8]
- Nur ein starkes *Passwort* (eine Kombination von Zahlen und Wörtern, klein und gross geschrieben), das sicher aufzubewahren ist, kann vor einem Missbrauch von Daten schützen.[9] Angesichts der zunehmenden Bedeutung des Internet und auf Grund der steigenden Bedrohungen durch das Internet ist ein starkes Passwort für den eigenen Schutz sehr wichtig.
- *Whistleblowing:* Hierbei handelt es sich um unternehmensinterne Hotlines, an welche mutmassliche Missstände gemeldet werden können. Aus Datenschutzsicht wird Wert darauf gelegt, dass die Meldung nicht anonym erfolgen darf, da sonst ein Denunziantentum gefördert werden könnte. Vielmehr muss der Whistleblower seinen Namen hinterlegen, wobei die Unternehmen die vertrauliche Behandlung der Angaben zu gewährleisten haben.[10]
- In einer Stellungnahme der Art.-29-Arbeitsgruppe wird der zentrale *Begriff der «Personendaten»* definiert. Da diese für die Praxis viele wertvolle Beispiele auflistet, informierte der DSB hierüber ausführlich auf der Internetseite, über welche auch die vollständige Stellungnahme abgerufen werden kann.[11]
- Die *Rechtssprechung der Eidgenössischen Datenschutzkommission* stellt eine wichtige Informationsquelle zum Datenschutzrecht auch in Liechtenstein dar, da das Bundesgesetz für den Datenschutz der Schweiz als Rezeptionsvorlage des DSG gedient hatte. Die Rechtsprechung der Eidgenössischen Datenschutz- und Öffentlichkeitskommission von 1993 – 2006 wurde auf dem Internet veröffentlicht.[12]

[4] Vgl. Art. 31 Abs. 2 und Art. 32 Abs. 1 Buchstabe a DSG.
[5] *http://www.sds.llv.li*
[6] Vgl. unten, 3.2. und 5.2.
[7] Vgl. *http://www.llv.li/amtsstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-technisches/llv-sds-spezialthemen-datenschutzfreundliche_informationstechnik.htm.*
[8] *www.llv.li/amtsstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-technisches/llv-sds-privacy_enhancing_technolgies.htm.*
[9] Vgl. *http://www.llv.li/amtsstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-technisches/llv-sds-informationssicherheit-internetsicherheit.htm.*
[10] Vgl. unten, 7.1., Tätigkeitsbericht 2006, 7.1 und *http://www.llv.li/amtsstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-finanzielles-2/llv-sds-spezialthemen-whistleblowing-5.htm.*
[11] Vgl. unten, 7.1. Die Stellungnahme ist abzurufen unter: *http://www.llv.li/pdf-llv-li-stellungnahme_4_2007_zum_begriff_personenbezogene_daten-2.pdf.*
[12] *http://www.fir.unisg.ch/Datenschutz/urteile.html.*

Ausführlichere Informationen zu diesen und anderen Themenbereichen sind auf der Internetseite verfügbar.

Das Konzept der Webseite ist einfach: Alle grundsätzlichen Informationen werden auf der Webseite veröffentlicht. Die Neuigkeiten bezüglich Datenschutz und werden zusätzlich per E-Mail verschickt, über die auf die Fundstellen hingewiesen wird, wo sich ausführliche Informationen befinden. Diese elektronischen **Newsletter** können als Dienstleistung auf einfache Weise in Anspruch genommen werden. Um den Newsletter zu abonnieren, genügt es, wenn man auf der Startseite unter der Rubrik «Newsletter» seine eigene E-Mail-Adresse eingibt. Es fallen keine Kosten an und wenn man keine Nachrichten mehr erhalten möchte, kann man sich selber abmelden. Mit Ende des Berichtsjahres waren es 236 Abonnenten, was im Vergleich zum Vorjahr einen Zuwachs von 42 Neuabonnenten bedeutet.[13]

Ein weiteres Mittel zur Information sind die vom DSB erarbeiteten **Richtlinien** zu ausgewählten Themenbereichen. Das DSG ist naturgemäss abstrakt gehalten und auch die Datenschutzverordnung (DSV) gibt nur wenige konkrete Anhaltspunkte für die Handhabung des Datenschutzes in der Praxis. Deshalb ist es sinnvoll, zu aktuellen, immer wieder auftretenden Fragen entsprechende Informationen herauszugeben, die einer konkreten Handhabung des Gesetzes dienlich sind.[14]

Im Berichtsjahr wurden zwei neue Richtlinien erarbeitet. Zum einen Richtlinien über *Videoüberwachung durch Behörden*. Die Erfahrungen zeigen, dass die Videoüberwachung des öffentlichen Raums durch Behörden ein Thema von zunehmenden Interesse ist. Die Notwendigkeit klarer Umschreibungen der Voraussetzungen für eine Videoüberwachung durch Behörden lag damit klar auf der Hand. Die vorliegenden Richtlinien sollen den Behörden daher die rechtlichen und praktischen Mindestanforderungen für eine geplante Videoinstallation erläutern:[15] *Bevor* eine Videoüberwachungsmassnahme tatsächlich angeordnet wird, muss die zuständige Behörde prüfen, ob eine Videoüberwachung überhaupt die einzig sinnvolle Lösung ist. Neben der Möglichkeit einer Videoüberwachung ist nach anderen Optionen zu suchen, welche nicht so stark in die Privatsphäre von betroffenen Personen eingreifen, z.B. bauliche Massnahmen oder vermehrte Polizeipatrouillen. Alle denkbaren Lösungsmöglichkeiten sind gegeneinander abzuwägen. Erst dann, wenn sich alle anderen Massnahmen als nicht tauglich oder als nicht durchführbar erweisen, und wenn zweitens eine genügend bestimmte Gesetzesgrundlage[16] vorhanden ist, stellt sich die Frage der Verhältnismässigkeit. Also erst in einem dritten Schritt ist zu prüfen, ob die Videoüberwachung im konkreten Fall sowohl geeignet als auch notwendig ist, um den verfolgten Zweck zu erreichen. Damit ist die Frage gemeint, ob die konkrete Videoüberwachung tatsächlich dazu geeignet ist, z.B. Vandalismus vorzubeugen, die Kriminalitätsquote zum Sinken zu bringen und im Rahmen der Strafverfolgung massgeblich zur Identifikation des Täters und Klärung des Sachverhalts beizutragen. Die Verhältnismässigkeit ist zudem in zeitlicher und räumlicher Hinsicht zu betrachten. Das bedeutet, dass eine Videoüberwachung vielleicht nur über Nacht stattfindet oder nur an ausgewählten Punkten, sog. hot spots, erfolgt.

Zum anderen erliess der DSB *Richtlinien über den Umgang mit unerwünschter Werbung und insbesondere mit Spam*, da viele Personen immer wieder mit unerwünschter Werbung konfrontiert werden. Dies gilt insbesondere für Spam. Mit den Richtlinien orientiert der DSB die betroffenen Personen über einen korrekten Umgang mit unerwünschter Werbung bzw. mit der Frage, was man dagegen tun kann:[17] In Bezug auf Direktwerbung kennt das DSG eine Spezialvorschrift.[18] Danach ist die betroffene Person grundsätzlich vorgängig zu informieren und auf das ihr zustehende unentgeltliche und sofort wirksame Widerspruchsrecht hinzuweisen, wenn ihre Personendaten für Zwecke der Direktwerbung bearbeitet werden sollen. Zu berücksichtigen ist in diesem Zusammenhang jedoch auch, dass eine Datenbearbeitung dann gerechtfertigt ist, wenn die betroffene Person ihre Daten selbst allgemein zugänglich gemacht hat, z.B. über eine private Homepage. Dies ist vielen privaten Internet-Benutzern nicht bewusst. Für elektronische Direktwerbung (Spam) gibt es eine weitere spezialgesetzliche Regelung.[19] Danach ist insbesondere E-Mail-Werbung grundsätzlich zulässig, wenn der Empfänger den Versand durch vorherige ausdrückliche Einwilligung gestattet hat oder der Empfänger als Kunde dem Spammer seine E-Mail-Adresse be-

[13] Ende 2006 hatten 194 Personen den SDS-Newsletter abonniert.
[14] Die Richtlinien sind ebenfalls über die Webseite abrufbar, können aber auch jederzeit bei der SDS angefordert werden.
[15] Vgl. *http://www.llv.li/richtlinie_videoueberwachung_behoerden.pdf*.
[16] Vgl. hierzu unten, 5.1.1.2.
[17] Vgl. *http://www.llv.li/richtlinie_umgang_unerwuenschter_direktwerbung_spam-2.pdf*.
[18] Art. 14. Abs. 3 DSG.
[19] Art. 50 Kommunikationsgesetz (KomG).

reits übermittelt hat und nicht von vorneherein oder nachträglich deren Verwendung zu diesem Zweck abgelehnt hat. Um die Einwilligung des Kunden zu erlangen, muss der Versender der Direktwerbung vor dem Versenden der eigentlichen Werbung einmalig mittels elektronischer Post den potentiellen Empfänger ersuchen, ob E-Mail-Werbung an besagte E-Mail-Adresse gesendet werden darf. Erst wenn der potentielle Empfänger in die Versendung eingewilligt hat, darf die eigentliche Direktwerbung per E-Mail verschickt werden (so genannte Opt-in-Lösung).[20] Um gegen die unerwünschte Werbung vorgehen zu können, hat die betroffene Person das Recht, jederzeit vom Inhaber einer Datensammlung Auskunft darüber zu verlangen, wie die Daten erhoben wurden und welche Daten bearbeitet werden. Auf der Webseite der SDS steht ein *Musterschreiben zur Geltendmachung des Auskunftsrechts* zur Verfügung; mit weiteren zur Verfügung stehenden Musterschreiben können auch die Sperrung oder Löschung von Daten verlangt werden.[21] In den Richtlinien werden noch viele weitere, insbesondere auch technische Hinweise gegeben, wie man sich gegen unerwünschte Werbung schützen kann. Als ausgewählte Beispiele können der Einsatz von Verschlüsselungen[22] und von Spam-Filtern[23] genannt werden. Damit die persönliche E-Mail-Adresse weitestgehend vor Spam geschützt ist, sollte diese nur für ausschliesslich private oder berufliche Zwecke verwendet werden. Für die Teilnahme an Wettbewerben oder für Bestellungen sollten eine zweite oder gar dritte, nicht namensbezogene E-Mail-Adresse benutzt werden. Auch der gute alte Brief sollte als Alternative nicht in Vergessenheit geraten; für persönliche Informationen ist der Brief immer noch der beste Weg der Übermittlung. Denn man sollte sich immer vor Augen halten, dass eine E-Mail wie eine Postkarte zu lesen ist.

Ausserdem nahm der DSB an mehreren **Schulungen und Informationsveranstaltungen** teil, anlässlich derer er zum Teil Vorträge bzw. Referate gehalten hat. So hielt er zum Beispiel am *NetworkingDay* des Fachbereichs Wirtschaftsinformatik der Hochschule Liechtenstein einen Vortrag zum Thema *«Datenschutz und Datensicherheit in Theorie und Praxis»*: So wurde die Bedeutung der Datensicherheit insbesondere in Bezug auf Wirtschaftsspionage oder allgemein Identitätsdiebstahl aufgezeigt. Auch die Technik kann dabei nicht einen totalen Schutz garantieren, auch mit biometrischen Systemen nicht. Schwachpunkt ist und bleibt der Mensch.[24]

In den liechtensteinischen **Medien** wurde verschiedentlich über Datenschutz oder die SDS berichtet. Im Zentrum stand die Veröffentlichung unseres Tätigkeitsberichts. Gerade die Veröffentlichung des Tätigkeitsberichts wurde auch von verschiedenen deutschen oder schweizer Medien zum Anlass einer Berichterstattung über den liechtensteinischen Datenschutz genommen.[25]

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,[26] 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 waren die Folgenden:

In Bezug auf die **SWIFT**-Affäre, die bereits im Jahr 2006 ihren Anfang nahm, kamen die Banken den Anforderungen des Datenschutzes nach. In diesem Zusammenhang sei darin erinnert, dass die Society for World Wide Interbank Financial Telecommunication (SWIFT) ein weltweit agierender Überwei-

[20] Vgl. unten, 5.2 sowie Tätigkeitsbericht 2006, 5.2.
[21] Vgl. *https://www.llv.li/form-llv-sds-musterschreiben.htm.*
[22] Vgl. unten, 4.1.
[23] Vgl. Tätigkeitsbericht 2006, 7.1.
[24] Vgl. auch Symantec Internet Security Threat Report Trends for July–December 06: *http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf.*
[25] Vgl. insbesondere Datenschutz und Datensicherheit (DuD), Ausgabe 9/2007, S. 713.
[26] Vgl. Art. 5 DSG; Tätigkeitsberichte 2004, 2005, 2006, je 3.2.

sungsdienst ist, welcher auch im Auftrag der in Liechtenstein tätigen Banken internationale Zahlungsanweisungen übermittelt. SWIFT unterhält einen Spiegelserver in den USA. Die U.S. amerikanischen Behörden nahmen sich die Möglichkeit heraus, unter Umständen auch auf europäische Transaktionsdaten zugreifen zu können. Vor allem von Seite der Art.-29-Arbeitsgruppe bestand die Forderung an die Banken darin, die Kunden über diesen möglichen Zugriff zu informieren.[27] Im Berichtsjahr fanden verschiedene Besprechungen zwischen dem DSB und dem Bankenverband zu diesem Thema statt. Der Bankenverband kam stellvertretend für die Banken der Aufforderung nach, den Datentransfer ins Ausland zu melden, wie es das Datenschutzgesetz vorsieht[28]. Weiters konnte über den Bankenverband eine koordinierte Information der Kunden erwirkt werden. Dies führte dazu, dass die Banken ihre Allgemeinen Geschäftsbedingungen änderten. Nun wird darauf aufmerksam gemacht, dass im Falle der Abwicklung über internationale Kanäle die Auftragsdaten ins Ausland gelangen. In diesem Fall sind die Daten nicht mehr durch liechtensteinisches Recht geschützt und es ist nicht mehr sichergestellt, dass das Schutzniveau hinsichtlich dieser Daten demjenigen in Liechtenstein entspricht. Schliesslich wird auch darüber informiert, dass ausländische Gesetze und behördliche Anordnungen die involvierten Banken und Systembetreiber dazu verpflichten können, diese Daten gegenüber Dritten offen zu legen.

In einem der liechtensteinischen *Schwimmbäder* wurde Ende des letzten Jahres eine **Videoüberwachung** eingeführt, als es zu beträchtlichen Sachbeschädigungen im Garderobenbereich kam. Auf Anfrage des Schwimmbades wurden folgende Bearbeitungszwecke ersichtlich: Erstens eine Verhinderung bzw. Aufklärung von Vandalismus und eine Überwachung des Schwimmbeckens, dessen Teil für den Bademeister nicht von der Kabine aus ersichtlich war. Diese Bearbeitungen sind nicht zu beanstanden. Demgegenüber war im Duschbereich ebenfalls eine Kamera angebracht. Da diese Kamera jedoch nicht mit den angegebenen Zwecken zu vereinbaren war, wurde empfohlen, diese Kamera zu entfernen. Insgesamt ist weiterhin darauf hinzuweisen gewesen, dass das Schwimmbad als Dateninhaber die stattfindende Videoüberwachung deutlich anzeigen muss. Auch bei der Videoüberwachung im *Städtle Vaduz* ist grundsätzlich auf die Videoüberwachung hinzuweisen. Dem kommt die Gemeinde Vaduz durch die mehrere Hinweisschilder nach, aus denen sich jedoch nicht die Orte der einzelnen, insgesamt 16 Kameras ergeben.[29]

Auch im Rahmen der Projektbegleitung zum **Integrierten Case Management** wurde auf eine entsprechende Information des betroffenen Personenkreises hingewiesen.[30]

[27] Vgl. Tätigkeitsbericht 2006, 5.2.
[28] Vgl. Art. 8 DSG.
[29] Vgl. unten. 5.1.1.2.
[30] Vgl. unten, 4.5.

4. Beratung

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

In der **Anfragenstatistik**[31] ist zu sehen, von wem Anfragen zu welchen Themenkreisen an die SDS gerichtet wurden.[32] Wie aus der Anfragenstatistik ersichtlich ist, nahmen im Vergleich zum Vorjahr die Anfragen leicht zu, von 320 auf 338 Anfragen. Während nach wie vor Behörden am meisten Anfragen stellen, war auf der einen Seite ein Anstieg der Anfragen von Anwaltsbüros zu vermerken, wohingegen auf der anderen Seite vor allem Medienanfragen markant zurückgingen. Die Anfragen von Privatpersonen nahmen weiter zu, was Zeichen eines weiterhin wachsenden Bewusstseins für den Datenschutz in der Bevölkerung ist.

Eine Darstellung sämtlicher Anfragen sowie Antworten würde den Rahmen dieses Berichts sprengen. Erwähnt sei an dieser Stelle jedoch das breite Spektrum derselben. Gerade in diesem Bereich spiegelt sich die Bandbreite wider, in wie vielen unterschiedlichen Themenbereichen Datenschutz relevante Fragen eine nicht unwesentliche Rolle spielen. Erwähnt seien an dieser Stelle exemplarisch folgende Anfragen:[33]

Bei verschiedenen Anfragen ging es um die *Veröffentlichung von Gerichtsurteilen* auch auf dem Internet bzw. der Frage der Anonymisierung von Personendaten. Hierzu ist Folgendes festzustellen: Auch wenn aufgrund der Kleinheit des Landes eine vollständige Anonymisierung der Daten von Parteien in einem Gerichtsverfahren sehr schwierig ist, muss dennoch das Mögliche getan werden um das Recht auf die Privatsphäre der betroffenen Personen zu berücksichtigen.

Vereinzelt wurde auch durch *Vereine* danach gefragt, ob eine interne und/externe Bekanntgabe von Vereinsmitgliedern möglich ist. Hierzu ist festzuhalten, dass ein Vereinsmitglied nicht dazu gezwungen werden kann, dass intern oder extern seine Mitgliedschaft bekannt gegeben wird. Vielmehr ist hier die (stillschweigende) Einwilligung nötig.

Weiters wurde danach gefragt, ob es aus Datenschutzsicht in Ordnung ist, wenn *amtliche Unterlagen an Mitglieder von Kommissionen nach Hause verschickt* werden, wenn diese Kommissionen sensible Personendaten bearbeiten. Diese Frage steht im Zusammenhang mit dem Stichwort «Datenschutz zu Hause».[34] Das Postgeheimnis gilt grundsätzlich nur bis zum Erhalt einer Postsendung.[35] Dies bedeutet, dass ab dem Erhalt einer Postsendung der Adressat derselben für eine vertrauliche Behandlung zuständig ist. Die Frage, ob z.B. Familienmitglieder solche Unterlagen einsehen können oder nicht steht in der Verantwortung des Adressaten. Eine solche Anfrage wurde auch gestellt in Bezug auf die *Versendung von Unterlagen durch die Invalidenversicherung*.

Eine Anfrage aus der Privatwirtschaft betraf die Frage, ob eine *Webcam* so positioniert werden kann, dass allein der öffentliche Raum vor dem Firmengebäude im Kamerablickfeld wäre. Damit sollte die Anzahl der Besucher und Kunden gesteigert werden. Die Bilder sollten übers Internet abrufbar sein. Eine private Webcam, deren Bilder übers Internet abrufbar sind, ist mit einer Videoüberwachung vergleichbar.[36] Für den rechtmässigen Einsatz von Webcams gibt zwei Möglichkeiten.[37] Kritisch ist auch, wenn die Bildaufnahmen übers Internet abrufbar und damit für jedermann zugänglich sind und unkontrolliert weiter verarbeitet werden können. Auch ein Abrufen von und nach Ländern, in denen der Datenschutz als nicht gleichwertig mit dem liechtensteinischen einzustufen ist, wäre so möglich. Unter Berücksichtigung all dieser Erwägungen ist es in jedem Fall zu bevorzugen, wenn die Personen nicht identifizierbar sind, so dass das DSG nicht anwendbar ist. Deshalb ist in diesen Fällen zu empfehlen, dass bei der Einstellung von privaten Webcams mit technischen und organisatorischen Massnahmen sichergestellt ist, dass die betroffenen Personen nicht bestimmbar sind.

In einer weiteren Anfrage richtete sich ein Unternehmen an den DSB und fragte danach ob eine *unverschlüsselte Sendung von E-Mails* an eine Behörde nicht problematisch ist. Hierzu ist festzustellen, dass ein E-Mail oft mit einer Postkarte verglichen

[31] Vgl. Anhang.

[32] Angaben wie Anzahl der geführten Telefonate, der behandelten Anfragen, der verfassten Stellungnahmen oder der verschickten E-Mails sind nur beschränkt aussagekräftig. Der Arbeitsaufwand für eine einzelne Anfrage variiert je nach Komplexität. Während es bei telefonischen Anfragen oft mit einem Telefonat erledigt ist, kann es aber auch sein, dass ein Telefonanruf eine grössere Akte auslöst. Gut dokumentiert ist der Arbeitsaufwand in Bezug auf Stellungnahmen zu Gesetzesvorhaben.

[33] Rückfragen zu ein und dem selben Themenkomplex werden bei ähnlicher Fragestellung nicht separat erfasst.

[34] Vgl. unten, 4.5.

[35] Vgl. Art. 25ff. Postgesetz.

[36] Vgl. Tätigkeitsbericht 2006, 5.1.1.2.

[37] Entweder wird die Webcam so ausgerichtet, dass keine Personen identifizierbar sind. Damit wäre das DSG nicht anwendbar. Sobald die abrufbaren Bilder es aber ermöglichen, Personen zu bestimmen, liegt ein Bearbeiten von Personendaten vor; die Bestimmungen des DSG sind einzuhalten. D.h. die Personen dürfen nur bei Vorliegen eines Rechtfertigungsgrundes nach Art. 16f. DSG erfasst werden.

wird. Bei beiden kann jeder grundsätzlich die Informationen einsehen bzw. bei einer E-Mail kann sogar der Inhalt geändert werden. Deshalb ist eine unverschlüsselte Versendung vertraulicher E-Mails nicht zu empfehlen.[38]

Eine wiederholte Anfrage betraf eine mögliche *Bekanntgabe von volljährigen Schweizer Bürgern an den Schweizer Verein hinsichtlich der Militärpflicht*. Hintergrund dieser Anfrage war eine Änderung der Rechtslage in der Schweiz. Während der DSB offen liess, ob eine solche Bekanntgabe im Interesse der betroffenen Personen nach Art. 23 DSG liegt, betont er in einer Stellungnahme, dass die Einwohnerkontrollen der Gemeinden die Doppelbürger nicht erfassen. Dementsprechend wäre eine teilweise Bekanntgabe, nämlich nur der «einfachen» Schweizer Bürger an den Schweizer Verein eine diskriminierende Behandlung. Demgemäss könne eine entsprechende Bekanntgabe nicht stattfinden. In diesem Zusammenhang ist immer wieder festzustellen, dass es Anfragen gibt, wonach bestimmte Personen persönlich zu gewissen Ereignissen eingeladen werden sollen. Es ist verständlich, dass z.B. eine Vereinigung oder ein Unternehmen ein eigenes Interesse daran hat, dass sie Adressen erfahren kann. Dies muss jedoch nicht dem Interesse der Personen, welche angeschrieben werden sollen, entsprechen. Eine persönliche Einladung wie dies im Fall des Schweizer Vereins gewünscht wurde, ist nicht das einzige Mittel, um auf ein Anliegen hinzuweisen. Vielmehr kann z.B. in den Zeitungen informiert werden, dass z.B. eine Informationsveranstaltung für Stellungspflichtige stattfindet. Man muss diese nicht persönlich dazu anschreiben.

Das Landesspital gelangte an den DSB mit der Bitte um Überprüfung eines *Vertrauensarzt-Konzeptes*, das zwischen dem Landesspital und den Kassen ausgehandelt worden war und unter anderem Regelungen über die Stellung des Vertrauensarztes und die Datenbearbeitung durch ihn vorsieht. Der DSB hielt fest, dass der Vertrauensarzt nach dem KVG eine Filterfunktion zwischen der Verwaltung und der Kasse und den Patienten einnimmt. Demgemäss hat er die Persönlichkeitsrechte des Patienten zu wahren. Es stellte sich die Frage wie vorzugehen ist, wenn bei der Krankenkasse Unklarheiten bestehen. Sollte demgemäss nur der Vertrauensarzt an den Belegarzt gelangen können oder unter Umständen auch die Verwaltung der Kasse selbst? Um den gesetzlichen Auftrag des genannten Filters nachzukommen, schlug der DSB vor, dass die Verwaltung der Kasse nur auf ausdrückliche Anweisung des Vertrauensarztes an den Belegarzt gelangen kann, um Unklarheiten zu regeln.

In einer Anfrage ging es darum, ob das Landesspital Daten von Patienten *an die Seelsorge bekannt gegeben* werden kann. Auch hier ist davon auszugehen dass eine Einwilligung bestehen muss. Wenn der Patient möchte dass ein Seelsorger über seinen Aufenthalt im Spital informiert ist, steht dem selbstverständlich nichts gegenüber.

Im Rahmen der Einführung eines Systems zum «*Integrierten Case Management*» trat die Projektleitung an den DSB mit der Bitte heran, die erforderlichen Vertragsabschlüsse, Erklärungen und Vollmachten aus datenschutzrechtlicher Sicht zu begutachten.[39] Im Laufe der sehr konstruktiven Zusammenarbeit wurden schlussendlich Musterdokumente erarbeitet, die den Voraussetzungen des DSG und einschlägigen Spezialgesetzen vollends Genüge tun. Die Einführung selbst konnte in 2007 noch nicht erfolgen, war aber für den Anfang des Folgejahres anvisiert.

Im Zusammenhang mit der Einführung eines *Krebsregisters* im Gesundheitsgesetz[40] kam die Frage auf, ob die Erfassung einer Person in so einem Krebsregister obligatorisch ausgestaltet werden soll. In Anbetracht der sensiblen Situation, in der sich die betroffenen Personen in der Regel befinden, wurde eine Meldepflicht nicht befürwortet. Ein Zwang wäre angesichts der heiklen Fragen nicht sachgerecht. Vielmehr sollte die Nützlichkeit einer solchen Datenbearbeitung mitgeteilt und die Einwilligung der Betroffenen eingeholt werden.

Nach Art. 44 Abs. 4 Versicherungsaufsichtsgesetz (VersAG) kann ein in Liechtenstein ansässiges Versicherungsunternehmen ausnahmsweise von dem Versicherungsgeheimnis entbunden werden. Die *Entbindung vom Versicherungsgeheimnis* erteilt bei Nachweis eines ausgewiesenen Interesse die zuständige Aufsichtsbehörde nach Rücksprache mit den DSB. Da es sich bei der Vorschrift um eine Ausnahmevorschrift handelt, sind entsprechende Anträge, restriktiv hand zu haben. Im Berichtsjahr gab es dann auch nur einen entsprechenden Antrag zu bearbeiten.

[38] Vgl. dazu z.B. Informationen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB): *http://www.edoeb.admin.ch/themen/00794/01124/01250/index.html?lang=de*.
[39] Vgl. ausführlich hierzu unten, 4.5.
[40] Vgl. unten, 4.4.

Die Frage, ob die *Übermittlung von liechtensteinischen Autohalterdaten an österreichische Behörden* im Falle von Verkehrsdelikten rechtmässig ist, war Gegenstand einer weiteren Anfrage. In diesem Zusammenhang ist wichtig zu wissen, dass eine umgekehrte Bekanntgabe, also eine Übermittlung von österreichischen Halterdaten an die liechtensteinischen Behörden aufgrund einer Entscheidung der österreichischen Datenschutzkommission aus dem Jahre 2005 für unzulässig erklärt worden war. Seit 2005 wurden demzufolge keine österreichischen Kfz-Halterdaten mehr an Liechtenstein bekannt gegeben. In Folge dieser Entscheidung stellte sich u.a. die Frage, ob dies bedeutet, dass liechtensteinische Halterdaten ebenfalls nicht mehr bekannt gegeben werden dürfen. Hierzu wurde festgehalten, dass dem nicht so ist.[41] Vielmehr hat aufgrund des Pariser Abkommens von 1926 in bestimmten Fällen eine Weitergabe der Halterdaten zu erfolgen. Auch für Österreich gilt das Pariser Abkommen als nach wie vor gültige Rechtsgrundlage für einen entsprechenden Datenaustausch. Dies wurde im Jahre 2006 zwischen Liechtenstein und Österreich bekräftigt. Danach wurde die frühere Praxis wieder aufgenommen; d.h. es wurde wieder ein Transfer der Halterdaten von Österreich nach Liechtenstein ermöglicht. In Bezug auf die gestellte Anfrage war zu bemerken, dass die Bekanntgabe von liechtensteinischen Autohalterdaten an österreichische Behörden im Zusammenhang mit Verkehrsdelikten auf Grundlage des vorgenannten Pariser Abkommens legal war und ist.

Ausserdem wurde die Frage behandelt, welche grundbuchrelevanten Daten den *Geometern* durch das Grundbuch- und Öffentlichkeitsregisteramt (GBOERA) in einem Abrufverfahren zur Verfügung gestellt werden können. Gesetzlich vorgesehen ist ein Zugriff auf alle notwendigen Daten.[42] Die Praxis zeigt, dass heute die Geometerbüros einen elektronischen Zugriff auf sämtliche Grundstücke in allen Gemeinden haben, obwohl die Büros nicht in allen Gemeinden tätig sind. Dies ist teils auch damit zu erklären, dass eine definitive Zuteilung noch nicht stattgefunden hat. Der DSB hielt fest, dass spätestens ab dem Zeitpunkt der definitiven Zuteilung der Gemeinden die Zugriffe durch die Geometer auf diese Gemeinden beschränkt werden müssen, da nur diese notwendig im Sinne des Gesetzes sind. Weiters wurde auch die Frage einer vertraglichen Regelung mit den Geometern bzw. sogar mit den Gemeinden besprochen. Aus Datenschutzsicht wurde hierzu festgehalten, dass es drei Elemente für eine Vereinbarung gibt, welche zu berücksichtigen sind: Erstens sind die Daten nur für den vorgesehenen Zweck zu bearbeiten. Dies ist deshalb wichtig, da die Geometer nicht nur einen öffentlich-rechtlichen sondern auch privatrechtlichen Zweck verfolgen. Damit kann eine Vermischung von Aufgaben stattfinden. Zweitens sind die Daten geheim zu halten und vertraulich zu behandeln. Und drittens sind die Daten zu löschen, wenn sie nicht mehr zur Arbeit benötigt werden.

Im Rahmen einer privaten Anfrage ging es um die *Weitergabe von Angaben aus dem Privatleben eines Zeugen*, die anlässlich seiner Aussage im Rahmen eines strafrechtlichen Ermittlungsverfahrens gemacht werden mussten und zum Teil über den konkreten Fall hinaus gingen. In der Folge hatte die angeklagte Person unter anderem Zugang zu dieser Zeugenaussage und machte den Inhalt einem grösseren Personenkreis zugänglich. Angaben, welche eine Person im Rahmen eines Strafverfahrens machen muss und welche über den konkreten Fall hinaus gehen, sind bestimmt nicht dafür da, anderen unbeteiligten Personen zugänglich gemacht zu werden; zumal wenn es sich um heikle Angaben über das Privatleben handelt. Ein solcher Sachverhalt kann strafbar sein.

Immer wieder werden Fragen in Bezug auf die *Internet- und / oder E-Mailüberwachung* am Arbeitsplatz gestellt. In diesem Zusammenhang gingen im Berichtsjahr auch einige Anfragen von Angestellten bzw. von ehemaligen Angestellten von Unternehmen ein, welche Auskunft in Bezug auf die sie betreffenden Daten insbesondere im Personalakt des Unternehmens erhalten wollten.[43] Diesbezüglich ist zu sagen, dass das *Auskunftsrecht* nach dem DSG[44] ein umfassendes Auskunftsrecht ist. Der (ehemalige) Arbeitnehmer hat ein gesetzliches Recht darauf, zu erfahren, was der Arbeitgeber über ihn weiss. In Bezug auf die Landesverwaltung wurde ebenfalls verschiedentlich das gesetzliche Auskunftsrecht in Anspruch genommen. Da es sich bei der ZPV um ein sehr komplexes System handelt, erklärte sich der DSB bereit, mit den jeweiligen Ämtern bzw. dem für die Informatik zuständige Amt für Personal und Organisation eine Wegleitung zur Beantwortung von Auskunftsbegehren zu erstellen. Der DSB wurde auch durch eine Gemeinde angefragt, wie auf die Inanspruchnahme des gesetzlichen Rechts auf Auskunft zu reagieren ist.

[41] Vgl. Tätigkeitsbericht 2006, 3.1.
[42] Vgl. Art. 632 e Abs. 1 des Sachenrechts.
[43] Vgl. unten, 5.2.
[44] Vgl. Art. 11 DSG.

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

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.[45]

An dieser Stelle sollte jedoch ein richtungsweisendes Urteil des Staatsgerichtshofs nicht unerwähnt bleiben, das zwar das DSG nicht direkt betrifft, das allerdings einen datenschutzrechtlichen Bezug aufweist: Der liechtensteinische Staatsgerichtshof hat als Verfassungsgerichtshof ein grundlegendes Urteil zur (internationalen) Amtshilfe und zum Bankkundengeheimnis gefällt.[46] Danach kommt dem **Bankkundengeheimnis** materiell **Verfassungsrang** zu, auch wenn es nur auf Gesetzesstufe verankert ist. Es soll die finanziellen Aspekte der Geheim- und Privatsphäre eines Rechtssubjektes im Rahmen der gesetzlichen Schranken schützen. Dieser Schutz wird durch das in Art. 32 der liechtensteinischen Landesverfassung genannte verfassungsmässig gewährleistete Recht der persönlichen Freiheit geschützt.

Das Bankkundengeheimnis wird danach nicht verletzt, wenn die zuständige Aufsichtsbehörde bei einer Anfrage um internationale Amtshilfe die in Art. 36 Bankengesetz[47] ausdrücklich verankerten Prinzipien der Spezialität, der Vertraulichkeit, des Grundsatzes der «langen Hand» und der Verhältnismässigkeit befolgt. Amts- und Rechtshilfe sind nicht immer leicht auseinander zu halten. Das Amtshilfeverfahren kann dann nicht die Strafrechtshilfe umgehen, wenn die Amtshilfe unter Einhaltung dieser Prinzipien erfolgt. Da zusätzlich zum Anfangsverdacht weitere Elemente vorliegen müssen, die einen hinreichend begründeten Verdacht auf das Vorliegen einer strafrechtlich relevanten Verhaltensweise ergeben, sind so genannte «fishing expeditions», d.h. das Amtshilfeverfahren als solches als Vorwand für eine reine Beweisausforschung zu missbrauchen, nicht möglich und nicht zulässig.

4.3 BEGUTACHTUNG DER GLEICHWERTIGKEIT DES AUSLÄNDISCHEN DATENSCHUTZES

Im Rahmen der Art. 29 Arbeitsgruppe wurde die Datenschutzgesetzgebung auf den *Faröer Inseln* und auf *Jersey* analysiert. Die Gruppe kam zu dem Schluss, dass von einer Gleichwertigkeit des Datenschutzes ausgegangen werden kann.[48]

4.4. STELLUNGNAHME ZU VORLAGEN UND ERLASSEN

Eine der Aufgaben des DSB ist es, zu gesetzlichen Vorlagen und Erlassen, die für den Datenschutz erheblich sind, Stellung zu nehmen und die Übereinstimmung mit den Bestimmungen der Richtlinie 95/46/EG zu überprüfen. 2007 gab der DSB zu mehr als 20 Gesetzesvorhaben eine Stellungnahme ab. Auszugsweise soll an dieser Stelle auf folgende Gesetzesvorhaben im Einzelnen kurz eingegangen werden:

Anlässlich der Stellungnahmen zu den Vernehmlassungsberichten über die Änderung des **Gesetzes betreffend die Anerkennung von Hochschuldiplomen und beruflichen Befähigungsnachweisen, des Ärztegesetzes, des Gesetzes über das Veterinärwesen, des Gesetzes über die Rechtsanwälte, die Treuhänder und die Patentanwälte sowie über des Gesetzes für die im Bauwesen tätigen Ingenieure und Architekten** war vor allem die Einführung des Internal Market Information System (IMI)[49] von datenschutzrechtlicher Relevanz. In den Stellungnahmen wurde auf die Wichtigkeit einer einheitlichen Regelung für die verschiedenen Berufsgruppen hingewiesen. Es wurde im Wesentlichen angeregt, sich in den verschiedenen Gesetzestexten möglichst nahe am Text von Art. 56 Abs. 2 der Berufsqualifikationsrichtlinie zu halten und auf die umfangreiche Stellungnahme der Art.-29-Datenschutzgruppe zu den durch das IMI aufgeworfenen datenschutzrechtlichen Aspekten verwiesen.[50] Zum Ende des Berichtsjahres 2007 waren noch nicht alle der im Zusammenhang mit IMI stehenden Gesetzesrevisionen abgeschlossen.

[45] Vgl. Art. 32 Abs. 1 Buchstabe b DSG.

[46] Urteil des Staatsgerichtshofs vom 06. Februar 2006, StGH 2005/50, das erst im Jahr 2007 veröffentlicht wurde in: Liechtensteinische Juristenzeitung, 2007, LES 4/07, S. 396ff.

[47] Bereits in 2003 bestätigte die Verwaltungsbeschwerdeinstanz (VBI) in einer Entscheidung die grundsätzliche Anwendbarkeit des Datenschutzes auf bank- und börsenrechtliche Amtshilfeverfahren. Im konkreten Fall ging es ebenfalls um die Auslegung von Art. 36 Bankengesetz, vgl. ausführlich hierzu Tätigkeitsbericht 2003, 3.3. Die vollständige Entscheidung ist abzurufen unter: *http://www.llv.li/pdf-llv-sds-vbi_entscheid-2.pdf*.

[48] Stellungnahme 9/2007 der Art.-29-Datenschutzgruppe zum Umfang des Schutzes personenbezogener Daten auf den Färöern, WP 142, angenommen am 09. Oktober 2007, abzurufen unter: *http://ec.europa.eu/Justice_home/fsj/privacy/index:de.htm, vgl. dazu und zu Jersey auch unten, 7.1*.

[49] Grenzüberschreitendes Computersystem zur grenzüberschreitenden Übermittlung von ausgewählten Personendaten innerhalb des EWR.

[50] Stellungnahme 7/2007 der Art.-29-Datenschutzgruppe zu Fragen des Datenschutzes im Zusammenhang mit dem Binnenmarkt-Informationssystem, WP 140, angenommen am 21. September 2007, abzurufen unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp140_de.pdf; vgl. unten, 7.1.

Im Rahmen der Abänderung des **Bankengesetzes** wurden datenschutzrelevante Pflichten in Bezug auf behördliche Zusammenarbeit oder in Zusammenhang mit Kunden, insbesondere eine allgemeine Informationspflicht gegenüber den Bankkunden, neu eingeführt. Erwähnenswert ist insofern, dass diese Informationspflicht nicht nur gegenüber dem bereits bestehenden Kundenkreis, sondern in Anlehnung an die Richtlinien 2004/39/EG und 2006/73/EG gleichwohl auch gegenüber potenziellen Kunden besteht. Eine entsprechende und umfängliche, wenn möglich vorherige Information von den betroffenen Personen ist ein zentrales Anliegen im Datenschutzrecht und ist unter anderem auch im Rahmen von Werbung von Wichtigkeit. Vor diesen Hintergrund ist die Einführung einer eigenen Bestimmung im Bankengesetz sehr zu begrüssen. Diese sollte den Vorgaben des Datenschutzgesetzes entsprechen.

Mit der Schaffung eines **Gesetzes über die Weiterverwendung von Informationen öffentlicher Stellen (Informationsweiterverwendungsgesetz)** wird die Informationsweiterverwendungs-Richtlinie 2003/98/EG in nationales Recht umgesetzt. In seiner Stellungnahme hat der DSB zum einen auf die aufschlussreiche Stellungnahme 7/2003 der Artikel-29-Datenschutzgruppe zur Weiterverwendung von Informationen des öffentlichen Sektors und Schutz personenbezogener Daten Bezug genommen.[51] Zum anderen wurde insbesondere eine gleichzeitige Abänderung des Datenschutzgesetzes in Art. 17 Abs. 2 Buchstabe f und Art. 23 Abs.1 Buchstabe c DSG angeregt. Im Unterschied z.B. zum deutschen DSG dürfen nach dem liechtensteinischen Gesetzestext nur dann Personendaten bearbeitet werden, wenn die betroffene Person die Daten selbst allgemein zugänglich gemacht hatte. Der DSB strebt hier jedoch eine liberalere Handhabung an. Aus diesem Grund hat der DSB eine Änderung dahingehend vorgeschlagen, dass es als Rechtfertigungsgrund ausreiche, wenn die Personendaten allgemein öffentlich zugänglich sind (z.B. Telefonbuch). Dies würde eine grosszügigere Praxis erlauben, die auch im Lichte des neuen IWG sinnvoll und wünschenswert wäre. Das Widerspruchsrecht nach Art. 16 Abs. 3 DSG bleibt hiervon unberührt.

Wie angedeutet, wurde der DSB frühzeitig in Bezug auf die Schaffung des **Gesetzes über das betriebliche Mobilitätsmanagement in der Landesverwaltung** einbezogen. Zur Regelung der Einsehung in die Motorfahrzeughalterdaten der MFK wurde grundsätzlich eine positive Stellungnahme abgegeben, da gesetzlich vorgeschrieben ist, dass die entsprechenden Daten nach Art. 9 DSG mit geeigneten technischen und organisatorischen Massnahmen zu schützen sind und somit den Vorgaben des DSG Genüge getan wird.

Von besonderer datenschutzrechtlicher Relevanz war ausserdem die Abänderung des **Polizeigesetzes**, die im Jahr 2007 in Kraft trat. Im Rahmen der polizeilichen Ermittlungskompetenzen wurden etliche neue Rechtsgrundlagen geschaffen: So ist unter bestimmten Voraussetzungen die Erhebung und Bearbeitung biometrischer Daten zulässig; auch der Einsatz von Bild- und Tonträgern bei Massenveranstaltungen oder an allgemein öffentlich zugänglichen Orten ist nun bei Erfüllung bestimmter Bedingungen möglich. Die grundsätzliche Zulässigkeit einer Videoüberwachung durch die Landespolizei ist in Liechtenstein die bislang erste und einzige gesetzliche Regelung einer Videoüberwachung im öffentlichen Raum und ist allein schon aus diesem Grunde von entscheidender Bedeutung für den Datenschutz. Weiterhin wurden zahlreiche Regelungen für die (internationale) Amtshilfe sowie die Rechtsgrundlage für ein elektronisches Informationssystem geschaffen. Dieses Informationssystem ist aus datenschutzrechtlicher Sicht nicht ganz unproblematisch, da es die Verknüpfung verschiedener Datenbanken ermöglichen soll. Gänzlich neu eingeführt wurde zudem ein indirektes Auskunftsrecht. Soweit Staatsschutz oder Ermittlungen zur vorbeugenden Bekämpfung einer Straftat tangiert sind, kann die betroffene Person nicht selbst, sondern nur über den DSB Auskunft von der Landespolizei begehren, ob Daten über sie bearbeitet werden.[52] Erfahrungen in der Schweiz hatten gezeigt, dass es bei der Einführung dieses indirekten Auskunftsrechtes eine Fülle von verfahrensmässigen und rechtlichen Problemen gab.[53] Dem Datenschutzbeauftragten war es ein grosses Anliegen, diese Fragestellungen frühzeitig zu lösen, was bis Jahresende nicht möglich war.

Als Folge der Revision des Polizeigesetzes stand auch eine Anpassung des **Heimatschriftengesetzes (HSchG)** an. Die Geset-

[51] Stellungnahme 7/2003 der Art.-29-Datenschutzgruppe zur Weiterverwendung von Informationen des öffentlichen Sektors und Schutz personenbezogener Daten, WP 83, angenommen am 12. Dezember 2003, abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp83_de.pdf*.

[52] Vgl. Art. 34h Polizeigesetz.

[53] Vgl. Tätigkeitsbericht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (früher EDSB, jetzt EDÖB), 1998/1999, S. 38f., abzurufen unter: *http://www.edoeb.admin.ch/dokumentation/00445/00509/00554/index.html?lang=de*.

zesänderung sah u.a. vor, dass der Landespolizei ohne jede zeitliche Einschränkung ein dauernder Online-Zugriff auf das Passregister gewährt werden soll. Dem ist aus datenschutzrechtlicher Sicht kritisch gegenüber zu stehen. Denn eigentlich benötigt die Landespolizei nur ausserhalb der Öffnungszeiten des Passamtes einen direkten Zugriff auf das Passregister; ansonsten können die Mitarbeiter des Passamtes in Erfüllung ihrer gesetzlichen Aufgabe die gewünschte Auskunft erteilen. De facto handelt es sich also lediglich um Zeiten am Wochenende und in der Nacht. Der DSB hat darauf hingewiesen, dass unter dem Gesichtspunkt der Verhältnismässigkeit eine zeitliche Eingrenzung des Zugriffs wünschenswert wäre.

Im Rahmen der anvisierten Abänderung des **Sanitätsgesetzes** wurde vom Datenschutzbeauftragten die Einbindung eines noch aufzubauenden *Krebsregisters*[54] angeregt. Bereits vor längerer Zeit wurde ein Anliegen an den Datenschutzbeauftragten herangetragen, ein Krebsregister aufzubauen. In verschiedenen Ländern und auch in verschiedenen Kantonen der Schweiz gibt es ein Krebsregister. Mit diesem Krebsregister werden Personen erfasst, welche unter Krebs leiden. Deren Daten werden zur Forschung im wichtigen Kampf gegen Krebs genutzt. Somit steht einem Krebsregister an und für sich nichts entgegen. Zentral bei diesem Anliegen ist jedoch, dass die betroffenen Personen ihre Einwilligung geben müssen. Da jedoch der Staat ein solches Register aufbauen und führen soll, wurde durch den Datenschutzbeauftragten geltend gemacht, dass es eine gesetzliche Grundlage braucht. Die Schaffung dieser Grundlage im Rahmen des Sanitätsgesetzes wurde daher angeregt.

Die Revision des **Statistikgesetzes** wurde begrüsst. Das bisherige Statistikgesetz stammt aus dem Jahr 1974 und weist einige Lücken auf, auf die die Regierung zu Recht hinwies. Die Schaffung eines modernen Statistikgesetzes ist wichtig, damit die Statistik die von der Regierung gewünschte Funktion als Führungsinstrument wahrnehmen kann. Die Statistik lebt zu einem überwiegenden Teil von Personendaten, welche ausgewertet werden. Dementsprechend wichtig ist der richtige Umgang mit Personendaten.

Die Modernisierung und Vereinheitlichung des **Zustellgesetzes**, wie sie in der Vernehmlassungsvorlage vorgestellt wurde, wurde aus Sicht des DSB begrüsst. Unter datenschutzrechtlichen Aspekten wurde jedoch insbesondere auf folgende zwei Punkte hingewiesen: Das neue Zustellgesetz regelt, wann welches Dokument von wem an wen wie zugestellt werden muss und ist vor allem im Rahmen von Gerichts- und Behördenverfahren anzuwenden. Das Datenschutzgesetz ist allerdings in Bezug auf hängige Zivil-, Straf- und Rechtshilfeverfahren sowie Verwaltungsbeschwerdeverfahren gerade nicht anzuwenden.[55] [56] Bedenklich ist die in der Vernehmlassungsvorlage vorgesehene Möglichkeit, dass die schriftliche Verständigung einer Hinterlegung unter gewissen Voraussetzungen auch an die Eingangstüre (Wohnungs-, Haus-, Gartentüre) angebracht werden kann.[57] Schon allein die Praktikabilität dieser Zustellmöglichkeit ist fragwürdig. Denn äussere, nicht beeinflussbare Umstände können ohne weiteres eine Kenntnisnahme der Verständigung verhindern. Sei es, dass ein starker Wind den Zettel fort reisst, Regen die Mitteilung unleserlich macht oder dass ein Nachbar das Papier wegnimmt. Aber auch aus Sicht der verfassungsrechtlich geschützten Privatsphäre ist diese Art der Ersatzzustellung nicht ganz unproblematisch: Durch den öffentlichen Anschlag an der Eingangs- oder Gartentüre können Mitbewohner, Nachbarn, aber auch zufällig vorbeikommende Passanten Kenntnis davon nehmen. Die Verständigung aber ist ausschliesslich für den Adressaten bestimmt, da bereits die Verständigung auch für Unbeteiligte gewisse Rückschlüsse zulassen kann. Dies bedeutet eine Verletzung der Privatsphäre der betroffenen Person, wenn die Verständigung Informationen zum Gegenstand der Zustellung enthält. Aus diesen Gründen hat der Datenschutzbeauftragte in seiner Stellungnahme zur Vernehmlassungsvorlage diese Art der Zustellung hinterfragt und dessen Streichung vorgeschlagen.

Eine Stellungsnahme zum Vernehmlassungsbericht betreffend die Verordnung über den Gesundheitsberuf **Naturheilpraktiker** wurde verfasst. Hinsichtlich der Bestimmung zur Aufbewahrung der Daten durch die Naturheilpraktiker wurde angeregt, sich möglichst an die Vorlage des Ärztegesetzes zu halten. Ausserdem wurde angeregt, dass die Daten nur zweckbestimmt bearbeitet werden dürfen.

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

[54] Vgl. oben, 4.1.
[55] Vorbehalt nach Art. 2 Abs. 3 Buchstabe c DSG.
[56] Dieser Ausschluss führt dazu, dass das Datenschutzgesetz in Zusammenhang mit dem neuen Zustellgesetz nicht immer anwendbar wäre. Aus Gründen der Rechtsicherheit und Normenklarheit hat der DSB daher in seiner Stellungnahme empfohlen, im neuen Zustellgesetz eine klare Aussage darüber zu treffen, ob das Datenschutzgesetz anwendbar ist oder nicht und wie mit dem Ausschlussvorbehalt umzugehen ist. Dies erscheint umso notwendiger, da die Vorlage des neuen Zustellgesetzes keine eigenen datenschutzrechtlichen Regelungen enthält.
[57] Art. 18 Abs. 2 Satz 2 des neuen Zustellgesetzes laut Vernehmlassungsvorlage.

Vorentwurf eines Ausländergesetzes, Bearbeitung von Personendaten (Sammelvorlage), Energieeffizienzgesetz, Finanzkonglomeratsgesetz, Gesetz über den Erwerb und Verlust des Landesbürgerrechts, Verordnung zur Festlegung der Kostenziele in der obligatorischen Krankenpflegeversicherung, Landwirtschaftsgesetz, Milchmengenregelungsgesetz, Personen- und Gesellschaftsrecht, Strafprozessordnung[58], Umweltschutzgesetz[59], Gesetz über den unlauteren Wettbewerb (UWG), Wirtschaftsmassnahmengesetz (neu: Sanktionengesetz), Stiftungsrecht sowie zu einem Vorhaben zur Schaffung einer rechtlichen Grundlage für die Zentrale Personenverwaltung der Landesverwaltung (Vorentwurf zum ZPVG).

4.5. PROJEKTBEGLEITUNG

Ein Schwerpunkt der Projekt begleitenden Arbeit des DSB lag in 2007 im Gesundheitsbereich.

Im Rahmen des Projekts **«Elektronisches Gesundheitsnetz (eGN)»** wurde eine Bestandsaufnahme zum Datenpool vorbereitet. Dieser *Datenpool*, welcher durch den Krankenkassenverband geführt wird, umfasst die Branchendaten der liechtensteinischen Krankenversicherungen nach KVG im Bereich der Krankenpflege (OKP) und der freiwilligen Versicherungen. Der Datenpool ist ein Instrument zur Beurteilung der Wirtschaftlichkeit der Behandlung nach Art. 19 KVG. Danach melden die Kassen dem Kassenverband für jedes Kalenderjahr die an die einzelnen Leistungserbringer erbrachten Kostenvergütungen. Der Kassenverband fasst diese Angaben im Datenpool zusammen. Dieser Datenpool wird nach Vorbild des Datenpools des Kassenverbandes der Schweiz, der Santésuisse, geführt. Die Regierung beauftragte die Projektgruppe eGN mit der Frage, wie die Zukunft des Datenpools, der (noch) in der Schweiz liegt, aussehen soll. Ein Kernproblem des gegenwärtigen Datenpools ist es, dass wenig Transparenz besteht und vor allem die Leistungserbringer nicht genau wissen, wie er funktioniert. In diesem Sinne schlägt die Arbeitsgruppe eine Sensibilisierung bzw. Information über den Datenpool vor. Damit soll Vertrauen geschaffen werden und die Schaffung eines zweiten Datenpools auf Seite der Leistungserbringer verhindert werden. Diskutiert wurde unter anderem auch, ob detailliertere Auswertungen bzw. sogar Publikationen gemacht werden sollten. Der DSB hielt hierzu fest, dass es aufgrund der Kleinheit des Landes sein kann, dass in Bezug auf einzelne Fachgruppen nur ein einziger bzw. sehr wenige Leistungserbringer vorhanden sind, wodurch die betroffenen Personen leicht bestimmbar wären. Bei einer Auswertung von Tarifpositionen, welche möglicherweise im Fall einer Erweiterung auf einen Tarifpool in Zukunft erfasst werden, ist das Augenmerk weiterhin auf eine statistische Auswertung der Daten zu richten.

Beim Teilprojekt *«Originalrechnung an den Patienten»* im Rahmen des Projektes eGN ging es um Folgendes: Die zunehmenden Kosten im Gesundheitswesen sind allseits bekannt und gelten als ein grosses Problem. Ein Aspekt davon ist die Verbesserung der Kenntnis der Patienten in Bezug auf die durch ihn ausgelösten Kosten im Gesundheitswesen. Heute ist es so, dass in Liechtenstein ein Patient eine Abrechnung durch die Krankenkasse erhält, auf welcher nur sehr rudimentäre Angaben zur einer Behandlung vorhanden sind. Angaben über die Behandlung und Medikamentenkosten werden bislang überhaupt nicht gemacht. Dies ist nicht ideal. Die Idee beim Teilprojekt «Originalarztrechnung» besteht nun darin, dass der Patient eine Kopie der Rechnung des Arztes bekommen soll, auf welcher die genauen Angaben zur Behandlung aufgestellt sind. Mit diesen genaueren Angaben über eine Behandlung soll das Bewusstsein der Patienten über die anfallenden Kosten vertieft werden. Ausgehend von dieser Grundidee befasste sich die Arbeitsgruppe eGN weiter mit der Frage, wie die Schaffung dieses Kostenbewusstseins anzugehen ist. Während es schon nach der aktuellen Gesetzeslage möglich ist, jederzeit Auskunft zu bekommen[60] und dies zwar in Bezug auf Ärzte, Krankenkassen oder auch Andere, soll es in Zukunft so sein, dass ein Patient bei seinem Arzt eine Art «Informations-Abonnement» bestellen kann hinsichtlich aller Behandlungen, welche ihn betreffen. Bei der Frage, wer die entsprechenden Kosten tragen soll, argumentierte der DSB, dass die Kosten nicht durch den Patienten selbst getragen werden sollen. Denn Ziel sei es ja, ein entsprechendes Kostenbewusstsein bei den Patienten zu schaffen; es sei widersinnig, ein solches Bewusstsein zu fördern, gleichzeitig aber den Patienten diesbezüglich zur Kasse zu bitten. Auf jeden Fall ist es aber durchaus im Sinne des Datenschutzes bzw. des Rechtes auf informationelle Selbstbestimmung, wenn eine möglichst gute Transparenz geschaffen und der Patient informiert wird. So gesehen begrüsste der DSB die Grundidee. Thematisiert wurde auch, dass durch ein solches «Abonnement» mehr gesundheitsbezogene Informationen an die Adres-

[58] Unter anderem zur Umsetzung der II. Geldwäscherei-Richtlinie 2001/97/EG sowie der revidierten 40 FATF-Empfehlungen.
[59] Hier wurde angeregt, eine Regelung einzuführen, wonach die Kataster elektronisch geführt werden.
[60] Auskunftsrecht nach Art. 11 DSG.

se des Patienten verschickt werden. Dabei ist festzuhalten, dass der Patient selbst dafür zuständig ist, wie solche Postsendungen insbesondere zu Hause eingesehen werden können («Datenschutz zu Hause»).[61] Das (Teil-)Projekt war 2007 noch nicht abgeschlossen.

Mit dem Integrierten **Case Management (ICM)** konnte noch ein weiteres Projekt im Gesundheits-/Versicherungsbereich erfolgreich begleitet werden.[62] Hierbei geht es in Kurzform um eine aktive Unterstützung eines längerfristig arbeitsunfähigen Arbeitnehmers bei der Wiedereingliederung ins Arbeitsleben. Eine solche Abwesenheit kann auf einen Unfall oder auch auf eine Krankheit zurückzuführen sein. In der heutigen Gesellschaft sind auch psychische Probleme am Arbeitsmarkt vermehrt zu verzeichnen (z.B. Mobbing, Burnout etc.). Um eine frühe Wiedereingliederung in die Arbeitswelt von Arbeitnehmern zu erleichtern, entstand die Idee der Einführung des ICM. Dabei geht es darum, dass im Fall der Meldung des Arbeitgebers an die Krankenkasse zur krankheitsbedingten Abwesenheit eines Arbeitnehmers, die Krankenkasse einen Case Manager einsetzen kann. Dieser Case Manager meldet sich sodann beim Arbeitnehmer und fragt nach, ob er etwas tun könne, damit eine Wiedereingliederung ins Arbeitsleben erleichtert wird. Der Arbeitnehmer kann dies ablehnen oder dem auch zustimmen. Eine Zustimmung erscheint gerade in Fällen von Problemen mit dem Arbeitgeber als sinnvoll, da hier somit eine fachlich geschulte, neutrale Zwischenstelle eingeschaltet wird.

In diesem Zusammenhang ist auch zu bedenken, dass mit der letzten Revision des Invalidengesetzes (IVG) eine Früherfassung eingeführt wurde, welche dasselbe Ziel verfolgt.[63] Im Rahmen der gesetzlichen **Früherfassung** gibt es ein bei der IV angesiedeltes Case Management, welches spätestens nach sechs Wochen beginnt.[64] Obwohl sich die Regierung der Gefahr bewusst war, das die Befassung der IV stigmatisierend sein könnte und konzeptionell den Nachteil aufweist, das damit in den Köpfen der Beteiligten die «Schiene in Richtung Rente» weist und daher die Schaffung einer IV-unabhängigen Stelle zu bevorzugen sei, wurde aus zeitlichen und organisatorischen Gründen zumindest vorläufig die Früherfassung im IVG eingeführt.[65] Wenn ein solcher Fall also IVG-relevant ist, wird er in einem Sachverständigenrat besprochen, an dem ein Vertreter der IV, der zuständigen Krankenkasse und dem jeweiligen Case Manager teilnehmen. Schliesslich beteiligt ist auch der Sozialfonds Liechtenstein, welcher als Projektpartner teilnimmt.[66] Neben der aktiven Unterstützung der Arbeitnehmer mit dem Ziel, seine Arbeitsfähigkeit wieder herzustellen, sollen durch das ICM mittelfristig auch Kosten eingespart werden. Eine längerfristige krankheitsbedingte Abwesenheit bzw. der Bezug von Invaliditätsrenten belasten das Gesundheitssystem mit enormen Kosten, die letztendlich die Allgemeinheit zu tragen haben. Die SDS wurde durch die Projektleitung zum Integrierten Case Management in Zusammenarbeit mit dem Sozialfonds um Stellungnahme gebeten. Grundsätzlich ist ein solches Vorhaben zu begrüssen. Durch das Projekt wird ein Handeln vor Eintreten der gesetzlichen Frist nach IVG ermöglicht. Wichtig aus Sicht des Datenschutzes ist, dass die teilnehmenden Arbeitgeber die Arbeitnehmer entsprechend transparent informieren. Eine Teilnahme durch den Arbeitnehmer ist freiwillig und hat nur mit dessen Einverständnis zu geschehen.[67] Deshalb erstellte die SDS eine Mustererklärung, mit der der Versicherte dem Case Manager der Krankenkasse bzw. der IV eine Vollmacht erteilt, seinen Fall zu behandeln und die nötigen Informationen bei beteiligten Personen (z.B. behandelnden Ärzten) einzuholen. Weiters ist auch das Verhältnis des Case Managers zur Krankenkasse bzw. zur IV ein sehr wichtiges Element. Die SDS arbeitete in diesem Zusammenhang ein weiteres Muster aus, welches für den Auftrag zwischen der Kasse bzw. der IV mit dem Case Manager dienen kann. Die Reaktionen auf diese Mustertexte waren positiv.

Im Rahmen des Vorprojektes **«Enterprise Content Management»** (ECM) der liechtensteinischen Landesverwaltung (Stichwort: papierloses Büro)[68] erfolgte keine nennenswerte Tätigkeit.

[61] Vgl. oben, 4.1.
[62] Vgl. auch 4.1.
[63] Vgl. dazu Tätigkeitsbericht 2006, 4.4.
[64] Nach Art. 32 a IVG hat der Arbeitgeber, die Krankenkasse oder der zuständige Arzt nach sechs Wochen die IV über eine seit sechs Wochen bestehende Abwesenheit vom Arbeitsplatz zu informieren.
[65] Vgl. Bericht und Antrag der Regierung zur Abänderung des Gesetzes über die Invalidenversicherung und weiterer Gesetze vom 23. Mai 2006, Nr. 48/2006; Auszug aus den Erläuterungen zu Art. 32bis IVG (Meldung und Abklärung und weitere Schritte), S. 33.
[66] Der Sozialfonds Liechtenstein ist eine der grössten Pensionskassen des Landes.
[67] Dies gilt auch im Falle der Früherfassung nach IVG.
[68] Vgl. Tätigkeitsbericht 2006, 4.5. und Tätigkeitsbericht 2005, 4.5.

5. Aufsicht

5.1. AUFSICHT ÜBER BEHÖRDEN

5.1.1. DATENSCHUTZWIDRIGE BEARBEITUNGEN

5.1.1.1. DATENBANKEN

Die Datenschutzverordnung (DSV) sieht für gewisse Bearbeitungen von Datenbanken vor, dass ein **Bearbeitungsreglement** zu erstellen ist. Das Bearbeitungsreglement zur ZPV, die eine sehr komplexe Datenbank darstellt, konnte von der Arbeitsgruppe ZPV in 2007 endlich abgeschlossen und an das Amt für Personal und Organisation zur Vervollständigung weiter geleitet werden. Andere Bearbeitungsreglemente sind insbesondere bei den Krankenkassen noch immer hängig. Dies hat aber vor allem damit zu tun, dass drei der vier in Liechtenstein zugelassenen *Krankenkassen* auch in der Schweiz tätig sind, wo ebenfalls die Erstellung von Bearbeitungsreglementen notwendig ist. Eine Koordinierung erscheint in diesem Zusammenhang als wichtig und sinnvoll. Bearbeitungsreglemente sind noch von weiteren Stellen, insbesondere auch von Behörden zu erstellen, wenn die gesetzlichen Regeln dies erfordern.[69] Aus Sicht des Bürgers erscheint eine automatisierte Bearbeitung dann wichtig, wenn seine Interessen tangiert sind. Dies ist vor allem bei einer Datenbearbeitung durch Strafverfolgungsbehörden der Fall. Es steht ausser Frage, dass diese über geeignete Mittel zur Strafverfolgung verfügen müssen. Dennoch ist die Erstellung eines Bearbeitungsreglements wichtig, da es auch zur eigenen internen Dokumentation über die entsprechenden Datensammlungen im Sinn eines Kontrollinstruments dient. Bis Jahresende war ein Entwurf durch die Staatsanwaltschaft[70] in Bearbeitung.

Die datenschutzrechtlichen Fragen zur **Beschaffenheit der ZPV** stellen sich nach wie vor. An dieser Stelle sei bloss daran erinnert, dass die Verhältnismässigkeit der Datenbearbeitung, der Zugriff auf Vergangenheitsdaten, eine fehlende Lesezugriffsprotokollierung oder eine fehlende Löschmöglichkeit von Personendaten die Hauptprobleme darstellen, welche nach wie vor bestehen.[71] Im Berichtsjahr wurde immerhin ein Rechtsgutachten in Auftrag gegeben, das sich insbesondere mit diesen Problemen beschäftigen soll. Der Auftrag des Gutachtens bestand in einer Analyse des Ist-Zustands sowie allenfalls mit der Beschreibung des notwendigen Handlungsbedarfs und dem Aufzeigen von Lösungsansätzen. Das Expertengutachten lag Ende 2007 noch nicht vor, so dass im kommenden Berichtsjahr über den Weitergang berichtet werden wird.[72]

5.1.1.2. ANDERES

Die Diskussion um die **Videoüberwachung** vor allem in Vaduz nahm im Berichtsjahr ihren Fortgang bzw. wurde auf Grund einer eingegangenen Beschwerde wieder aufgenommen.[73] Im Hinblick auf eine abschliessende Beurteilung des Sachverhalts und insbesondere der Verhältnismässigkeit der Videoüberwachung, mussten zunächst die noch offen gebliebenen Fragen aus dem Jahr 2006 geklärt werden. Hierzu fand auch ein Gespräch mit dem Bürgermeister von Vaduz statt. Nach wie vor aber fehlt es für die Videoüberwachung durch Behörden nach Auffassung des DSB an einer genügend bestimmten Rechtsgrundlage.[74] Aufgrund der massiven Bedenken an der Zulässigkeit der Videoüberwachung im Städtle Vaduz und aufgrund der Tatsache, dass sich die Gemeinde Vaduz nicht an die zuvor ausgesprochene Empfehlung des DSB gehalten hat,[75] legte der DSB die Sache der Datenschutzkommission zur Entscheidung vor. Das Verfahren, welches zur Hauptsache die Verhältnismässigkeit der 16 in der Fussgängerzone installierten Kameras beurteilen soll, war Ende 2007 noch nicht entschieden.

5.1.2. GESETZLICHE GRUNDLAGEN

Am 31. Juli 2007 lief eine **Übergangsfrist**, welche im Datenschutzgesetz vorgesehen war, ab.[76] Danach dürfen seither keine Datensammlungen mit besonders schützenswerten Daten und Persönlichkeitsprofilen mehr bearbeitet werden, ohne dass die Voraussetzungen von Art. 18 und Art. 21 DSG erfüllt sind. Während bei privaten Personen verschiedene Rechtfertigungsgründe für eine Datenbearbeitung möglich sind, wie vor allem die (ausdrückliche) Einwilligung, sind Behörden in der Regel auf eine gesetzliche Grundlage für eine Datenbearbeitung angewiesen. In Liechtenstein wurde nicht ein

[69] Vgl. Art. 21 DSV.
[70] Dieser Entwurf betrifft auch das Landgericht, wobei dieses nicht als Strafverfolgungsbehörde qualifiziert werden kann.
[71] Vgl. TB 2006, 5.1.1.1.
[72] Vgl. hierzu auch oben, 4.1.
[73] Vgl. Tätigkeitsbericht 2006, 5.1.1.2. zum Sachverhalt und zu den allgemeinen Regeln der Videoüberwachung im öffentlichen Raum.
[74] In diesem Zusammenhang bestehen Überlegungen, entsprechende Gesetzesänderungen auf den Weg zu bringen, um eine genügend bestimmte gesetzliche Grundlage zu schaffen, die möglicherweise nicht nur Gemeinden zur Videoüberwachung im öffentlichen Raum berechtigt.
[75] Die Empfehlung wurde anlässlich einer offiziellen Beschwerde gegen die Videoüberwachung in Vaduz ausgesprochen.
[76] Vgl. Art. 44 Abs. 3 DSG.

Gesetzespaket geschaffen wie in der Schweiz,[77] um notwendige Grundlagen zu schaffen. Somit kann es durchaus sein, dass seit dem 01. August 2007 für die Befugnis, besonders schützenswerte Daten und/oder Persönlichkeitsprofile zu bearbeiten, ungewollt verschärfte Bedingungen gelten, wenn nicht sogar gewisse Datenbearbeitungen unzulässig wären.[78]

Dies gilt insbesondere für die **ZPV**, welche ohne Zweifel nicht nur einzelne besonders schützenswerte Daten, sondern vor allem umfassende Persönlichkeitsprofile umfasst: an dieser Stelle sei daran erinnert, dass die ZPV Identifikations- und Wohnsitz- und andere z.B. Zivilstandsdaten oder die Angabe des Arbeitgebers umfasst, welche von etlichen Behörden eingesehen werden können.[79]

Die Regierung führte auf Ende Jahr eine neue *AHV-Nummer* ein. Dies hat damit zu tun, dass die bisherige Nummer, welche auch in der Schweiz geführt wurde, in der Schweiz abgelöst wurde. Somit war auch in Liechtenstein eine neue Nummer zu definieren. Man entschied sich für die so genannte **PEID** (Personenidentifikationsnummer), eine verwaltungsinterne Kennnummer der ZPV, welche einmalig für eine Person vergeben wird und welche die meisten der mittlerweile knapp 30 Amtsstellen und die FMA verwenden. Dadurch ist eine Person leicht identifizierbar, was angesichts der oft doppelt oder mehrfach vorkommenden Namen in Liechtenstein zu einer entscheidenden Arbeitserleichterung führt. Diese Entscheidung fusst darauf, dass auch die AHV/IV/FAK-Anstalten über einen Zugriff auf die ZPV verfügen; ausserdem ist der Datenaustausch mit der Landesverwaltung rege. In Liechtenstein kam es somit zu einer *Verschmelzung der PEID mit der AHV-Nummer*. Die Tendenz geht somit eindeutig in die Richtung, dass der Bürger sich auf eine blosse Nummer reduziert. Diese Nummer verfügt – im Gegensatz etwa zur AHV-Nummer oder zur Nummer der Krankenversichertenkarte (IDN) – bis heute über keine gesetzliche Grundlage.[80] Eine Verwendung eines behördenübergreifenden, einheitlichen Personenidentifikators birgt die Gefahr von unberechtigten Verknüpfungen verschiedener Datenbanken, wodurch ein nicht unerhebliches Missbrauchspotenzial geschaffen wird. Dabei ist insbesondere zu beachten, dass die Gefährdungen sich durch den Einsatz elektronischer Kommunikations- und Informationssysteme potenzieren und Private ein Interesse haben können, den Personenidentifikator in Erfahrung zu bringen. Daraus wiederum erwächst die Gefahr eines schleichenden Verlusts der Souveränität über die eigenen Daten. Neben der Schaffung einer gesetzlichen Grundlage für eine nationale Kennnummer geht es auch darum, mit organisatorischen und technischen Vorkehren das Gefährdungspotenzial einzuschränken, so dass eine solche Nummer nur durch die notwendigen Amtsstellen, und nicht etwa auch die Privatwirtschaft, gebraucht werden darf. Der Gesetzgeber sollte festlegen, welche Stelle zu welchem Zweck den Identifikator nutzen darf oder etwa ein «Zulassungssystem» einzuführen, damit die Kontrolle über die Ausbreitung des Personenidentifikators zu gewährleisten.[81] Die komplexe Angelegenheit konnte 2007 noch nicht abgeschlossen werden und wird im kommenden Berichtsjahr sehr aufmerksam und aktiv insbesondere im Rahmen des Arbeitsgruppe ZPV weiter verfolgt werden.

5.2. ABKLÄRUNGEN UND EMPFEHLUNGEN IM PRIVATRECHTSBEREICH

Die im Berichtsjahr eingegangen Beschwerden betrafen verschiedene Sachverhalte.[82] Die meisten Beschwerden waren auf der einen Seite dem **Arbeitsbereich** und auf der anderen Seite dem Themenblock **«Unerwünschte Werbung»** zuzuordnen.

Unerwünschte Werbung kann mit normalen Briefsendungen oder per Telefon / Fax / Email erfolgen. Heutzutage erfolgt sie jedoch meistens und zu Hauf per E-Mail (sog. Spam). Diese darf in Liechtenstein nur nach vorheriger Einwilligung des Adressaten erfolgen.[83] Leider halten sich nicht alle Anbieter an diese gesetzlichen Vorgaben, der Adresshandel floriert. So nimmt es nicht Wunder, dass gerade in Bezug auf unerbetene Werbung mehrere Beschwerden eingingen:

In einer Beschwerde ging es darum, dass ein Unternehmen in Liechtenstein unerwünschte Werbung per E-Mail verschickte, ohne zuvor die erforderliche Einwilligung des Adressaten hierzu

[77] Vgl. Bundesgesetz über die Schaffung und Anpassung gesetzlicher Grundlagen für die Bearbeitung von Personendaten vom 24. März 2000.
[78] Vgl. Tätigkeitsbericht 2006, 5.1.2.
[79] Vgl. Tätigkeitsbericht 2003, 4.1.2.
[80] Vgl. dazu auch Tätigkeitsbericht 2006, 4.5
[81] Vgl. Rechtsgutachten von Giovanni Biaggini, Professor für Staats- und Verwaltungsrecht an der Universität Zürich, Ein Personenidentifikator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes (Art. 13 BV), Dezember 2002), abzurufen unter: *http://www.edoeb.admin.ch/themen/00794/01189/index.html?lang=de*.
[82] Insgesamt gingen in 2007 dreizehn Beschwerden bei der SDS ein.
[83] Art. 50 Kommunikationsgesetz (KomG); vgl. auch Tätigkeitsbericht 2006, 5.2.

anzufordern.[84] In dem Fall war es jedoch so, dass die E-Mail-Adresse des Beschwerdeführers frei über das Internet zugänglich war. Es bestanden zudem konkrete Anzeichen dafür, dass der Beschwerdeführer seine E-Mail-Adresse selbst der Allgemeinheit zugänglich gemacht hatte. Hat die betroffene Person aber ihre Daten selbst allgemein zugänglich gemacht und eine Bearbeitung derselben nicht ausdrücklich untersagt, liegt in der Regel keine Persönlichkeitsverletzung vor.[85] Aus datenschutzrechtlicher Sicht war daher diese E-Mail-Werbung grundsätzlich erst einmal nicht zu beanstanden. Etwas anderes kann jedoch nach dem Kommunikationsgesetz gelten.[86] Zur Prüfung, ob die Voraussetzungen nach dem Kommunikationsgesetz erfüllt sind, wurde diese Beschwerde daher an das Amt für Kommunikation weitergeleitet, welches die zuständige Aufsichtsbehörde im Kommunikationsgesetz darstellt.

Im selben Themenblock wurde eine Beschwerde in Bezug auf einen *Listbroker* fortgeführt und eine neue Beschwerde in Bezug auf den *Adresshandel* behandelt, wobei die unerwünschte Werbung in diesen Fällen auf dem normalen Postweg versandt worden war. Um zunächst einmal die ungeklärte Herkunft der Daten zu eruieren, wurden die Beschwerdeführer auf die generelle Möglichkeit des Auskunfts- und Löschungsrechts hingewiesen. Danach können nur sie selbst als betroffene Personen diese Rechte geltend machen.

Die vermehrten Beschwerden waren Anlass genug, um einmal grundsätzliche Informationen über den Umgang mit unerwünschter Werbung zu erarbeiten. Im Hinblick auf den Teilbereich von Spam wurde die Zusammenarbeit mit der zuständigen Aufsichtsbehörde gesucht. In Folge konnten die neuen *Richtlinien über den Umgang mit unerwünschter Werbung und insbesondere mit Spam* herausgegeben werden.[87] Ausserdem wurden aufgrund von Angaben des britischen Datenschutzbeauftragten, dem Information Commissioner (ICO), ein interner Kriterienkatalog erstellt, nach welchen ein Intervenieren sinnvoll bzw. zwingend ist.

Im sensiblen Bereich der Arbeitswelt gingen ebenfalls verschiedene Beschwerden ein. In einer Beschwerde ging es darum, dass eine Angestellte einer Firma aus dem Finanzsektor sich darüber beklagte, dass die *Mitarbeiter videoüberwacht* werden. Der Arbeitnehmer hatte Videokameras an den beiden Enden des Korridors zwischen den Büroräumen installiert. Auch wenn klar ist, dass im Finanzbereich gewisse Massnahmen zum Schutz von Finanzdaten nötig sind, ist dennoch festzustellen, dass eine Videoüberwachung am Arbeitsplatz nur unter sehr strengen Voraussetzungen zulässig ist. Vor allem sind die betroffenen Mitarbeiter vorab hierüber zu informieren, was in concreto nicht der Fall war. Auch wenn nicht der eigentliche Arbeitsplatz videoüberwacht wurde, resultiert auch eine Überwachung der Bürokorridore in einer Überwachung des Verhaltens des Arbeitnehmers, insbesondere wenn sich auf dem Gang Arbeitsgeräte wie zum Beispiel Aktenvernichter oder Kopiergerät befinden, und ist als solche nicht gestattet.[88]

Eine andere Beschwerde betraf die Sperrung einer E-Mailbox am Arbeitsplatz. Hierzu konnte ebenfalls auf die entsprechenden Richtlinien des DSB verwiesen werden.[89] Eine weitere Beschwerde wurde von einem Arbeitnehmer erhoben, welcher bei seinem früheren Arbeitgeber *Einsicht in seinen Personalakt* gewünscht hatte. Der ehemalige Arbeitgeber verweigerte ihm die Einsicht mit der Begründung, dass einem aus dem Unternehmen ausgeschiedenen Arbeitnehmer dieses Recht nicht mehr zustehe. Der DSB informierte daraufhin den Beschwerdeführer, dass das gesetzliche Auskunftsrecht keine Unterscheidung zwischen aktuellem oder ehemaligem Arbeitnehmer trifft. Das gesetzliche Auskunftsrecht ist vielmehr umfassend anwendbar, womit auch ein ehemaliger Arbeitgeber Einsicht in Personalakten geben muss.

Eine Beschwerde zur Einhaltung des *Arbeitsvermittlungsgesetzes (AVG)* und des Kommunikationsgesetzes (KomG) wurde behandelt. Anlass hierzu hatte eine Personalvermittlung gegeben, die ungefragt Bewerbungsunterlagen an potentiell interessierte Unternehmen per Fax verschickt hatte. Darin ist eine Verletzung der Persönlichkeitsrechte des betroffenen Bewerbers zu sehen. Die Personalvermittlungsagentur wurde daraufhin vom DSB zunächst auf die gesetzesmässige Handhabung von Personendaten hingewiesen. Da die Zusendung der Bewerbung per Fax von der Absenderin auch als Werbung in eigener Sache gedacht war, bestand auch ein Bezug zum

[84] Sog. Opt-in-Lösung; vgl. ausführlich hierzu oben, 3.1.
[85] Art. 16 Abs. 3 DSG.
[86] Vgl. Art. 50 KomG und oben, 3.1.
[87] Vgl. ausführlich hierzu oben, 3.1.
[88] Vgl. Richtlinien der SDS über Internet und E-Mailüberwachung am Arbeitsplatz für öffentliche Verwaltungen und Privatwirtschaft, abzurufen unter: *http://www.llv.li/richtlinie_internet_email_ueberwachung_arbeitsplatz_oktober_2005.pdf*.
[89] Vgl. Fussnote 83.

Kommunikationsgesetz. Die Arbeitsvermittlungsagentur war daher auch auf die bereits oben ausführlich dargestellten gesetzlichen Vorgaben zu Werbesendungen hinzuweisen.

Eine weitere Beschwerde betraf die *Publikation von privaten Daten* im Internet, die anlässlich der Kandidatur für die Wahl in einen Ausschuss des Europarates erfolgte. Kandidaturen zu solchen Ausschüssen werden – wie auch die Ergebnisse der Wahlen – durch den Europarat über das Internet zugänglich gemacht. Im konkreten Fall ging es allerdings um einen Ausschuss, welcher eine sehr heikle Aufgabe zu erfüllen hat, so dass die Beschwerdeführerin die Publikation von privaten Angaben (insbesondere private Adresse) als problematisch erachtete. Der DSB leitete diese Beschwerde an den Europarat weiter, welcher daraufhin eine Löschung der Daten auf dem Internet veranlasste.

Unabhängig von Swift informierte eine Bank ihre Kunden darüber, dass bei internationalen Zahlungen gewisse Personendaten an die Empfängerbank im Ausland bekannt zu geben seien. Gegen diese Bekanntgabe der Personendaten wandte sich eine Beschwerde. Die Ermittlungen ergaben dann, dass sich die Bank durch die entsprechenden Vorgaben der *EU-Verordnung 1781/2006* (Übermittlung von Angaben zum Auftraggeber bei Geldtransfers) zu der Datenbekanntgabe veranlasst sah. Problematisch ist jedoch, dass die Verordnung in 2007 noch keine Gültigkeit in Liechtenstein hatte, aber bereits in der EU anwendbar war und somit auch eine gewisse Wirkung für Liechtenstein hatte. Beim grenzüberschreitenden Zahlungsverkehr zwischen einer liechtensteinischen Bank mit einer Bank im EU-Raum war die Verordnung für die Bank im EU-Raum an die Verordnung gebunden und die Bank in Liechtenstein war es somit indirekt auch. Aus diesem Grunde wollte die liechtensteinische Bank daher ihre Kunden schon im Berichtsjahr über die Auswirkungen besagter Verordnung informieren, obwohl sie noch nicht in das liechtensteinische Recht übernommen wurde. Die Kundeninformation und Datenbekanntgabe waren daher von der Sache her grundsätzlich nicht weiter zu beanstanden.

Beim DSB gingen verschiedene Beschwerden ein, die sich gegen die Auflistung von ehrverletzenden Namen im Rahmen des zur Veröffentlichung anstehenden *Namenbuches* wandten. Schon seit längerem ist geplant, ein Buch zum Thema Übernamen herauszugeben. Schon früh war der Kontakt mit dem DSB gesucht worden, der zur notwendigen Einholung der Einwilligung der betroffenen Personen ein ähnliches Vorgehen wie bei den Familienstammbüchern empfohlen hatte.[90] Danach sollte mit einer öffentliche Auflage des Entwurfes die Öffentlichkeit auf dieses Vorhaben aufmerksam gemacht werden. Personen, welche im Entwurf erwähnt werden, nicht aber eine definitive Veröffentlichung im Buch wünschen, können dies dem Namenbuch mitteilen, so dass davon auszugehen ist, dass die Einwilligung nicht gegeben ist. In einer Kundmachung der Herausgeber war auch explizit davon die Rede, dass auf anstössige Namen im Voraus verzichtet wird. Wie sich dann aber herausstellte, war das nicht der Fall, woraufhin die eingangs erwähnten Beschwerden eingingen. Der DSB monierte daraufhin gegenüber den Herausgebern, dass offensichtlich die eigene Kundmachung nicht eingehalten wurde und forderte die Vorlage eines neuen, datenschutzkonformen Konzepts zur weiteren Vorgehensweise. Diese Angelegenheit war bis Ende des Jahres nicht abgeschlossen.

In Zusammenhang mit der gesetzlichen Neueinführung der Früherfassung im Rahmen des Invalidenversicherungsgesetzes (IVG)[91] wurde eine Meldepflicht für den Arbeitgeber der versicherten Person, die behandelnden Ärzte der versicherten Person und die Träger der sozialen Sicherheit bestimmt.[92] Ein Beschwerdeführer vertrat hierzu die Ansicht, dass diese Meldepflicht mit dem Berufsgeheimnis kollidiere und daher möglicherweise sogar zu einer Strafbarkeit führen könne. Die SDS konnte aber in Rücksprache mit der Staatsanwaltschaft abklären, dass die Ausübung einer Rechtspflicht grundsätzlich als Rechtfertigungsgrund gilt. Deshalb machen sich Ärzte, Arbeitgeber und Träger der sozialen Sicherheit nicht wegen Verletzung ihres Berufsgeheimnisses strafbar, wenn und soweit sie ihrer gesetzlichen Meldepflicht im Rahmen der Früherfassung ordnungsgemäss nachkommen.

[90] Vgl. Tätigkeitsbericht 2003, 3.1.3.
[91] Vgl. oben, 4.5.
[92] Vgl. Art. 32bis Abs. 3 IVG.

6. Register der Datensammlungen

Die liechtensteinischen Behörden sammeln und bearbeiten eine Unzahl von Daten über die liechtensteinische Bevölkerung. In einem Rechtsstaat dürfen diese Datenbearbeitungen nicht im Geheimen vor sich gehen. Jede betroffene Person hat deshalb von Gesetzes wegen das Recht, zu erfahren, welche Behörde welche Daten über sie oder ihn bearbeitet. Damit dieses Recht auf Einsicht und Auskunft in die eigenen Daten in der Praxis überhaupt ausgeübt werden kann, muss der Bevölkerung zuerst transparent aufgezeigt werden, welche Behörden welche Daten bearbeiten. Um diese Transparenz zu schaffen, müssen die Behörden[93] alle ihre Datensammlungen in einem öffentlich zugänglichen Register bekannt geben. Aufgabe des Datenschutzbeauftragten ist es, dieses **Register der Datensammlungen** zu führen und auf der Website im Internet zu veröffentlichen.[94] 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 jederzeit direkt beim Inhaber der Datensammlung auf Grund des gesetzlichen Auskunftsrechts erhalten.

Das Register ist so auch für die Behörden selber von Nutzen. Diese erhalten einen besseren Überblick über ihre Datensammlungen und über ihre Datenflüsse. Es bietet zudem die Möglichkeit, kritisch zu überprüfen, ob die vorhandenen Datensammlungen (noch) zu Recht geführt werden und inhaltlich in Ordnung sind.

Zuständig für die Führung und die Pflege des Registers ist, wie gesagt, die SDS, welche gerne bei diesbezüglichen Fragen Auskunft gibt. Die Behörden haben die Datensammlungen an sich selber zu führen, das heisst, sie sind für die inhaltliche Richtigkeit, Vollständigkeit und Aktualität der Einträge im Register selbst verantwortlich.

Zum Ende des Berichtsjahrs umfasste das Register 530 Datensammlungen, die im Internet abgerufen werden können.[95]

Das Gesetz sieht vor, dass die Datensammlungen vor ihrer Eröffnung angemeldet werden müssen, wobei Behörden sämtliche, private Personen nur bestimmte Datensammlungen anmelden müssen. Eigentlich sollten die Inhaber der Datensammlungen von sich aus die Anmeldung tätigen oder Änderungen bekannt geben. Da die Inhaber der Datensammlungen aber erfahrungsgemäss dieser Pflicht nicht immer von alleine aus nachkommen, hat der Datenschutzbeauftragte jedes Jahr an diese Pflicht erinnert. Es wird nachgefragt, ob Aktualisierungen nötig sind. Diese Praxis hat den Nachteil, dass sie sehr arbeitsaufwendig ist und auch nicht die Stellen erfasst, die zwar Datensammlungen bearbeiten, diese aber noch nicht pflichtgemäss angemeldet haben.

Aus diesem Grund stellt sich die Frage nach der Art der Fortführung des Registers. Dazu konnten mit verschiedenen Datenschutzbeauftragten Gedanken ausgetauscht werden, die ähnliche Erfahrungen gemacht haben. Es bestehen erste Überlegungen, das Führen und Pflegen des Registers für alle Beteiligten zu vereinfachen. Eine konkrete Umsetzung wird jedoch frühestens 2008 realisiert werden können.

[93] Private Personen müssen nur in wenigen, gesetzlich vorgeschriebenen Fällen ihre Datensammlungen zum Register anmelden.
[94] Vgl. Art. 15 DSG.
[95] Vgl. *http://www.llv.li/amtsstellen/llv-sds-register_der_datensammlungen.htm*.

7. Internationales

7.1. ARTIKEL-29-ARBEITSGRUPPE DER RICHTLINIE 95/46/EG

Das Gremium unabhängiger nationaler Datenschutzbehörden des EWR, die so genannte Art.-29-Arbeitsgruppe, behandelte auch 2007 Themen internationaler Relevanz, die auch für Liechtenstein Auswirkungen haben werden. In diesem Jahr wurden Dokumente[96] vor allem zu folgenden Themen verabschiedet:

In einer Stellungnahme der Art.-29-Arbeitsgruppe wird der Begriff der **«Personendaten»** definiert.[97] Festgehalten wird zum Beispiel, dass es bei Personendaten sowohl um objektive als auch subjektive Informationen in Bezug auf Personen gehen kann; dass es nicht darauf ankommt, ob die Information wahr oder unwahr ist; dass es egal ist, in welcher Form die Information vorhanden ist – von Papier, über Ton-/Bildträger bis zum Barcode im Personalausweis oder dem RFID-Chip in den neuen Reisepässen. Auch die Frage, ob Verstorbene oder ungeborene Kinder datenschutzrechtlich geschützt werden, erörtert die Stellungnahme. Personendaten sind Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Bestimmbar ist eine Person z.B. über ihre Telefon-, Auto-, AHV-Nummer oder normaler Weise IP-Adressen. Biometrische Daten und verschlüsselte Daten beziehen sich ebenso auf Personen wie Videoüberwachungssysteme, deren Zweck eben in der Identifikation von Personen besteht. Dabei spielt es keine Rolle, ob die breite Öffentlichkeit oder z.B. nur Verwandte eine Person bestimmen können. Entscheidend ist der Umstand, dass eine Person identifiziert werden kann. Schliesslich werden nach der Richtlinie nur natürliche Personen geschützt. In Liechtenstein fallen auch juristische Personen unter den Schutz des Datenschutzgesetzes.

Auf Anfrage der Europäischen Kommission hin erarbeitete die Art.-29-Arbeitsgruppe eine **Stellungnahme zu Fragen des Datenschutzes im Zusammenhang mit dem Binnenmarkt-Informationssystem (IMI)**[98]. Das IMI hat die Verbesserung der Kommunikation unter den Verwaltungen der Mitgliedstaaten zum Ziel, die oftmals aufgrund unterschiedlicher Verwaltungs- und Arbeitsstrukturen oder Sprachbarrieren erschwert ist. Das IMI ist ein elektronisches Hilfsmittel, das ein System für den Austausch von Informationen bietet, das den Mitgliedstaaten eine effizientere Zusammenarbeit in ihren laufenden Aktivitäten[99] ermöglichen soll.[100] Aufgrund der Fülle von Personendaten oder gar sensibler Daten, die in dem System bearbeitet werden, und aufgrund der hohen Komplexität des Systems ist es unabdingbar, dass das IMI vollständig im Einklang mit den geltenden Grundsätzen des Datenschutzes gestaltet wird. Daher betont die Art.-29-Datenschutzgruppe, wie wichtig es ist, dass die Erfordernisse des Datenschutzes hinsichtlich der Qualität der Daten, der Notwendigkeit und der Verhältnismässigkeit eingehalten werden. In diesem Sinne ist es vor allem nötig, die Ziele der Datenverarbeitungen klar und eindeutig festzulegen und auch die genauen Funktionen aller Nutzer im System klarzustellen. Da das IMI niemals 27 bzw. 30 verschiedenen einzelstaatlichen Rechtsystemen untergeordnet werden kann, appelliert die Art.-29-Datenschutzgruppe an die Europäische Kommission, eine entsprechend spezifische Entscheidung zu treffen, die genaue Bestimmungen enthalten sollte unter Berücksichtigung aller in der Stellungnahme aufgeworfenen Bedenken.[101] In Liechtenstein wurde im Rahmen der Umsetzung der Berufsqualifikationsrichtlinie eine erste Testphase des IMI gestartet, an dem die Stabsstelle EWR, das Gewerberegister, die FMA und das Amt für Gesundheit beteiligt sind. Zu diesem Zweck fand im Berichtsjahr auch eine Besprechung mit der Stabsstelle EWR statt, um die Einhaltung der datenschutzrechtlichen Grundsätze zu gewährleisten. Eine Umsetzung der Dienstleistungsrichtlinie ist erst zum Ende 2009 geplant.

Das Arbeitspapier zur **Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)**[102] soll als Interpretationshilfe zu den auf EPA-Systeme anwendbaren Datenschutzbestimmungen dienen sowie konkrete Hinweise zu den Anforderungen geben, die bei der Einrichtung derselben an den

[96] So genannte Working Papers (WP), chronologisch abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_de.htm*.

[97] Stellungnahme 4/2007 zum Begriff «personenbezogene Daten», WP 136, angenommen am 20. Juni, vgl. Fussnote 11.

[98] Stellungnahme 7/2007 der Art.-29-Datenschutzgruppe zu Fragen des Datenschutzes im Zusammenhang mit dem Binnenmarkt-Informationssystem (WP 140), angenommen am 21. September 2007, abzurufen unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp140_de.pdf.

[99] Insbesondere bei der Umsetzung der Richtlinie 2006/123/EG über Dienstleistungen (Dienstleistungsrichtlinie) und der Richtlinie 2005/36/EG über die Anerkennung von Berufsqualifikationen für reglementierte Berufe und Dienstleistungen.

[100] Vgl. zur Berufsqualifikationsrichtlinie oben, 4.4.

[101] Die Kommission erliess eine Entscheidung noch im Dezember des Berichtsjahres: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:013:0018:0023:EN:PDF*.

[102] Arbeitspapier der Art.-29-Datenschutzgruppe zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), WP 131, angenommen am 15. Februar 2007, abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_de.pdf*.

Datenschutz und an die Schutzmechanismen zu stellen sind. Unter dem Begriff der elektronischen Patientenakte[103] wird ein ausführliches Dokument verstanden, in dem der frühere und aktuelle körperliche und geistige Gesundheitszustand einer Person in elektronischer Form festgehalten wird, so dass diese Daten zum Zweck der ärztlichen Versorgung oder zu verwandten Zwecken umgehend abgerufen werden kann. Bisher ist es oft so, dass sich die medizinischen Unterlagen bei den unterschiedlichen Leistungserbringern befinden (jeder behandelnde Arzt hat eigene Krankenakten, ein Austausch mit weiteren behandelnden Ärzten findet nicht automatisch statt). Mit dem EPA würden *alle* verfügbaren Unterlagen über die medizinische Versorgung einer Person zentral erfasst und in einer einzigen Akte gesammelt werden. Diese zentral erfassten EPA-Daten wären dann in elektronischer Form allen medizinischen Fachkräften und Einrichtungen, die über eine Zugangsberechtigung verfügen, zugänglich. Der Vorteil dieses Systems liegt unter anderem darin, dass es die Qualität der Behandlung verbessern kann, da sich die Leistungserbringer ein besseres Bild von dem Patienten machen können. Auch der Aspekt der Reduzierung der Kosten ist nicht zu vernachlässigen. Aus Sicht des Datenschutzes ist allerdings darauf hinzuweisen, dass die zentrale Verarbeitung einer solcher Vielzahl von besonders schützenswerten Daten, die noch dazu einem sehr grossen Kreis vom Empfängern zugänglich sind, nicht bedenkenlos befürwortet werden kann. Die Einhaltung der datenschutzrechtlichen Grundsätze ist unbedingt zu gewährleisten, um die Rechte der Patienten zu schützen. Wie dies im Einzelnen in der Praxis umzusetzen ist, erläutert die Stellungnahme ausführlich, insbesondere sollten die ausdrückliche Einwilligung der Patienten eine grosse Rolle spielen sowie die Sicherheit, dass die Vertraulichkeit und der Schutz ihrer persönlichen Daten von allen medizinischen Fachkräften auch im EPA konsequent gewahrt wird.

Die erste gemeinsame und europaweite Überprüfung eines ganzen Sektors, dem des **Krankenversicherungsbereiches**, wurde im Vorjahr begonnen[104] und im Berichtsjahr abgeschlossen. In einem Bericht über die erste gemeinsame Durchsetzungsmassnahme fand eine Bewertung derselben statt und es wurden zukünftige Schritte festgelegt. Der Bereich der Krankenversicherungen war ausgewählt worden, da es sich um einen Sektor mit hochgradig harmonisierten Aktivitäten handelt, welcher einen grossen Einfluss in Bezug auf Personendaten aufweist. Neben der Bewertung der Vorgehensweise und Verbesserungsvorschlägen zu neuen Massnahmen kommt der Bericht zum Schluss, dass eine gemeinsame Durchsetzung bzw. Überprüfung eines ganzen Sektors als positiv zu beurteilen ist. Auf Einzelheiten der Ergebnisse soll an dieser Stelle nicht eingegangen werden, da ja die SDS an der Ausarbeitung dieses Berichtes nicht beteiligt war. Immerhin ist aber darauf hinzuweisen, dass hinsichtlich der Einwilligung der betroffenen Personen zur Bearbeitung ihrer Personendaten nicht immer klar ist ob die Einwilligung immer freiwillig und aufgrund ausführlicher Informationen erteilt wird.[105] Die Frage der Einwilligung betroffener Personen im Bereich der freiwilligen Zusatzversicherung ist auch in Liechtenstein unklar.[106]

In einem weiteren Dokument beschloss die Arbeitsgruppe ihre **Arbeit transparenter** zu machen und die Kommunikationspolitik zu verbessern um ihr Profil und die Akzeptanz, die Qualität und das Wissen über ihre Arbeit zu verbessern. In diesem Zusammenhang wurde unter anderem beschlossen, die Arbeit weiterhin über die Internetseite für die Öffentlichkeit leicht verfügbar zu machen.[107]

In einem Beschluss zum **ersten Europäischen Datenschutztag**[108] äusserte sich die Arbeitsgruppe sehr positiv über diese Initiative des Europarates, mit welcher das Bewusstsein der Öffentlichkeit zum Schutz ihrer Privatsphäre gestärkt werden soll. Gleichzeitig werden öffentliche wie private Stellen aufgefordert, aktiv an diesem Tag teilzunehmen um dieses Bewusstsein zu stärken.

Die Arbeitsgruppe nahm zudem erneut eine Stellungnahme zum Folgeabkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika vom Juli 2007 über die **Verarbeitung von Fluggastdatensätzen** (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security wie auch eine Stellungnahme 2/2007 zur Information von Fluggästen über die Übermittlung von PNR-Daten an amerikanische Behörden an.[109]

[103] Synonym verwendet werden auch die Begriffe der elektronischen Krankenakte, elektronische Gesundheitsakte oder Krankheitsblatt.
[104] Vgl. Tätigkeitsbericht 2006, 7.1.
[105] Vgl. Bericht 1/ 2007 über die erste gemeinsame Durchsetzungsmassnahme: Bewertung und zukünftige Schritte, angenommen am 20. Juni 2007, WP 137, Seite 16.
[106] Vgl. Dr. Philipp Mittelberger, die Einwilligung als zentrales Element des Datenschutzrechts, in: Liechtensteinische Juristenzeitung (LJZ) 4/06, Seite 136.
[107] Vgl. *http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm*.
[108] Vgl. unten, 7.3.
[109] Vgl. Tätigkeitsberichte 2006, 7.1.; 2004, 7.1. und 2003, 6.1.

Schliesslich äusserte sich die Arbeitsgruppe noch zur Frage der Gleichwertigkeit des Datenschutzes in **Jersey** und auf den **Färöern**.[110]

7.2. VEREINIGUNG DER SCHWEIZERISCHEN DATENSCHUTZBEAUFTRAGTEN

An der Frühjahrstagung der Vereinigung der Schweizerischen Datenschutzbeauftragten konnte nicht teilgenommen werden.

Anlässlich der Herbsttagung der Vereinigung der Schweizerischen Datenschutzbeauftragten fand eine Tagung zum künftigen Beitritt der Schweiz zu den Abkommen von **Schengen und Dublin** statt. An dieser Tagung wurden die Auswirkungen eines Beitrittes beleuchtet. Der Europäische Datenschutzbeauftragte (EDPS) informierte über die Bedeutung eines Beitritts im Bereich von Schengen. Das heisst insbesondere dass die Arbeit der Polizei im Zusammenhang mit dem Schengener Informationssystem (SIS) kontrolliert werden muss. Dies wird bereits durch das Schengener Durchführungsabkommen (SDÜ) vorausgesetzt, in dem fest gelegt wird, dass eine nationale Datenschutzbehörde Zugriff auf den nationalen Teil des Schengener Informationssystems hat, welcher durch die Polizeibehörden betrieben wird.[111] Der EDPS wies darauf hin, dass in der Praxis nicht nur die Arbeitsweise der Polizei im Zusammenhang mit dem SIS verstanden und analysiert werden muss, vielmehr sind auch Kontrollen durchzuführen, welche teils durch eine entsprechende internationale Arbeitsgruppe koordiniert wird. Ausserdem wurde auf den Umstand hingewiesen, dass es sich im Schengenbereich um einen dynamischen Bereich handelt, welcher sich in Ausdehnung befindet. So wurde der Schengen Acquis seit der Unterzeichnung der Verträge von Schengen und Dublin durch die Schweiz[112] durch 43 weitere Verträge erweitert. Darunter seien auch solche von Relevanz für den Datenschutz. Dementsprechend komme laufend mehr Arbeit auf die Datenschutzbeauftragten zu und es sei ihre Aufgabe, die Ressourcenfrage ständig zu prüfen.

Der Datenschutzbeauftragte informierte die Regierung über diese Tagung, hielt dabei aber fest, dass sich die durch die genannten Vertreter angesprochene Ressourcenfrage bei der SDS für Datenschutz erst dann stellt, wenn ein Beitritt Liechtensteins ansteht. In Bezug auf Liechtenstein war der Beitritt zu den Abkommen von Schengen und Dublin bis Ende des Berichtsjahres noch nicht rechtlich fixiert. Das Schweizerische Datenschutzgesetz wurde im Jahr 2006 auch im Hinblick auf einen Beitritt zum Abkommen von Schengen und Dublin revidiert. Dabei wurden die Bestimmungen zur Organisation des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) angepasst, indem seine Unabhängigkeit durch eine Ratifikation des Zusatzprotokolls des Europarates zum Datenschutzabkommen gestärkt wurde. Eine solche wäre für Liechtenstein ebenfalls angezeigt.

7.3. EUROPARAT

An der jährlich stattfindenden Sitzung des Expertenausschusses über den Datenschutz wurde über die Ergebnisse des *Ersten Europäischen Datenschutztage*s informiert. Dieser Tag hat zum Ziel, das Bewusstsein zum Datenschutz in der Bevölkerung zu erhöhen. Die Teilnehmer informierten über verschiedene Initiativen. In Liechtenstein wurde vorerst mit einer Teilnahme abgewartet. Angesichts der positiven Erfahrung wurden in Bezug auf den Datenschutztag am 28. Januar 2007 Vorbereitungen getroffen. Die Diskussion über die Aufnahme eines *Grundrechts auf Datenschutz* im System der Europäischen Menschenrechtskonvention wurde fortgesetzt und über den aktuellen Stand in Bezug auf das *Zusatzprotokoll zum Datenschutzabkommen* informiert, welches bis Jahresende von den meisten EWR-Staaten unterzeichnet oder ratifiziert wurde. Eine Unterzeichnung des Zusatzprotokolls durch Liechtenstein ist noch ausstehend.[113] Im Zusammenhang Datenschutz in Belangen von globalen Telekommunikationsnetzwerken wurde im letzten Jahr beschlossen, verschiedene Begriffe des Datenschutzabkommens genauer zu umschreiben und auszulegen. Diese Arbeit wurde fortgesetzt.

7.4. EUROPÄISCHE DATENSCHUTZKONFERENZ

An der **Frühjahrskonferenz** der Europäischen Datenschutzbehörden wurden unter anderem folgende Themen behandelt: *Elektronische Gesundheitsakten, Datenschutz: Wie weiter?, Bericht über den Case Handling Workshop und die Auswertung des jährlichen Fragebogens über die Organisation der*

[110] Stellungnahme 9/2007 der Art. 29 Datenschutzgruppe zum Umfang des Schutzes personenbezogener Daten auf den Färöern, WP 142, angenommen am 09. Oktober 2007, abzurufen unter: *http://ec.europa.eu/Justice_home/fsj/privacy/index:de.htm*, vgl. dazu auch oben, 4.3.
[111] Vgl. dazu Art. 114 SDÜ.
[112] Diese fand im Oktober 2004 statt.
[113] Vgl. Tätigkeitsbericht 2006, 7.3.

nationalen Datenschutzbehörden. In Bezug auf die *Frage des Datenschutzes in der Zukunft wurde festgestellt*, dass man sich der technologischen Herausforderung stellen müsse. Nationale Grenzen seien keine Probleme mehr. Eine rechtliche Herausforderung sei die richtige Bestimmung des Begriffs des Verantwortlichen für eine Bearbeitung. SWIFT oder der elektronische Gesundheitsakt würden zeigen, wie schwierig dieser Begriff ausgelegt werden kann. Eine politische Herausforderung stelle der Kampf gegen das Verbrechen und Terrorismus dar. Datenschutz könne nicht als ein Hindernis für die Entwicklung angesehen werden. Von französischer Seite wurde auf die Initiative von London, welche an der internationalen Konferenz im letzten November angenommen wurde, hingewiesen. Eine erste Auswertung würde für die nächste internationale Konferenz, welche im September 2007 in Montreal statt finden wird, vorgenommen werden. Die Auswertung des *jährlichen Fragebogens* über die Organisation der Datenschutzbehörden war sehr interessant, da sich hierbei sinnvolle Vergleiche der Arbeitsorganisation ergeben.

Im Rahmen der Europäischen Konferenz werden zwei mal pro Jahr so genannte *Case Handling Workshops* abgehalten. An diesen Workshops werden aktuelle Themen oder vielmehr konkrete Fälle behandelt, welche für die Datenschutzbehörden in Europa wichtig sind. Im Berichtsjahr konnte nur an einem Workshop teilgenommen werden, der in Lissabon erstmals in einer neuen Form durchgeführt wurde. An der Frühjahrskonferenz war festgestellt worden, dass das Themenspektrum bisher zu breit gefasst war. Deshalb wurde beschlossen, sich auf weniger Themen zu konzentrieren. Der Workshop in Lissabon beschäftigte sich schwerpunktmässig mit der Frage der Datenbearbeitung mit der *Prüfung der Kreditvergabe* an mögliche Kunden und insbesondere der Frage, welche Daten dabei beschafft und wie die Kreditwürdigkeit eingestuft wird. Dieses Thema wurde zwar in die Prioritätenliste für das Berichtsjahr aufgenommen;[114] da die Sitzung aber erst im November stattfand, konnten die Informationen dieses Workshops bis Jahresende nicht in Bezug auf Liechtenstein ausgewertet werden.

7.5. INTERNATIONALE DATENSCHUTZKONFERENZ

An der Internationalen Datenschutzkonferenz konnte im Berichtsjahr nicht teilgenommen werden.

[114] Vgl. oben, 2.

8. Personelles und Organisatorisches

Im Berichtsjahr wurde eine juristische Teilzeitkraft befristet angestellt. Weiters bewilligte der Landtag den Ausbau der Sekretariatsstelle von 50 auf 80 %. Und schliesslich konnte eine ständige 0.2-Stelle im Informatikbereich geschaffen werden. Diese Massnahmen bewirkten eine merkliche Verbesserung der Personalsituation.

9. Ausblick

ABSCHLUSS PENDENZEN 2007

- Allgemeine Informationen für die Datenbearbeitung durch private Personen
- Informationen zur Sicherheit von mobilen Datenträgern
- Information zur Datenbearbeitung auf dem Internet
- Bearbeitung von Daten bei Kreditauskunfteien[115]
- Vorlage für eine Geheimhaltungserklärung
- Richtlinien zur Bearbeitung von medizinischen Daten
- Kommentar zu den Bestimmungen der DSV
- Arbeiten in Bezug auf die ZPV
- Vorbereitung eines Beitritts zu Schengen / Dublin
- Bearbeitungsreglemente

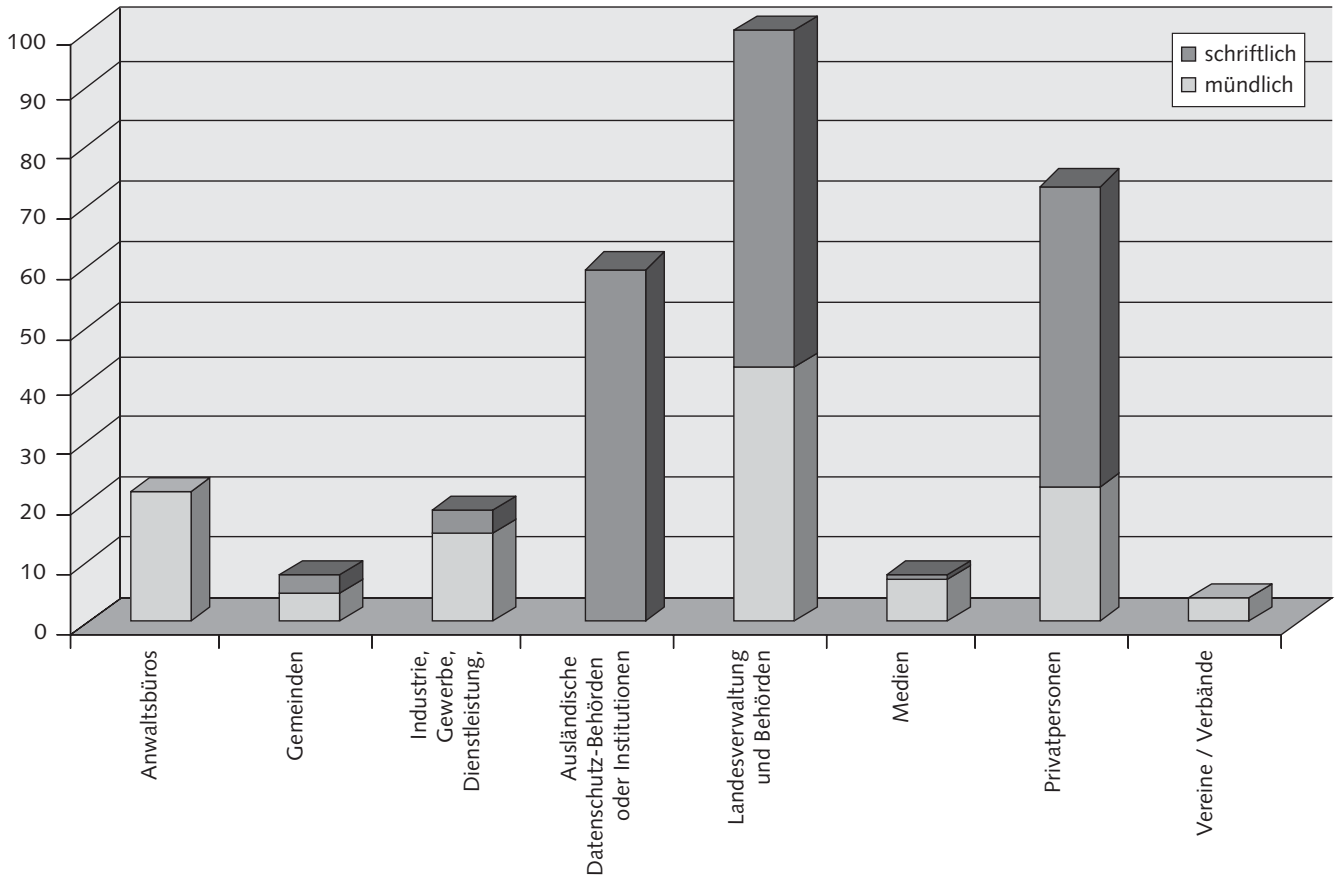
NEUE AUFGABEN FÜR 2008

Angesichts der Menge von Tätigkeiten, welche im Berichtsjahr nicht abgeschlossen werden konnten, empfiehlt es sich, nur wenige Prioritäten für 2008 festzulegen. Eine dieser Prioritäten besteht in der *erstmaligen Durchführung des Europäischen Datenschutztages* in Liechtenstein.

[115] Vgl. oben, 7.4.

Anhang

ANFRAGEART



GESETZESTHEMEN

	Anwalts-büros	Gemein-den	Industrie, Gewerbe, Dienst-leistung	Ausländische Datenschutz-behörden oder Institutionen	Landes-verwaltung und Behörden	Medien	Privat-personen	Vereine / Verbände	Gesamt-ergebnis
Anmeldung, Datensammlungen	3		2		1				6
Auskunftsrecht		1			11		9		21
Datenbekanntgabe	4	7	8		52		32	2	105
Datenschutz allgemein	9	2	5	60	36	7	26	1	146
Gesetzesvorlagen					27		1		28
Sicherheit			3		2		6	1	12
Übermittlungen ins Ausland	8		5		1	1	2		17
Überwachung am Arbeitsplatz			1				2		3
TOTAL	**24**	**10**	**24**	**60**	**130**	**8**	**78**	**4**	**338**

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