Tätigkeitsbericht

Datenschutzbeauftragter des Fürstentums Liechtenstein

2005

Inhaltsverzeichnis

1. Vorwort

Der 3. 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.

Der Begriff «Datenschutz» ist unglücklich, da er nicht den Bezug zu einer Person, um die es schlussendlich geht, erfasst. Es geht vielmehr um den Schutz der Privatsphäre. Es geht somit um ein Recht, das durch die Verfassung geschützt wird. Im Rahmen der Gesetze soll jede Person selbst bestimmen können, wer was wann über die eigene Person weiss. Das oft gehörte Argument «ich habe nichts zu verbergen» zeigt von einem ungenügenden Kenntnisstand in Bezug auf Bearbeitungen, welche heute oft im Hintergrund stattfinden. So ist vielen Leuten nicht bewusst, dass sie bei einer Benutzung des Handys, des Internets oder einer Kundenkarte elektronische Spuren hinterlassen, die auf die eine oder andere Art ausgewertet werden. Die auch in Liechtenstein zunehmende Videoüberwachung, neue Technologien wie Ortungstechniken oder die RFID-Technologie verbessern die Möglichkeiten der Verknüpfung von Daten und von kommerziellen Auswertungen im Sinn des so genannten «Data Mining». Zum Schutze der Privatsphäre wird oft von Datenschutzvertretern gefordert, solche neue Technologien datenschutzfreundlich zu gestalten (siehe dazu unten 7.1.).

Der Schwerpunkt des vergangenen Jahres war die Information der Öffentlichkeit zu verschiedenen Themen: Neben den Richtlinien zur Internet- und Emailüberwachung des Arbeitnehmers, welche übrigens ihren Ursprung in einer Medienanfrage haben, wurde z.B. ein Dokument über die Rechte des Datenschutzgesetzes erstellt. Auf der Internetseite wurde zudem u. a. zu den Themen Biometrie, Personalakten, RFID-Funkchips oder Spam-Mails informiert (siehe dazu unten, 3.1.). Anfragen an die Stabsstelle für Datenschutz (SDS) nahmen weiterhin zu und dies qualitativ und quantitativ. Tarmed ist nur ein Bereich in diesem Zusammenhang (siehe dazu unten, 4.1.). Stellungnahmen zu Vorlagen und Erlassen erfolgten u. a. zur Revision des Heimatschriftengesetzes und der Schaffung einer Staatsschutzverordnung (siehe dazu unten, 4.4.). Im Aufsichtsbereich wurde neben einer Beschwerde zu Spam-Mails beispielsweise vor den Landtagswahlen den Gemeinden in Übereinstimmung mit dem Ressort Inneres mitgeteilt, dass eine Übermittlung des Stimmregisters an politische Parteien zu wahlpolitischen Zwecken gesetzlich nicht erlaubt ist (siehe dazu unten, 5.1.). Ausserdem wurde das Register der Datensammlungen auf der Internetseite der Stabsstelle für Datenschutz (www.sds.llv.li) aufgeschaltet (siehe dazu unten, 6.). Im internationalen Bereich ist u. a. eine Stellungnahme zu biometrischen Daten in Pässen, zur Nutzung von Standortdaten zur Ortung von Personen, zur RFID-Technologie oder künftigen Pflicht zur Vorratsspeicherung von Telekommunikationsdaten im europäischen Bereich oder eine Erklärung zum Datenschutz im Gesundheits- und Sozialversicherungsbereich des Vereins der Schweizerischen Datenschutzbeauftragten zu nennen (siehe dazu unten, 7.).

Die Wichtigkeit des Schutzes der Privatsphäre wird zum Beispiel durch den Skandal um die Telefonüberwachung in den USA vor einigen Wochen verdeutlicht. Weiters ist zu erwähnen, dass mittlerweile das so genannte «Phishing»[1] sich nicht nur auf Emails, sondern nun auch anscheinend auf das Telefon erstreckt. Ausserdem entstand allein in den USA im Jahr 2004 ein Schaden von 6.4 Milliarden Dollar durch Identitätsdiebstahl, wobei ca. 50 % Kreditkarten betrafen. Zur Sicherheit von Computersystemen ist weiters zu nennen, dass kürzlich ein Pentagon-Computer gehackt wurde und Daten von über 14 000 Mitarbeitern und Armeeangehörigen gestohlen wurden. Diese Beispiele zeigen, dass es sich beim Schutz der Privatsphäre nicht um einen Papiertiger handeln darf. Vielmehr sind wichtige, auch geldwerte, Interessen im Spiel. Auch die Diskussion um die Einführung von Tarmed Anfang dieses Jahres hat gezeigt, dass der Schutz der Privatsphäre ernst genommen werden muss.

Der Kampf gegen den Terrorismus hat mittlerweile auch Liechtenstein erreicht. Die nun in Kraft getretene Staatsschutzverordnung ist ein Mittel in diesem Kampf. In der Schweiz ist gemäss jüngerer Presseberichte u. a. eine ausführliche Internetüberwachung geplant. Zudem sind in der Schweiz verstärkte Mittel zur Stärkung des Staatsschutzes geplant, welche massiv in die Privatsphäre der Betroffenen eingreifen, wie die Beobachtung von privaten Räumen ausserhalb jeglichen Strafverfahrens. Auch in Liechtenstein werden in Zukunft auf Grund der EWR-Mitgliedschaft verschiedene Kommunikationsdaten zu speichern sein, welche im Kampf gegen den Terrorismus eingesetzt werden sollen. Von verschiedener Seite wird in Europa

[1] Unter «Phishing» versteht man Versuche durch unberechtigte Personen, per Email an persönliche Daten wie Kreditkartennummern und ähnliches zu kommen. Phishing ist somit eine Arte des Identitätsdiebstahls.

ein Paradigmenwechsel festgestellt, in dem die Sammlung von Personendaten auf Vorrat zur Norm wird. Dadurch wird nicht mehr gezielt nach Verdächtigten gesucht, sondern es werden global und pauschal grosse Personengruppen erfasst. Das kürzlich ergangene Urteil des Bundesverfassungsgericht in Deutschland zur so genannten «Rasterfandung» zeigt, dass dies der falsche Ansatz ist. Dies wird bei der schon länger hängigen Revision des Polizeigesetzes dementsprechend zu berücksichtigen sein. Die Zuschauerausschreitungen bei einem Fussballspiel in Basel haben den Ruf nach einer Hooligan-datenbank verstärkt. Dieser berechtigte Ruf sollte aber nicht zu dem in der Schweiz gefundenem Ergebnis führen, wo es u. a. keine festgelegten Kriterien für die Erfassung einer Person in der Datenbank gibt und wo allein die Glaubhaftmachung von bestimmten Tätigkeiten ausreicht, um in diese Datenbank auf-genommen zu werden. Dies wird ein wichtiger Punkt bei der Frage eines möglichen Anschlusses Liechtensteins sein.

Die oben genannte Bespiele dürfen in Liechtenstein nicht zur Wirklichkeit werden. Richtig verstandener Datenschutz bewirkt einen Wettbewerbsvorteil in der Privatwirtschaft. Ein Mittel dazu ist eine Zertifizierung nach «Good Privacy», welche letztes Jahr durch die Liechtensteinischen Kraftwerke (LKW) als erstem Unternehmen in Liechtenstein vorgenommen wurde. Es ist zu hoffen, dass weitere Unternehmen diesem Beispiel fol-gen, damit der Schutz der Privatsphäre genügend beachtet wird.

Vaduz, im Juni 2006

Dr. Philipp Mittelberger
Datenschutzbeauftragter

2. Allgemeines und Prioritäten

Im letzten Tätigkeitsbericht wurden folgende Prioritäten für 2005 festgelegt:

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

Dazu waren noch verschiedene Pendenzen aus dem Vorjahr zu erledigen:

- Abschluss des Aufbaus und Veröffentlichung des Registers der Datensammlungen;
- Überprüfung der ZPV auf Datenschutzkonformität;
- Erstellung einer Broschüre «Datenschutz in der Schule».[2]

Das dritte vollständige Berichtsjahr stand im Zeichen der **Schaffung von Informationsmaterial** zum Datenschutz. Leider konnten aus Personalmangel nicht alle Informationsbroschüren, welche geplant waren, abgeschlossen werden. Insbesondere allgemeine Informationen für erlaubte Bearbeitungen durch Behörden und Private konnten nicht abgeschlossen werden. Dies wird 2006 nachzuholen sein.[3]

Weiters zu erwähnen ist, dass die vorbereitenden Arbeiten an einer Krankenversichertenkartenverordnung letztes Jahr noch nicht abgeschlossen waren. Dies konnte jedoch im Berichtsjahr bewerkstelligt werden.[4] Auch das Antragsverfahren in Bezug auf Datenfelder der Zentralen Personenverwaltung (ZPV) der Landesverwaltung konnte abgeschlossen werden.[5] Dagegen war die Schaffung eines Bearbeitungsreglements für die ZPV bei Jahresende noch in Arbeit. Das Register der Datensammlungen wurde bis zum Jahresende auf die Internetseite der SDS aufgeschaltet.[6]

Auch die Umsetzung von Zugriffsberechtigungen im Rahmen der ZPV konnte nicht abschliessend geprüft werden. Dies hat auch damit zu tun, dass in diesem sehr informatikbezogenen Bereich der SDS kein Informatiker zur Verfügung stand, welcher diese Aufgabe hätte wahrnehmen können.[7]

[2] Dies wurde nicht weiter verfolgt, da das Schulamt kein dementsprechendes Interesse gemeldet hat.
[3] Mehr dazu unten, 3.1.
[4] Siehe unten, 4.5.
[5] Vgl. unten, 5.1.1.1.
[6] Vgl. unten, 6.
[7] Erst im Oktober des Berichtsjahrs wurden die grössten Lücken dank einer bis Jahresende angestellten Aushilfe geschlossen.

3. Information

3.1. INFORMATIONSPFLICHTEN DES DSB

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

Die Schaffung von Informationsmaterial war wie angedeutet einer der Arbeitsschwerpunkte. Neben dem Tätigkeitsbericht über Aktivitäten im Vorjahr[8] erstellte die SDS gestützt auf entsprechende Dokumente des Eidgenössischen Datenschutzbeauftragten (EDSB) Richtlinien zum Thema **«Internet- und Emailüberwachung des Arbeitsnehmers am Arbeitsplatz»** und zum Thema **«Rechte nach dem Datenschutzgesetz»** und zur Ergänzung dazu **Musterschreiben** für die Inanspruchnahme von gesetzlichen Rechten. Richtlinien über die Bearbeitung von Personendaten bei Behörden und bei privaten Personen konnten wie beschrieben nicht abgeschlossen werden.

Neben diesen eher allgemeinen Informationen informierte die SDS auf der **Internetseite** über aktuelle und/oder wichtige Themen. Diese betrafen folgende Themenbereiche: Der *Datentransfer europäischer Fluggesellschaften von Flugpassagierdaten an die Zollbehörden der USA* ist aus datenschutzrechtlicher Sicht kritisch. Mögliche Flugpassagiere in die USA müssen über diesen Transfer informiert werden.[9] Der datenschutzgerechte Umgang mit *Personalakten* ist sehr wichtig, da Personalakten sehr detailliert sind und oft heikle Daten enthalten. Zu diesem Thema wurde auf einen Leitfaden des EDSB verwiesen. Eine Präsentation zu *Grundsätze und Anwendung des Datenschutzes bei Forschung, Medien und Internet* wurde aufgeschaltet sowie eine Präsentation zu einer *Schulung*, welche innerhalb der Landesverwaltung durchgeführt wurde. Eine aktualisierte *Liste* derjenigen Länder, welche einen zu Liechtenstein *gleichwertigen Datenschutz* aufweisen, wurde veröffentlicht.[10] Weiters wurde über die Verwendung *biometrischer Daten* für Identifikationszwecke und mittels zehn Fragen und Antworten zum Thema informiert.[11] *RFID-Funkchips* gelten bereits heute als revolutionär, werfen aber auch datenschutzrechtliche Fragen auf.[12] Ein Datenschutzwegweiser zum Thema *«Surfen am Arbeitsplatz»* des Deutschen Bundesbeauftragten für Datenschutz wurde ebenso veröffentlicht wie Richtlinien zum Thema «Internet und Email-Überwachung des Arbeitnehmers am Arbeitsplatz». Informationen zu *Rechten*, welche betroffenen Personen nach dem Datenschutzgesetz zukommen, wurden erstellt und für die Öffentlichkeit verfügbar gemacht. Ausserdem wurde eine *Online-Umfrage zu technischen Entwicklungen* um den Datenschutz der Wochenzeitung «Die Zeit» verlinkt. Weiters wurde auch auf die *neue Datenschutzverordnung* hingewiesen.[13] *Spam-Mails* sind bekanntlich inzwischen zu einer Plage geworden. Die Eidgenössische Datenschutzkommission hat dazu eine interessante Entscheidung erlassen, welche die Zustellung von unverlangter Email-Werbung an Unbekannte und wahllos zusammen gestellte Adressen betrifft.

Die Bemühungen der SDS, die Öffentlichkeit über wichtige und aktuelle Themen zu informieren, wurden auch international wahrgenommen. So fragten die Betreiber des **Virtuellen Datenschutzbüros**,[14] ein Verbund nationaler Datenschutzbehörden, die SDS um eine **Projektpartnerschaft** an. Somit werden Informationen, welche die SDS auf der Internetseite veröffentlicht auch teils auf dieser sehr informativen Internetseite publiziert. Diese bietet unter anderem Informationen über Literatur, Schulungen, Veranstaltungen sowie ein sehr detailliertes Schlagwortsystem zu 53 rechtlichen und 18 technischen Hauptthemen an. Davon seien hier bloss die Schlagwörter «Banken», «Biometrie», «Gesundheitswesen», «Internet», «Polizei», «Schulen», «Versicherungen», «Werbewirtschaft», «Datenbanken und Informationssysteme» oder «Technikentwicklung» genannt. Auch wenn diese Informationen sich fast ausnahmslos auf das Ausland beziehen, kann doch festgestellt werden, dass es sich hierbei um eine Fundgrube zu datenschutzrelevanten Themen handelt, die zumeist an den Rechtsrahmen des EWR gebunden, und damit auch für Liechtenstein sehr informativ sind.

Die **Medien** zeigten sich im Vergleich zum Vorjahr vermehrt[15] interessiert an datenschutzrelevanten Themen. Dabei ging es um folgende Bereiche: Die ab Anfang 2006 neu einzuführende

[8] *http://www.llv.li/pdf-llv-sds-taetigkeitsbericht_2004.*
[9] Vgl. Tätigkeitsbericht 2003, 6.1 und Tätigkeitsbericht 2004, 3.2 und 7.1.
[10] Vgl. unten, 4.3.
[11] Vgl. unten, 4.4. und 7.1.
[12] Vgl. unten, 7.1.
[13] Vgl. unten, 4.4.
[14] *http://www.datenschutz.de/.*
[15] Vgl. dazu unten, 4.1.

Krankenversichertenkarte weckte ein Medieninteresse, da diese an die ganze Bevölkerung auszuliefern war und damit administrative Vereinfachungen einhergehen sollten.[16] Auch die sich abzeichnende Einführung der *biometrischen Pässe* war ein wichtiges Thema, da ebenfalls weite Teile der Bevölkerung davon betroffen sind. Die Aufnahme von Beitrittsverhandlungen in Liechtenstein zu den Abkommen von *Schengen/Dublin* nach der positiven Volksabstimmung in der Schweiz führte zu weiteren Anfragen, da gerade bei einem Beitritt zu «Schengen» Liechtenstein an das Schengen Informationssystem (SIS) angebunden würde. Mit der möglichen *Überwachung des Arbeitnehmers am Arbeitsplatz* wurde ein weiteres Thema aufgegriffen, das für sehr viele Personen relevant sein kann. Schliesslich gab es verschiedene Anfragen anlässlich der Präsentation des *Tätigkeitsberichts 2004*.

Übrigens werden fortlaufend Presseartikel zu datenschutzrelevanten Themen in einer eigenen Rubrik auf der Internetseite der SDS aufgeschaltet.[17]

Wie angedeutet wurden vereinzelt **Vorträge** gehalten. Thematisiert wurden *«die Grundsätze des Datenschutzes, aktuelle Themen und internationale Themen mit Einfluss auf Liechtenstein»* und die *«Grundsätze des Datenschutzes und dessen Auswirkungen auf Wissenschaft, Forschung, die Medien und Internet»*. Schliesslich wurde eine landesverwaltungsinterne Schulung zum Thema *«Datenschutz – wirklich etwas Neues in Liechtenstein?»*[18] und eine öffentliche Informationsveranstaltung bei der Erwachsenenbildung zum Thema *«Big Brother» in Liechtenstein – wer hat Einblick in Ihre Daten?»* durchgeführt.

3.2. INFORMATIONSPFLICHTEN VON DATENINHABERN

Ein Grundpfeiler des Datenschutzes besteht darin, dass die betroffene Person darüber Kenntnis hat, wer was wann über sie weiss (Recht auf informationelle Selbstbestimmung). Dies bedeutet, dass die Daten bearbeitende Person oder Behörde die betroffene Person über den Sinn und den Zweck der stattfindenden Datenbearbeitung vorgängig zu informieren hat.[19]

In diesem Sinn kann das folgende praktische Beispiel erwähnt werden: Bei **Stipendienanträgen** ist es üblich, dass die Stipendienstelle bei den Gemeinden und der Steuerverwaltung die Einkommensverhältnisse der Eltern eines Antragsstellers überprüft. Grundsätzlich hat die Datenbeschaffung bei der betroffenen Person selbst zu erfolgen, damit diese soweit wie möglich selbst über ihre Daten verfügen kann. Ist dies nicht der Fall, muss sie wenigstens darüber informiert werden, dass Daten bei einer anderen Person oder Behörde beschafft werden. Zwar wurde mit der letzten Revision des Stipendiengesetzes die Möglichkeit geschaffen, dass diese Daten bei den Gemeinden und der Steuerverwaltung beschafft werden können,[20] doch wurden die Betroffenen über diesen Umstand nicht genügend informiert. Auf Grund einer Beschwerde machte der DSB die Stipendienstelle darauf aufmerksam, dass die Betroffenen auf diese Datenbeschaffung bei einer Drittstelle hinzuweisen sind. Dies sollte mindestens im Rahmen der Information zu Stipendienanträgen auf der Internetseite des Schulamtes und auf einem Beiblatt geschehen, das jedem Stipendienantrag beizulegen ist.[21] Den Datenschutzanforderungen wurde bis Ende 2005 (noch) nicht nachgekommen.

Ähnlich verhält es sich bei der **Videoüberwachung des Vaduzer Saals**, wo je nach stattfindender Veranstaltung eine Überwachung durchgeführt wird. Die Betroffenen sind über eine stattfindende Datenbearbeitung durch eine Hinweistafel aufmerksam zu machen.[22]

Die **Ortung von Personen** mittels GPS oder mit Mobiltelefonen ist ein Thema, das zunehmend an Bedeutung gewinnt. Bezweckt wird z.B., dass das eigene Kind oder auch ein Arbeitnehmer, der für das Unternehmen unterwegs ist, geortet werden kann. Die betroffenen Personen sind im Voraus über eine solche Datenbearbeitung zu informieren. Sonst fände eine heimliche Überwachung statt, welche illegal ist. Ähnlich ist die Situation beim Einsatz von so genannten **RFID-Chips** in der Privatwirtschaft. Auch solche Chips können eine Ortung von Personen ermöglichen, wenn sie z.B. in einem Geschäft in Kleidung integriert werden, der Chip beim Kauf des Produktes aber nicht deaktiviert wird. Dasselbe gilt im Bereich des **Geistigen Eigentums**, wenn z.B. Musikstücke aus dem Internet auf den

[16] Vgl. unten, 4.5.
[17] *http://www.llv.li/amtsstellen/llv-sds-spezialthemen-presseartikel_und_interviews-2.htm.*
[18] *http://www.llv.li/pdf-llv-sds-llv_schulung.pdf.*
[19] Vgl. Art. 5 DSG und Tätigkeitsbericht 2004, 3.2.
[20] Vgl. Art. 32 Abs. 2 des Stipendiengesetzes.
[21] Vgl. auch unten, 5.1.2.
[22] Vgl. unten, 5.1.2. und Tätigkeitsbericht 2003, 4.2. zu einer Videoüberwachung in einem Nachtclub.

eigenen Computer geholt werden. In diesem Fall sind oft Personendaten anzugeben. Die für den Inhalt der Internetseite verantwortliche Stelle hat dabei im Voraus über den Umfang der Datenbearbeitung zu informieren. Zu diesen Themen äusserte sich die so genannte Art. 29 Arbeitsgruppe.[23]

Schliesslich fällt nach wie vor auf, dass **Internetseiten** in Liechtenstein oft keinen **Datenschutzhinweis** enthalten. Im Sinne einer vorgängigen Information muss die Datenbearbeitung in einer separaten Rubrik auf der Internetseite (oft «Disclaimer», «Privacy Policy», «Rechtshinweis» oder «Datenschutzhinweis» genannt) klar definiert werden. In der Praxis wird dies nicht immer so gehandhabt. Die betroffenen Personen sind über die Identität des Inhabers zu informieren sowie über die Daten, welche bei einem Besuch der gegebenen Internetseite bearbeitet werden.[24] Dieses Erfordernis ergibt sich daraus, dass bei der Übertragung von Informationen im Internet automatisch eine bestimmte Menge von Informationen über den Benutzer bearbeitet werden. Diese automatisch gespeicherten Daten[25] und andere Informationen[26] dienen einem bestimmten Zweck. So werden Angaben auf der *Internetseite der Landesverwaltung* zur Beantwortung von Anfragen, zur Verbesserung der Webseite oder für die Kommunikation mit dem Benutzer gebraucht, wobei sämtliche automatisch erfassten Informationen ausschliesslich zu verwaltungsinternen Zwecken ausgewertet werden. Anderseits werden Daten auf einer *kommerziellen Seite* zudem z.B. für die Wiedererkennung eines Benutzers eingesetzt. Diese Informationen ermöglichen die Abwicklung von Bestellungen (inklusive Zahlungen), die Lieferung von Waren und das Erbringen von Dienstleistungen. Weitere Bearbeitungszwecke beziehen sich auf Marketingangebote, Kundenrezensionen und Produkte, welche auf Grund früherer Besuche der Internetseite für den Benutzer interessant erscheinen.[27]

[23] Vgl. unten, 7.1.

[24] Vgl. als positives Beispiel: *http://www.hilti.com/holcom/base/base_privacy.jsp* und Tätigkeitsbericht 2004, 3.2. und 7.1.

[25] Z.B. Rechner- bzw. IP-Adresse, angefordertes Formular, Zeit und Datum des Zugriffs auf die Internetseite.

[26] Z.B. Formulardaten, welche auf einer Internetseite aktiv angegeben werden müssen.

[27] Somit ist es möglich das Einkaufsverhalten individuell zu erfassen. Grundsätzlich können aus den riesigen angesammelten Datenmengen personifizierte Inhalts-, Struktur- und Verhaltensmuster extrahiert werden. Z.B. wird bei einem bekannten Online-Shop nebst den selbst angegebenen Informationen und Informationen aus anderen Quellen Folgendes automatisch erfasst: Rechner-Adresse, Empfangs- und Lesebestätigungen von E-Mails, Logins, Email-Adresse, Passwörter, Informationen über Computer und Verbindung zum Internet (Browsertyp und -version), Betriebssystem, Bestellhistorie, Clickstream (Reihenfolge der Seiten die aufgesucht werden), Datum und Zeit, angeschaute und gesuchte Produkte, History bei Auktionen, Telefonnummer, Dauer des Besuches.

4. Beratung

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

Die Anzahl der Anfragen gemäss der **Anfragenstatistik**,[28] die im Berichtsjahr an die STS gerichtet wurden, nahmen weiter zahlenmässig zu. Es wurde insgesamt ein starker Anstieg gegenüber dem Vorjahr verzeichnet. Auffällig ist eine Zunahme von Anfragen der *Medien* (444 %) und vor allem von *privaten Personen* (842 %). Vor allem der beachtliche Anstieg der Anfragen von privaten Personen ist bemerkenswert und als Zeichen eines wachsenden Bewusstseins für den Schutz der Privatsphäre zu bewerten. Diese Tendenz eines steigenden Bewusstseins wird auch durch die zunehmenden Besuche der *Internetseite* bestätigt,[29] die sich gegenüber dem Vorjahr mehr als verdoppelt haben.

Neben der steigenden **Quantität** von Anfragen ist auch eine **zunehmende** Qualität oder **Komplexität** zu verzeichnen.[30]

Eine Darstellung sämtlicher Anfragen sowie der Antworten würde den Rahmen dieses Berichtes sprengen. Erwähnt sei an dieser Stelle immerhin das **breite Spektrum** derselben: Neben allgemein bedeutenden Anfragen wie z.B. zu Massnahmen gegen Werbung,[31] der internen und externen Bekanntgabe von Vereinsmitgliedern oder dem Rechtsrahmen zur Videoüberwachung wurden auch weitere Anfragen gestellt.[32]

Im Zusammenhang mit der Einführung von **Tarmed** wurde das Problem der systematischen *Diagnosebekanntgabe* an die Kassen, das in der Schweiz immer wieder thematisiert wird, behandelt. Dabei konnte erreicht werden, dass die Detailliertheit der Diagnosebekanntgabe im Vergleich zum bestehenden FL-Tarif sogar reduziert wurde. Gültig ist nunmehr der so genannte «Tessiner Code», der blosse Rahmendiagnosen enthält.[33] Dazu sieht dieser Code auch vor, dass für bestimmte sensible Bereiche wie psychiatrische Erkrankungen oder Behandlungen der Geschlechtsorgane ein Vermerk angebracht werden kann, wonach die Rahmendiagnose nicht an die Krankenkasse selbst, sondern an den Vertrauensarzt bekannt gegeben wird. Ausserdem wurde von Seite der Ärztekammer auch das so genannte *«Profiling»* problematisiert. Es wurde argumentiert, dass die Kassen mit der automatischen Datenverarbeitung, welche mit Tarmed unumgänglich wird, einfacher und schneller Profile über ihre Versicherten erstellen könnten. Dazu ist zu bemerken, dass die elektronische Datenbearbeitung bereits heute – und dies unabhängig von Tarmed – Realität ist. Eine gewisse Verschärfung ist jedoch mit der Einführung von Tarmed möglich, z.B. mit den über 4 500 *Tarifpositionen*, welche der Tarmed vorsieht. Zudem wird aus Ärztekreisen wiederholt vorgebracht, dass die Krankenkassen die Daten nicht rechtskonform bearbeiten würden; so würden Daten, zu welchen die Kassen aus der obligatorischen Versicherung kämen, für den freiwilligen Versicherungsbereich zum Nachteil des Patienten missbraucht, indem z.B. ein Vorbehalt angebracht werde.[34] Das Hauptproblem einer solch vermischten Datenbearbeitung ist im System des *Gesetzes über die Krankenversicherung* (KVG) zu finden und ist unabhängig von Tarmed. Denn das KVG sieht vor, dass die Kassen eine solche *Doppelfunktion* wahrnehmen können. Trotz dieser Möglichkeit stellt sich die Frage, ob eine solche Datenbearbeitung dem Zweckgebundenheitsgebot des DSG entspricht. Um diese Frage zu beantworten wäre eine Analyse der Arbeitsweise der Kassen nötig. Schliesslich haben nach der DSV die Kassen, welche automatisiert Daten bearbeiten, ein *Bearbeitungsreglement* zu erstellen. Ein solches wurde im Sommer von den Kassen angefordert. Eine Antwort der Kassen ging jedoch bis Jahresende bei der SDS nicht ein. Diese komplexen Fragestellungen konnten bis Jahresende nicht abgeschlossen werden, doch bestand ein intensiver Kontakt mit den Kassen, dem Kassenverband, der Ärztekammer und dem Ressort Gesundheit. Es ist abschliessend zu betonen, dass sich im Rahmen von Tarmed Fragen stellen, die sich auch in den letzten Jahren gestellt hatten und nicht gelöst wurden. Nach Ansicht des DSB sollten diese allgemeinen Fragen im Interesse aller Betroffenen und vor allem der Patienten gelöst werden. Ansätze dazu, vor allem legislativer Art, sind in einem

[28] Vgl. Anhang.
An der Statistik ist auch die hohe Zahl an internationalen Anfragen auffällig. Diese kann damit erklärt werden, dass für die (einmalige) Akkreditierung zur Europäischen und zur Internationale Datenschutzkonferenz jeweils detaillierte Fragebogen auszufüllen waren. Daneben werden Fragebogen auch in anderen Gremien verwendet, damit spezifische Fragen, die sich auch in Liechtenstein stellen, international verglichen bzw. abgeklärt werden können (vgl. dazu unten, 7.).

[29] Die Anzahl von Zugriffen auf die Internetseite stieg von 16 320 (2004) auf 36 373 Zugriffe.

[30] Vgl. unten, 4.5.

[31] Vgl. Tätigkeitsbericht 2003, 3.1.2. und *http://www.llv.li/amtsstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-direktvertrieb_adresshandel.htm*

[32] Vgl. oben, 3.1. zu Anfragen der Medien und unten, 4.4. zu Gesetzesvorhaben, 4.5. zu Projekten und 5.1.1.2. zu Be-schwerden.

[33] Anwendbar ist seit Inkrafttreten der neuen Bestimmung in der Krankenversichertenverordnung (Art. 76) nicht mehr der ICD-10 Code.

[34] Nach Art. 8f. des Krankenversicherungsgesetzes (KVG) können die Kassen die Zusatzversicherung einer Person gar verweigern. Dies vor allem bei Personen, welche ungesund leben. Denn diese werden wahrscheinlich zu höheren Versicherungsleistungen Anlass geben.

Expertenbericht zu finden, der durch das Schweizerische Bundesamt für Sozialversicherungen veröffentlicht wurde.[35]

Auf Grund einer Medienanfrage[36] wurde das Thema **Internet- und Email-Überwachung des Arbeitnehmers am Arbeitsplatz** behandelt. Diese Gelegenheit wurde dazu genutzt, gestützt auf ein Dokument des EDSB *Richtlinien* für Behörden und die Privatwirtschaft zu diesem Thema zu erstellen.[37] Allgemein kann festgehalten werden, dass jeder Gebrauch von Internet und Email am Arbeitsplatz, auch zu bloss geschäftlichen Zwecken, gewisse Gefahren für das Unternehmen birgt.[38] Deshalb sollten unbedingt Schutzmassnahmen gegen den Missbrauch des Surfens und von Emails eingesetzt werden. Die Bandbreite solcher Massnahmen kann jedoch u.U. ein erhebliches Ausmass erlangen, so dass es zu zweifelhaften Massnahmen kommen kann, welche die Privatsphäre der Mitarbeiter durch ständiges Überwachen mittels Spionprogrammen und permanente namentliche Auswertung der Protokollierungen verletzt.[39] Ausserdem hat die Nutzung von Internet und Email mittlerweile ein solch bedeutendes Ausmass im privaten, aber auch im geschäftlichen Bereich erlangt, dass die private Nutzung in einem vernünftigen Ausmass auch am Arbeitsplatz sinnvoll sein kann.[40] Das Interesse des Arbeitgebers steht der privaten Nutzung von Internet und Email in dem Sinn gegenüber, als dieser berechtigterweise an der ordnungsgemässen Arbeitserledigung interessiert ist. Auf Grund des Weisungsrechts des Arbeitgebers bestimmt der Arbeitgeber über den Gebrauch von Internet und Email.[41] Es ist empfehlenswert die Nutzung von Internet und Email in einem schriftlich verfassten *Nutzungsreglement* zu regeln. Dieses (nicht obligatorische) Nutzungsreglement schafft Klarheit darüber, ob und in welchem Umfang Internet und Email auch zu privaten Zwecken erlaubt ist.[42] Die *anonyme Überwachung* ist grundsätzlich immer erlaubt. Da fast alle Protokollierungseinträge in der Regel direkt oder indirekt mit einer Person verbunden werden können, dürfen diese Einträge nur *stichprobenartig pseudonymisiert ausgewertet* werden. Jegliche Überwachung des Arbeitnehmers stellt einen Eingriff in die Privatsphäre dar. Deshalb hat der Arbeitgeber die Pflicht, ein *Überwachungsreglement* zu erstellen. Dieses enthält Informationen darüber, dass personenbezogene Auswertungen erfolgen können, falls ein Missbrauch festgestellt wird. Nur wenn ein Missbrauch durch anonyme oder pseudonymisierte Überwachung nicht verhindert werden kann, darf der Arbeitgeber personenbezogene (namentliche) Auswertungen der Protokollierungen vornehmen.[43] Die personenbezogenen Daten dürfen nur unter Einhaltung des Zweckbindungs- und Verhältnismässigkeitsprinzip von einem Sicherheitsbeauftragten ausgewertet werden.

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.[44]

4.3. BEGUTACHTUNG DER GLEICHWERTIGKEIT DES AUSLÄNDISCHEN DATENSCHUTZES

Weder im Tätigkeitsbericht 2003 noch im Tätigkeitsbericht 2004 wurde dargelegt, worin der Sinn und Zweck der Gesetzeskompetenz über die Begutachtung der Gleichwertigkeit des ausländischen Datenschutzes besteht. Dies soll an dieser Stelle nachgeholt werden: Die Datenschutzrichtlinie, welche mit dem DSG umgesetzt wurde, sieht vor, dass Personendaten nur ausnahmsweise den EWR-Raum verlassen dürfen. Dies ist

[35] Dieser Bericht trägt den Titel «Persönlichkeitsschutz in der sozialen und privaten Kranken- und Unfallversicherung» und kann beim Bundesamt für Sozialversicherungen bestellt werden.

[36] Vgl. oben, 3.1.

[37] *http://www.llv.li/leitfaden_technische_und_org_massnahmen_fl_a.pdf*

[38] Unerlaubtes und übermässiges Surfen kann z.B. den Datenverkehr beinträchtigen, die Speicherkapazität überfordern oder den gesamten Arbeitsplatz blockieren. Das Besuchen von illegalen Internetseiten kann für das Unternehmen rufschädigend und sicherheitsgefährdend sein oder sogar in manchen Fällen strafrechtliche Fragen aufwerfen.

[39] Der Gesetzesrahmen wird in den erwähnten Richtlinien dargestellt.

[40] Beispielsweise während der Mittagspause oder nach Feierabend.

[41] Wichtig ist dabei, dass der Arbeitgeber die effektiven beruflichen Bedürfnisse seiner Arbeitnehmer differenziert überprüft, bevor er ihnen den arbeitsbezogenen Internetzugriff gewährt bzw. untersagt. Durch spezifische Mitarbeiterschulungen sollen die Arbeitnehmer zusätzlich auf die Sicherheitsgefahren bei der Benutzung netzbasierter Anwendungen sensibilisiert werden.

[42] Das Nutzungsreglement sollte darüber informieren, wer für die personenbezogene Auswertung der Protokollierungen zuständig ist, welche konkreten arbeitsrechtlichen Sanktionen ergriffen werden können und wie bei Verdacht auf eine Straftat vorgegangen wird. Ratsam ist ferner die Information über die eingesetzten Protokollierungen, deren Zweck, Inhalt, Aufbewahrungsdauer und das Auskunftsrecht in Bezug auf die Protokollierung.

[43] Ein Missbrauch liegt vor, wenn das Nutzungsreglement verletzt wird. Aber auch im Falle eines Missbrauchsverdachtes kann die pseudonymisierte Auswertung der Protokollierung herangezogen werden, um einen Missbrauch zu bestätigen oder einen Verdacht zu eliminieren.

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

darin begründet, dass die EU in Sachen Datenschutz eine Vorreiterrolle weltweit einnimmt. Denn ausserhalb von Europa ist kaum ein Datenschutz gegeben, welcher mit dem nach der Datenschutzrichtlinie verglichen werden kann. Dementsprechend sieht das DSG vor, dass eine Datenbekanntgabe innerhalb des EWR in der Regel nicht problematisch ist (wohl aber u.U. dem DSB gemeldet werden muss). Was nun aber andere Länder betrifft ist es so, dass verschärfte Bedingungen für einen Datentransfer eingehalten werden müssen.

Der Unterschied zwischen dem europäischen Datenschutz und Datenschutz ausserhalb Europas soll im Folgenden am Beispiel der **USA** aufgezeigt werden, da die SDS immer wieder angefragt wird, welche Bedingungen für einen Datentransfer in die USA gelten. Deshalb soll an dieser Stelle eine grundsätzliche Aussage zum Datenschutz in der USA gemacht werden: Während der Datenschutz in Europa vielfach durch die nationale Verfassung oder nationale Datenschutzgesetze für den öffentlichen und privaten Bereich verbindlich ist, stellt sich in den USA eine andere Situation. Die Mischung zwischen nur beschränkt gültigen sektoriellen Rechtsvorschriften und freiwilliger Selbstregulierung reicht nach Meinung der Art. 29 Arbeitsgruppe[45] nicht aus, um bei jeder Übertragung personenbezogener Daten in die USA einen gleichwertigen Schutz zu gewährleisten.[46] Diese Mischung führt z.B. dazu, dass das so genannte «data mining»[47] als legitime und von der Verfassung der USA als gedeckte Wirtschaftstätigkeit angesehen wird, die den wirtschaftlichen Nutzen der Datensammlung fördere und letztlich Mehrwert schaffe.[48] Dieses «data mining» führt z.B. dazu, dass der Verkauf von Mobilfunkdaten (Anruflisten, angerufene Teilnehmer, Uhrzeit usw.) in den USA möglich und weitgehend frei handelbar ist. Solche Mobilfunkdaten werden bspw. von Scheidungsanwälten und Detektiven viel genutzt.[49] In Europa wäre dies unvorstellbar. Da die USA ein wichtiger Handelspartner von Europa sind, wurde dieser Unterschied in Bezug auf den Datenschutz mit dem **Übereinkommen zum Safe Harbour** etwas ausgeglichen. Die Grundsätze, die in diesem Abkommen festgehalten werden, beruhen auf einer Selbstverpflichtung der Unternehmen, die sich diesem Abkommen anschliessen können, um sich damit zur Verpflichtung von gewissen Datenschutzgrundsätzen verpflichten. Das Abkommen stützt sich auf sieben Grundsätze.[50]

Auf Grund einer Anfrage eines international tätigen Anwaltsbüros verfasste der DSB eine umfassende Stellungnahme zur **Datenbekanntgabe an Drittländer**. Dabei wurde festgehalten, dass ein Unternehmen z.B. die Bearbeitung der Personaldaten in ein Drittland, welches nicht über einen zu Liechtenstein gleichwertigen Datenschutz verfügt unter gewissen Umständen möglich ist: Nämlich wenn der Datenexporteur den Datenimporteur gemäss von der Europäischen Kommission genehmigten *Standardvertragsklauseln*[51] vertraglich zur Einhaltung des liechtensteinischen bzw. europäischen Datenschutzes verpflichtet. Weiters ist auch die Verwendung von verbindlichen unternehmensinternen Vorschriften (oder *Binding Corporate Rules*) denkbar, doch nur in Fällen, in denen sich Standardvertragsklauseln als besonders problematisch erweisen.[52]

Die Übermittlung persönlicher Daten bezüglich **Flugpassagierdaten** stellt sich nicht nur bei den USA,[53] sondern auch in geringerem Ausmass in Bezug auf **Kanada**. Die Europäische Kommission entschied am 19. Juli 2005, dass das Datenschutzniveau Kanadas mit dem der EG Staaten gleichwertig ist. Grundlage dieser Entscheidung ist die Stellungnahme der Art. 29 Arbeitsgruppe zu diesem Thema.[54] Diese Gleichwertigkeitsentscheidung der Europäischen Kommission wird in der Folge noch in den Anhang zur DSV aufzunehmen sein, wo die Drittstaaten aufgelistet sind, welche einen zu Liechtenstein gleichwertigen Datenschutz aufweisen.

In Bezug auf den Transfer von **Flugpassagierdaten** in die **USA** ist anzufügen, dass diesbezüglich ein Verfahren vor dem Europäischen Gerichtshof hängig ist.

[45] Vgl. 7.1.
[46] *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp15de.pdf.*
[47] Mit dem «data mining», das eine weit verbreitete Praxis darstellt, können grosse Datenmengen so analysiert werden, dass neue Informationen gewonnen werden (z.B. interessante Verhaltensmuster bei Kunden. Diese Muster können dann wiederum benutzt werden, um einzelne Kunden als beispielsweise «unsicherer Schuldner» zu klassifizieren. Dabei sind die gewonnen Ergebnisse aber nicht immer problemlos verwertbar (Philip Scholz: Datenschutz bei Data Warehousing und Data Mining, in: Handbuch Datenschutzrecht, München 2003, S. 1844f.).
[48] Axel Spies, Oliver Stutz: «Microsoft als Initialzünder für mehr Datenschutz in den USA?», Datenschutz und Datensicherheit 3/2006 (DuD), S. 170.
[49] Axel Spies, Oliver Stutz: «Microsoft als Initialzünder für mehr Datenschutz in den USA?», Datenschutz und Datensicherheit 3/2006 (DuD), S. 176.
[50] Information der Betroffenen, Einwilligungsrecht, Weitergabe, Auskunftsrecht, Sicherheit, Richtigkeit. Dazu wird vorgesehen, dass die genannten Grundsätze umgesetzt werden können. Mehr dazu auf: *http://www.llv.li/amtsstellen/llv-sds-spezialthemen-datentransfer_ins_ausland.htm.*
[51] Vgl. LGBl. 2002 Nr. 46 Anhang 4 zu Art. 1 und LGBl. 2002 Nr. 117 Anhang 6 zu Art. 1.
[52] Vgl. *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_de.pdf.*
[53] Vgl. Tätigkeitsbericht 2004, 7.1.
[54] *http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp103_de.pdf.*

4.4. STELLUNGNAHME ZU VORLAGEN UND ERLASSEN

Nach einer **Teilrevision der DSV** im Jahr 2004[55] wurde die Verordnung 2005 erneut revidiert: Dabei wurden Bestimmungen zur *Datenbekanntgabe durch Behörden auf Anfrage* und durch *offene Abrufverfahren*, das heisst Internetseiten, ergänzt: Anlässlich der Landtagsdebatten zur Einführung des DSG wurde bemerkt, dass es Behörden möglich sein soll, Vorname, Name, Geburtsdatum und Adresse einer Person oder einer Gruppe von Personen an politische oder soziale Institutionen bekannt zu geben; nicht aber z.B. an Fahrlehrer, da letztere ein kommerzielles Interesse verfolgen.[56] In der Praxis wurde die in Frage stehende Bestimmung des DSG so ausgelegt, dass die Bekanntgabe zu ideellen, nicht aber zu kommerziellen Zwecken möglich sein soll. Dazu erliess der DSB Richtlinien, welche sich an die Behörden im Allgemeinen und an die Bedürfnisse der Einwohnerkontrollen der Gemeinden richteten[57]. Diese Richtlinien wurden während des Berichtsjahres durch eine Verordnung abgelöst. Die neue Verordnungsbestimmung sieht nun vor, dass die *Datenbekanntgabe an private Personen* weiterhin zu ideellen Zwecken möglich sein soll. Bekannt gegeben werden dürfen Name, Vorname, Adresse und Geburtsdatum einer Person oder einer Gruppe von Personen, wenn ein berechtigtes Interesse glaubhaft gemacht wird. Dabei ist eine Bekanntgabe auch nach bestimmten Gesichtspunkten[58] geordnet möglich. Ergänzend sieht die neue Verordnungsbestimmung vor, dass die Behörde den Gesuchsteller bei der Datenbekanntgabe ausdrücklich darauf hinzuweisen hat, dass die Daten nicht weitergegeben und ausschliesslich für den im Gesuch angegebenen Zweck verwendet werden dürfen. Die angefragte Behörde kann bei erheblichem Aufwand eine Gebühr zu einem Stundensatz von 100 Franken erheben. Der zweite Punkt betraf die Schaffung einer rechtlichen Grundlage für Behörden, welche in der Praxis verschiedene Personendaten über ihre Internetseite in einem *offenen Abrufverfahren* bekannt gegeben hatten. Diese Praxis, die durchaus sinnvoll sein kann, sollte auf eine rechtliche Grundlage gestellt werden. Konkret geht es um die Bekanntgabe von Namen und Kontaktdaten von Mitarbeitern der Landesverwaltung oder um die Bekanntgabe etwa der Rechtsanwälte durch die Rechtsanwaltskammer, die Ärzte durch die Ärztekammer, die der Finanzmarktaufsicht (FMA) unterstellten Finanzdienstleister, der Bekanntgabe von Hotels durch Liechtenstein Tourismus, der Vereinspräsidenten in den einzelnen Gemeinden usw. Dabei wurde vorgesehen, dass gewisse weitere Daten von den betroffenen Personen bekannt gegeben werden können, wenn diese darüber informiert werden und damit einverstanden sind. Diese Zusatzbestimmung ist vor allem für den Fall der Einstellung von Fotos von Mitarbeitern einer Behörde gedacht. Solche Fotos sind zur Kontaktaufnahme nicht nötig, können aber praktisch sein. Da sie aber nicht notwendig sind, soll die Entscheidung über die Einstellung von Fotos auf eine Internetseite einer Behörde allein der betroffenen Person überlassen sein. Diese Entscheidung sollte von der betroffenen Person vor allem vor dem Hintergrund stattfinden, dass es sehr einfach ist, Fotos von einer Internetseite herunter zu laden und sie für irgendwelche Zwecke zu verwenden.

An der seit 2003 geforderten **Rechtsgrundlage zur ZPV** wurde im Berichtsjahr vor allem mit dem Feder führenden Ressort Justiz intensiv gearbeitet. Diese riesige Datenbank umfasst, wie schon früher berichtet,[59] insbesondere die ganze ständige Wohnbevölkerung, aber auch fremdenpolizeilich relevante Personen oder andere Personen, welche mit der Landesverwaltung in Verbindung treten. Vor allem auf die folgenden Aspekte wurde aus Datenschutzsicht besonderen Wert gelegt: Die einzelnen personenbezogenen Felder der so genannten Personenübersichtsmaske, auf welche etliche Amtsstellen Zugriff haben, sind abschliessend zu definieren; die Personenkennzahl, mit der jede erfasste Person eindeutig identifiziert werden kann (PEID) ist auf eine rechtliche Basis zu stellen; die Benutzung dieser Nummer durch die Amtsstellen oder eventuell durch Dritte ist zu regeln;[60] die Amtsstellen, welche auf diese Übersichtsmaske zugreifen können, sind zu umschreiben; die Rechte der betroffenen Personen sind festzuhalten; ein

[55] Vgl. dazu Tätigkeitsbericht 2004, 4.4., bzw. LGBl. 2004 Nr. 221.
[56] Vgl. Landtagsprotokoll vom 13. und 14. März 2002 zur 2. Lesung zum Datenschutzgesetz (DSG).
[57] *http://www.llv.li/amtsstellen/llv-sds-richtlinien.htm.*
[58] Geordnet nach Vorname, Name, Adresse und Geburtsdatum.
[59] Vgl. Tätigkeitsbericht 2003, 4.1.2. und Tätigkeitsbericht 2004, 5.1.1.1.
[60] In Bezug auf die PEID wurden die anderen Datenschutzbehörden in Europa angefragt, ob es im jeweiligen Land eine eindeutige Nummer gibt, welche v.a. die ganze Bevölkerung erfasst und wie die Verwendung der Nummer geregelt ist. Neben Ländern wie Deutschland, wo es eine solche Nummer nicht gibt oder der Schweiz, wo sie kürzlich vom Bundesrat beschlossen wurde, ist sie in etlichen Ländern in Gebrauch. Was die Verwendung der Nummer durch Drittpersonen angeht, war die Regelung in Irland sehr hilfreich, welche vorsieht, dass die Nummer dann verwendet werden darf, wenn es um Daten der Angestellten geht. Ausserhalb dieses Kreises ist in Irland die Verwendung der Nummer verboten. Diese Regelung ist im Gesetzesentwurf vorgesehen.

Verfahren ist festzulegen, das bestimmt, nach welchen Kriterien zusätzliche Amtsstellen Zugriff auf diese Datenbank erhalten[61] oder wie zusätzliche Datenfelder nötigenfalls geschaffen werden können. Die Arbeiten an diesem Vorhaben erwiesen sich als sehr umfassend und komplex und konnten bis Jahresende nicht abgeschlossen werden.

Im **Gesetz über das Halten von Hunden** fehlte bisher eine Grundlage für eine Bekanntgabe von Besitzern entlaufener Hunde durch die Gemeinden[62] an die Landespolizei. Diese Situation kann vor allem dann unbefriedigend sein, wenn ein Hund am Wochenende entlaufen ist und dem Halter während des Wochenendes nicht zugeführt werden kann. Da bereits im Berichtsjahr in der Praxis Hunde elektronisch über einen Mikrochip identifiziert wurden, wurde angeregt, diese Identifikation und das entsprechende Zugriffsrecht auf eine Datenbank im Gesetz festzulegen. Diese Anregung, welche sich auf die schweizerische Lösung stützt, wurde durch die Regierung angenommen. Demgemäss sieht der Entwurf zum überarbeiteten *Gesetz über das Halten von Hunden* in Art. 9 und 10 vor,[63] dass der Hund mit einem Chip zu kennzeichnen ist. Zudem soll auch der Name und die Adresse des Tierhalters im Register geführt und der Landespolizei im Fall von entlaufenen Hunden ein Zugriff auf die Daten gegeben werden.

Des Weiteren stand eine Revision des **Heimatschriftengesetzes** an, welche die *Einführung der biometrischen Pässe* vorsieht. Die Regierung hatte beschlossen, diese Pässe bis Ende Oktober 2006 einzuführen, obwohl Liechtenstein dazu rechtlich nicht verpflichtet ist (möglicherweise aber faktisch). Denn eine Pflicht besteht nur für EU-Staaten, welche dem Schengen Abkommen beigetreten sind. Die SDS wurde von Anfang an in die Revision dieses Gesetzes einbezogen. In einer Stellungnahme zu den verschiedenen Aspekten wurde vor allem die Sicherheit der biometrischen Daten[64] betont, unter Hinweis auf ein Dokument, das von der Art. 29 Arbeitsgruppe zu diesem Thema angenommen worden war.[65] Die Anregung der Löschung von personenbezogenen Daten im Passregister nach maximal einer fünfjährigen Frist nach Ablauf der Gültigkeit des Passes, welche durch die SDS gemacht worden war, wurde nicht berücksichtigt. So ist weiterhin die allgemeine Bestimmung des DSG anwendbar.[66] Aus Sicherheitsgründen ist es beispielsweise in Deutschland nicht erlaubt, eine zentrale Datenbank zu den gespeicherten biometrischen Daten zu führen.[67] Da das im Heimatschriftengesetz vorgesehene Passregister nicht ein Register im eigentlichen Sinn, sondern eine einfache Exceltabelle ist und dazu weder im Gesetzesentwurf noch in den Erläuterungen dazu die Rede davon ist, dass die Daten zentral gespeichert werden,[68] kann davon ausgegangen werden, dass eine zentrale Speicherung der biometrischen Daten in Liechtenstein ebenfalls nicht vorgesehen ist. Dies ist aus Sicherheitsgründen zu begrüssen.

Bei der Bearbeitung von Personendaten in besonderen Bereichen der **Verbrechensbekämpfung** (Terrorismus, gewalttätiger Extremismus, organisiertes Verbrechen und des verbotenen Nachrichtendienstes) und im Bereich der **inneren Sicherheit** sind nach Art. 43 DSG Ausnahmen von bestimmten Grundsätzen des DSG[69] möglich. Solche Ausnahmen sind im Entwurf einer **Staatsschutzverordnung** vorgesehen, welche bei Jahresende kurz vor Verabschiedung durch die Regierung stand. Die baldige Schaffung eines Staatsschutzgesetzes nach Inkrafttreten der Verordnung wird wichtig und dringend sein, da dann wieder ein Gleichgewicht zu den Grundsätzen des DSG zu schaffen sein wird; dies unter Beachtung des verfassungsmässigen Rechts auf Achtung der Privatsphäre.

Bei der Schaffung bzw. der Revision des **Versicherungsvermittlungsgesetzes**, des **Vermögensverwaltungsgesetz (VVG)** und des **Unfallversicherungsgesetzes** wurde eine Stellungnah-

[61] Das gewählte Verfahren stützte sich auf dasjenige des Kantons Basel-Stadt, vgl. Tätigkeitsbericht 2004, 5.1.1.1. Das Verfahren in Belgien weist zudem viele Ähnlichkeiten auf.

[62] Nach diesem Gesetz haben die Gemeinden ein Register zu führen, in dem die Hundeverzeichnisse zu führen sind.

[63] Vgl. Bericht und Antrag der Regierung betreffend die Abänderung des Gesetzes über das Halten von Hunden (und die Abänderung des Gesetzes über die Landes- und Gemeindesteuern (Steuergesetz), Nr. 109/2005.

[64] Bei biometrischen Daten geht es um Folgendes: Während man bisher für Identifikationszwecke Angaben benötigte, die man hatte (wie die Identitätskarte: «was habe ich?») oder die man wusste (wie eine PIN-Nr. bei Auszügen an Bankomaten, «was weiss ich?») geht es bei biometrischen Daten um Angaben, die in der Regel universell, einzigartig und dauerhaft sind, da sie sich auf den eingenen Körper beziehen (Bsp. Fingerabdruck, «Wer bin ich?»). Die für Identifikationszwecke erforderlichen Angaben sind somit bei biometrischen Daten höchstpersönlich.

[65] Vgl. unten, 7.1.

[66] Vgl. Art. 26 DSG.

[67] Vgl § 4 Abs. 4 des deutschen Passgesetzes.

[68] Im Gegenteil: Der Entwurf zu Art. 16a spricht an mehreren Stellen davon, dass die Daten im Reisepass bzw. auf einem Datenchip gespeichert werden.

[69] Diese Ausnahmen beziehen sich auf die Grundsätze der Zweckgebundenheit (Art. 4 Abs. 3), der Datenbekanntgabe ins Ausland (Art. 8), die Meldepflicht und die Registrierung (Art. 15), die Beschaffung von Daten (Art. 22) und das Erfordernis der ausdrücklichen gesetzlichen Grundlage für die Bearbeitung von besonders schützenswerten Daten und Persönlichkeitsprofilen (Art. 21 Abs. 2).

me abgegeben und angeregt, dass eine allgemeine Datenschutzbestimmung eingeführt wird,[70] damit massgeschneiderte Lösungen für diese Gesetze geschaffen werden können. Dabei ging es auch teils darum, dass eine ausdrückliche gesetzliche Grundlage für die Bearbeitung von besonders schützenswerten Daten und von Persönlichkeitsprofilen[71] geschaffen wird.

Weitere Stellungnahmen erfolgten zu Vorentwürfen in Bezug auf ein **Gesetz über Massnahmen im Wirtschaftsverkehr mit fremden Staaten,** ein revidiertes **Strafvollzugsgesetz** und zu einem Revisionsentwurf betreffend das **Polizeigesetz**.

Im **internationalen Bereich** wurde zur Schaffung eines Staatsvertrages zwischen Österreich, der Schweiz und Liechtenstein über den gegenseitigen *Austausch in Asylangelegenheiten* Stellung genommen. Am Entwurf, der sich an einem Staatsvertrag zwischen Österreich und Bulgarien orientiert hatte, war nichts Grundsätzliches zu bemerken. Dazu erfolgte eine erste Stellungnahme zu einem Vorentwurf einer *Vereinbarung* zwischen der Schweiz und Liechtenstein über eine Beteiligung Liechtensteins an der *Führung und Nutzung von automatisierten schweizerischen Registern im Strassenverkehrsbereich*. Auch wurde zur *Cyber-Crime Konvention* des Europarates Stellung genommen. Diese Konvention, die als erstes internationales Abkommen im Bereich der an Bedeutung zunehmenden Computerkriminalität gilt, scheint auch deswegen wichtig zu sein, da mit den USA ein sehr wichtiger Akteur in diesem Bereich an der Ausarbeitung der Konvention beteiligt war. Dieser Umstand ist denn auch im Konventionstext ersichtlich. Das Abkommen ist ein eigentliches Abkommen zur Stärkung der Zusammenarbeit im Bereich der Strafverfolgung. Der Datenschutz wurde darin kaum berücksichtigt. Deshalb konnte dieses einseitig angelegte Abkommen aus Sicht des Datenschutzes nicht begrüsst werden. In der Praxis wurde es bisher nicht den ursprünglichen Ansprüchen gerecht. Bisher wurde es z.B. weder von Deutschland, der Schweiz, Österreich oder gar den USA ratifiziert.

4.5. PROJEKTBEGLEITUNG

Oft wird nicht nur von «Datenschutz» gesprochen, sondern von «Datenschutz und Datensicherheit». Obwohl die Datensicherheit ein (wenn auch wichtiger) Aspekt des Datenschutzes darstellt, wird damit die Sicherheit angetönt, welche bei automatisierten Datenbearbeitungen essentiell ist. Bei den folgenden komplexen Vorhaben bildete dementsprechend die Datensicherheit einen Kernpunkt aus Sicht des Schutzes der Privatsphäre.

Mit dem zunehmenden Gebrauch der elektronischen Kommunikation (Email, Internet) wurde in den letzten Jahren auch das Dienstleistungsangebot der Landesverwaltung erweitert. Heute werden vermehrt Anfragen per Email an die Landesverwaltung gestellt. Ideal und sehr kundenfreundlich wäre es, wenn solche Anträge rechtsverbindlich per Email an die Verwaltung gestellt werden könnten (Bsp. elektronische Steuererklärung). Das Problem dabei besteht aber darin, dass bei Emails, so wie sie im Alltag gebraucht werden kann, nicht fest steht, dass der Absender die Person ist, für die er sich ausgibt (Authenzität), noch dass der Inhalt der Email nicht verfälscht wurde (Integrität).[72] Konkret erfordert auch die Einführung von biometrischen Pässen eine verbesserte und sicherere Identifikation des Passinhabers. Aus verschiedenen Gründen wurde durch die Regierung eine Arbeitsgruppe ins Leben gerufen, welche die technischen, organisatorischen und rechtlichen Rahmenbedingungen für eine so genannte **«Public Key Infrastructure» (PKI)** in einem Detailkonzept ausarbeiten sollte.[73] In diesem System ist die Datensicherheit und damit auch der Datenschutz inhärent. Somit ist PKI grundsätzlich eine datenschutzfreundliche Technologie.

[70] Eine solche Regelung sollte den Grundsatz der Datenbearbeitung, allenfalls die Datenbekanntgabe (mittels Internet), technische und organisatorische Massnahmen sowie möglicherweise die Löschung der Daten erfassen.

[71] Zu den angesprochenen ausdrücklichen Grundlagen vgl. unten, 5.1.2.

[72] Anforderungen wie Integrität, Echtheit und Vertraulichkeit sind zu erfüllen. Der Empfänger muss die Garantie haben, dass die übermittelten Daten vom genannten Urheber stammen. So kann der Absender später auch nicht leugnen, die Nachricht verfasst zu haben. Weiter müssen Sender und Empfänger die Sicherheit haben, dass die Nachricht so, wie sie abgeschickt wurde, auch den Empfänger erreicht und Dritte sie nicht verändern können.

[73] Eine PKI besteht dabei aus einem einfachen aber wirkungsvollen Prinzip. PKI-Lösungen funktionieren mit asymmetrischer Verschlüsselung. Bei diesem System hat jeder Nutzer zwei Schlüssel. Einer ist privat (Private Key) und ein Schlüssel ist öffentlich (Public Key). Dieses Schlüsselpaar wird von einer vertrauenswürdigen Stelle (Certification Authority) nach einer persönlichen Authentifizierung ausgestellt. Praktisch gesehen heisst dies, dass auf einer Smartcard (ähnlich einer Bankomatkarte) das persönliche Schlüsselpaar gespeichert ist. Diese Signaturkarte wird über elektronische und mechanische Mechanismen vor unbefugtem Zugriff geschützt. Über ein Lesegerät kann mit der Smartcard auf die Signatur-Software auf dem Computer zugegriffen, das gewünschte Dokument unterschrieben und verschlüsselt übertragen werden. Die Konzeption und der Betrieb einer PKI ist ein sehr komplexer Prozess, der eine genaue Kenntnis der Rechtsgrundlagen [vgl. Signaturgesetz (SigG), vom 18. September 2003, LGBl. 2003 Nr. 215, und Signaturverordnung (SigV) vom 1. Juni 2004, LGBl. 2004 Nr. 130] und der Technologie voraussetzt. Neben der Einführung für die neuen Pässen wird der Gebrauch von PKI auch für den neuen Ausländerausweis, die Identitätskarte oder für die Umsetzung der Publizitätsrichtlinie (Richtlinie 2003/58/EG des Europäischen Parlaments und des Rates vom 15. Juli 2003 zur Änderung der Richtlinie 68/151/EWG des Rates in Bezug auf die Offenlegungspflichten von Gesellschaften bestimmter Rechtsformen) diskutiert.

Zudem beschloss die Regierung, eine Vorstudie zum Thema **Enterprise Content Management (ECM)** durchzuführen. Mit dieser Vorstudie sollten die Stärken und Schwächen der aktuellen Schriftgutverwaltung beurteilt werden. Dabei geht es im Wesentlichen darum, ob ein **Dokumentenmanagementsystem (DMS)** in der Landesverwaltung eingeführt werden soll. Dieses System kann kurz mit dem Schlagwort «papierloses Büro» umrissen werden und dient der Verwaltung der zunehmenden Dokumentenbestände in physischer und elektronischer Form.[74] DMS ermöglicht ein schnelleres Auffinden von Dokumenten und Informationen in diesen Dokumenten. Somit kann über Suchkriterien nach gezielten Informationen und Dokumenten gesucht werden. Auch soll die Sachbearbeitung von der Notwendigkeit entlastet werden, sich zu einem Vorgang erst die Papierakten kommen zu lassen. Somit besteht ein wesentliches Ziel von DMS in der Beschleunigung der verwaltungsinternen Arbeit. Diese Vorteile schaffen aber auch neue Gefahren für den Schutz der Privatsphäre. Es ist wichtig, dass ein solches Vorhaben die datenschutzrechtlichen Auswirkungen von Beginn weg im Blick haben muss: Wenn beliebige Dokumente in elektronischen Akten zusammengeführt werden, können ohne grossen Aufwand und Zusatzwissen Persönlichkeitsprofile erstellt werden. Deshalb ist es sehr wichtig, dass personenbezogene Daten gemäss dem Stichwort «Datensparsamkeit»[75] bearbeitet werden. Aus Sicht des Datenschutzes kommt dabei der Gewährleistung eines entsprechenden Zugriffsschutzes und einer genau definierten Suchfunktion[76] zentrale Bedeutung zu. Das Zugriffsberechtigungs- und das Suchsystem müssen dabei die verschiedenen Aufgaben in der Landesverwaltung berücksichtigen und das Amtsgeheimnis oder gar eine gesetzliche Schweigepflicht sind unbedingt zu beachten. Eine totale Transparenz der Akten innerhalb der Landesverwaltung ist somit unbedingt zu vermeiden, da sie auch dem Gesetzmässigkeitsprinzip der Landesverfassung widerspricht. Ausserdem ist die Zweckgebundenheit der Bearbeitung zu beachten; d.h. dass Daten, die für einen bestimmten Zweck verarbeitet werden, nicht auch für einen anderen (gesetzlich nicht vorgesehenen) Zweck bearbeitet werden dürfen. Ausserdem ist eine Protokollierung[77] und die Erstellung eines Bearbeitungsreglements unumgänglich. Daneben sind die notwendigen Löschungsmöglichkeiten festzulegen und allfällige Überwachungsmöglichkeiten von Mitarbeitern der Landesverwaltung zum Zwecke der Verhaltens- und Leistungskontrolle durch die Protokolldaten sind zu vermeiden. Die Datensicherheit ist selbstverständlich ebenso zu berücksichtigen.[78] Werden Dokumente nicht mehr für eine Aufgabe benötigt, sind sie zu anonymisieren oder zu löschen, wenn sie nicht insbesondere im Landesarchiv gelagert werden. Die Bestimmungen des Archivgesetzes und insbesondere die gesetzlichen Sperrfristen für die Bekanntgabe von Personendaten, sind auch bei Einführung eines «papierlosen Büros» zu beachten. Insgesamt ist die Einführung eines DMS ein komplexes Vorhaben, das unter Beachtung der erwähnten Anforderungen, zahlreiche Vorteile für eine moderne Verwaltung mit sich bringt.[79]

Die Krankenversicherungskarten-Verordnung (KVKV) vom 15. März 2005, LGBl. 2005 Nr. 55, regelt den Rahmen für die Benutzung der Krankenversicherungskarte, welche auf Anfang 2006 von den Kassen geschaffen werden soll. Diese Verordnung ist ein Ergebnis der Arbeitsgruppe **«Elektronisches Gesundheitsnetz»** (eGN), Phase I. Darin wird festgehalten, dass administrative Daten, welche zur Identifikation eines Versicherten dienen, auf die Karte aufzunehmen sind. Demgegenüber sind Gesundheitsdaten nur mit einer schriftlichen Zustimmung der betroffenen Person aufzunehmen. Nachdem die Arbeit in Bezug auf die Vorbereitung der Aufnahme administrativer Daten abgeschlossen worden war, beschäftigte sich die Arbeitsgruppe 2005 damit, ob und welche Gesundheitsdaten auf die Karte aufgenommen werden sollen. Aus Sicht des Datenschutzes wurde betont, dass die Aufnahme von Gesundheitsdaten praktisch sein kann, dass dies aber nur mit der ausdrücklichen Einwilligung des Versicherten geschehen darf, wie dies auch in der KVKV festgehalten wird. Da es sich bei Gesundheitsangaben um besonders schützenswerte Daten

[74] Mit DMS soll die Integration von Dokumenten (eingescannte Dokumentoriginale, Faxeingänge, Dateien aus Büroanwendungen, Emails, Multimediadateien, usw.) unterschiedlicher Herkunft und Abbildung von Geschäftsprozessen der Verwaltung unterstützt werden.

[75] Mit der Datensparsamkeit ist insbesondere gemeint, dass nur die Dokumente, die für die Aufgabenerfüllung erforderlich sind, in das DMS aufgenommen wird.

[76] Das DMS integriert verschiedene Möglichkeiten der Suche in einem System und ermöglicht somit zielgenau und effektiv innerhalb kurzer Zeit die gewünschten Informationen zu erhalten. Es muss sichergestellt sein, dass jeder Nutzer nur solche Suchergebnisse angezeigt erhält und nur auf solche personenbezogenen Informationen zugreifen kann, die er zur Erfüllung seiner dienstlichen Aufgaben benötigt.

[77] Es muss jederzeit nachträglich überprüfbar und feststellbar sein, ob und vom wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind. Diese Informationen dürfen aber nicht zum Zwecke der Verhaltens- und Leistungskontrolle genutzt werden.

[78] Sicherheit wie Integrität, Verfügbarkeit, Authentizität, Vertraulichkeit müssen erfüllt sein.

[79] Vgl. die umfassende Orientierungshilfe «Datenschutz bei Dokumentenmanagementsystemen» einer Arbeitsgruppe der deutschen Konferenz der Datenschutzbeauftragten vom März 2006:
http://www.bfdi.bund.de/cln_029/nn_530772/DE/Themen/TechnologischerDatenschutz/TechnologischeOrientierungshilfen/Artikel/OrientierungshilfeDMS.html.

handelt, wurde zudem betont, dass dafür ein sehr hohes Sicherheitsniveau zu schaffen ist. Im Sinne von Gesundheitsdaten ist die Aufnahme von Notfalldaten in der Verordnung vorgesehen. Die Arbeitsgruppe hatte als Aufgabe diese Notfalldaten zu definieren, konnte dies jedoch nicht bis Jahresende abschliessen. Die Zugriffsberechtigung auf solche Gesundheitsdaten wird ebenfalls durch die KVKV geregelt: So ist vorgesehen, dass diese Daten ausschliesslich von Ärzten, Zahnärzten und Apothekern bearbeitet werden dürfen, welche in dem aktuellen Fall medizinisch und therapeutisch involviert sind und für einen konkreten Anlassfall für eine Gesundheitsabklärung oder eine versicherungstechnische Abklärung erforderlich ist. Ein Zugriff auf die Gesundheitsdaten durch die Krankenkassen ist dem gegenüber nicht vorgesehen.

5. Aufsicht

5.1. AUFSICHT ÜBER BEHÖRDEN

5.1.1. DATENSCHUTZWIDRIGE BEARBEITUNGEN

5.1.1.1. Datenbanken

An dieser Stelle sei daran erinnert,[80] dass die **Zentrale Personenverwaltung (ZPV)** eine umfassende Datenbank der Landesverwaltung darstellt, welche primär die Erleichterung von administrativen Abläufen bezweckt. Ein Pfeiler ist eine eindeutige Nummer, welche für die erfassten Personen vergeben wird. Etliche Amtsstellen haben Zugriff auf eine Übersichtsmaske, welche folgende Datenfelder enthält: Name, Vorname, Anrede, Titel, Erwerbsstellung, Geschlecht, Geburtsdatum, Geburtsort, Zivilstand, Heiratsdatum, Todesdatum, Todesort, Bürgerort, Staatsbürgerschaft, Personenbeziehungen, Adresse, Arbeitsverhältnis sowie verschiedene ausländerrechtliche Angaben. Da in der Vergangenheit nicht datenschutzrechtlich geprüft worden war, ob eine Amtsstelle eines der genannten Felder zur Arbeit wirklich benötigt, wurde das nachgeholt. Nachdem im letzten Berichtsjahr noch nicht alle Anträge auf Zugriffsberechtigungen von Feldern der ZPV abgeschlossen werden konnten, war dies Mitte 2005 der Fall.[81] Die *Verteilung der Zugriffsberechtigung* musste danach in der Praxis dahingehend überprüft werden, ob die Berechtigungen richtig umgesetzt wurden. Diese aufwändige Arbeit wurde mit einer Aushilfskraft angegangen, konnte jedoch nicht bis Jahresende abgeschlossen werden. Es gibt auch in anderen Ländern in Europa Datenbanken, in denen die ganze Bevölkerung erfasst wird. Dort sind aber die Daten nur sehr punktuell zugänglich. Dies ist in Liechtenstein anders, da es keine Filter zu gewissen *Personengruppen* (Kinder, Pensionisten, u.a.) gibt. Mit anderen Worten ist stets insbesondere die gesamte Bevölkerung erfasst. Deren Daten sind auch dann für diese Amtsstellen sichtbar, wenn es keinen Behördenverkehr mit solchen Personengruppen gibt.[82] Deshalb wurde im Berichtsjahr versucht, so weit wie möglich Filter einzubauen, um die Personengruppen zu verkleinern. Dies erwies sich auf Grund der Beschaffenheit der ZPV bisher als unmöglich. Somit stehen den Amtsstellen, welche über Zugriffsberechtigungen verfügen, wohl Zugriffe auf Felder zu, welche sie für die Arbeit benötigen, aber gleichzeitig auch auf Personengruppen, mit denen kein amtlicher Kontakt besteht. Diese Personengruppen sind für die Verrichtung der Arbeit einer Amtsstelle somit nicht nötig, weshalb ein Zugriff auf solche Personengruppen unverhältnismässig ist und in das Privatleben der betroffenen Personen eingreift. Durch eine *History-Funktion* sind auch Daten in der Vergangenheit einsehbar und bisher ohne Eingrenzung. Die einzelnen Amtsstellen wurden befragt, ob und bis zu welchem Zeitpunkt *Daten der Vergangenheit* für die Arbeit nötig sind. Das Selbe wurde für *Verstorbene* gemacht, damit der Zugriff von Amtsstellen weiter reduziert werden kann. Auf Grund der Beschaffenheit der ZPV stellte sich eine solche Einschränkung als nur schwer bis nicht möglich heraus. Dies bedeutet, dass z.B. bei Stipendienanträgen Daten angegeben werden müssen, welche teils bis zehn Jahre in die Vergangenheit reichen. Ereignisse vor elf Jahren sind aber für die Stipendienstelle grundsätzlich irrelevant. Dies ist ein weiterer Verstoss gegen das Verhältnismässigkeitsprinzip. Es ist erstaunlich, wie die ZPV in den letzten Jahren an Beliebtheit in der Landesverwaltung zugenommen hat. Dies mag damit verbunden sein, dass durch die Arbeiten zur Datenschutzkonformität die ZPV an Bekanntheit zunahm. Dabei ist aber zu beachten, dass es sich bei dieser Datenbank, welche im Laufe der Jahre ausgebaut wurde, nicht um das Wunderinstrument handelt, als das es oft wahrgenommen wird. In diesem Sinne verfasste die Arbeitsgruppe ZPV ein Schreiben an ein anwendendes Amt, um auf verschiedene Missstände und/oder Missverständnisse hinzuweisen. In diesem Schreiben wurde festgehalten, dass die Daten in der Regel für Zwecke eingegeben werden, die für die erfassende Amtsstelle, nicht aber unbedingt für eine andere Amtsstelle wichtig sind. Somit kann es sein, dass Daten falsch interpretiert werden. Dem Inhalt der ZPV darf nicht ‹blind› vertraut werden. Vielmehr muss der Erfassungszweck der Daten dem eigenen Verwendungszweck gegenüber gestellt werden. Als weitere Schwachstelle gilt, dass die ZPV sowohl doppelte als auch falsche Einträge enthält. Zudem ist eine Löschung dieser Einträge momentan nicht möglich. Dieser Widerspruch gegen das DSG ist ebenfalls in der grundsätzlichen Beschaffenheit der ZPV begründet und ist nur schwer zu lösen. Zu erwähnen ist schliesslich, dass es etliche Fachapplikationen in der Landesverwaltung gibt, welche auf die erwähnten globalen Daten aufbauen. Bei Jahresende war eine abschliessende Liste über solche Fachapplikationen in Zusammenarbeit mit dem Amt für Personal und Organisation noch in Vorbereitung.

[80] Vgl. Tätigkeitsbericht 2003, 4.1.2. und Tätigkeitsbericht 2004, 5.1.1.1.

[81] Vgl. dazu Tätigkeitsbericht 2003, 4.1.2. und Tätigkeitsbericht 2004, 5.1.1.1.

[82] Beispiele: das Schulamt benötigt kaum Daten von kinderlosen Personen, das Amt für Soziale Dienste (ASD) kaum Angaben von Millionären, das Amt für Volkswirtschaft (AVW), Abteilung Gewerbe nicht von Rechtsanwälten, Ärzten und anderen Personengruppen, die Finanzmarktaufsicht (FMA) nur Daten von Finanzdienstleistern, usw..

5.1.1.2. ANDERES

Wie schon früher berichtet[83] machten die oder zumindest einige **Gemeinden** bewilligte **Einbürgerungen** bzw. Stellungnahmen zu Einbürgerungsanträgen und bewilligte **Baugesuche** bekannt, ohne dass es dafür eine Rechtsgrundlage gibt. Obwohl in der Sache der Baubewilligungen eine rechtskräftige Entscheidung der Datenschutzkommission besteht, welche die Bedingungen für Bekanntgaben verbindlich festlegt, gab es danach noch Unregelmässigkeiten, welche inzwischen behoben werden konnten. Die **Bekanntgabepraxis** von **Einbürgerungen bei den Gemeinden** wurde weiter behandelt. Dazu wurde ein Fragebogen an die Gemeinden verschickt. Einzig die Gemeinde Vaduz antwortete dahingehend, dass sie bewilligte Einbürgerungen nicht bekannt gibt. Die anderen Gemeinden halten an einer Bekanntgabe fest[84] oder beantworteten den Fragebogen nicht.[85]

Bei **Grenzgängermeldebestätigungen** des Ausländer- und Passamtes war es üblich, den Zivilstand der betroffenen Person zu erfragen. Damit sollte abgeklärt werden können, ob diese Person in der ZPV bereits erfasst wurde, um Doppeleinträge zu vermeiden. Auf Grund einer Beschwerde einer privaten Person wurde diese Praxis geändert. Für eine Grenzgängermeldebestätigung ist der Zivilstand irrelevant. Diese Praxis war dementsprechend nicht gesetzeskonform. Das entsprechende Formular wurde geändert. Nun wird der Ledigenname erfragt. Diese Angabe geht weniger weit, da somit nicht in allen Fällen ersichtlich ist, ob die Antrag stellende Person ledig, verheiratet oder geschieden ist.

Wie bereits erwähnt[86] wurden die Eltern über die Befragung ihrer Einkommensverhältnisse bei **Stipendienanträgen** ihrer Kinder nicht benachrichtigt. Zwar wurde das Stipendiengesetz in dem Sinne angepasst, dass die Stipendienstelle berechtigt ist, bei den Gemeinden und bei der Steuerverwaltung die für die Berechnung der Ausbildungsbeihilfen notwendigen Steuerdaten einzuholen. Damit wurde aber lediglich die geltende Praxis auf eine rechtliche Grundlage bestellt. Aus Transparenzgründen sind aber die betroffenen Eltern von der Stipendienstelle über diese Befragung zu informieren. Auf Grund einer Beschwerde machte der DSB die Stipendienstelle darauf aufmerksam, dass die Betroffenen auf diese Datenbeschaffung bei einer Drittstelle hinzuweisen sind. Dies sollte mindestens im Rahmen der Information zu Stipendienanträgen auf der Internetseite des Schulamtes und auf einem Beiblatt geschehen, das jedem Stipendienantrag beizulegen ist.[87] Den Datenschutzanforderungen wurde bis Ende 2005 (noch) nicht nachgekommen.

Das Bürgermeisteramt in **Vaduz** wurde angefragt, zu welchem Zweck der Vaduzer Saal **videoüberwacht** wird. Zudem wurde darauf aufmerksam gemacht, dass die Betroffenen über eine stattfindende Datenbearbeitung zu informieren sind. Dementsprechend ist eine Hinweistafel über die stattfindende Videoüberwachung anzubringen.

Den Gemeinden wurde vor den Landtagswahlen in Absprache mit dem Ressort Inneres mitgeteilt, dass eine **Bekanntgabe der Wählerlisten** an die politischen Parteien vor den Landtagswahlen gesetzlich nicht vorgesehen ist. Dennoch kam es anscheinend vor, dass die Listen von Wahlberechtigten zu Wahlwerbezwecken an die oder einzelne Parteien weiter gegeben wurden. Dies ist ein Rechtsverstoss. Denn Art. 11 des Volksrechtegesetzes (VRG) sieht die Bekanntgabe von Wählerlisten nur vor, damit sich eine Person, welche nicht auf der Liste aufgeführt ist, darüber beschweren kann oder, im umgekehrten Fall, kann geltend gemacht werden, dass eine Person zu Unrecht auf der Wählerliste erscheint. Die öffentliche Auflage der Wählerlisten dient einzig diesem Zweck. Zudem ist von «Auflage» die Rede; dies bedeutet, dass eine Liste öffentlich eingesehen, nicht aber aus politischen Gründen zugeschickt werden kann.

5.1.2. GESETZLICHE GRUNDLAGEN

Mit Volkszählungen erhebt ein Staat wichtige Daten, die unter anderem statistisch ausgewertet werden. Die Fragebogen zur Durchführung von Volkszählungen sind jeweils sehr detailliert und führen in jedem Fall dazu, dass mit der Durchführung einer Volkszählung Persönlichkeitsprofile bearbeitet werden. Für solche Bearbeitungen sieht das DSG aber qualifizierte Voraussetzungen vor; demnach muss in der Regel eine ausdrückliche gesetzliche Grundlage geschaffen werden, wenn diese noch

[83] Vgl. Tätigkeitsbericht 2004, 5.1.1.2.
[84] Eschen, Planken, Ruggell, Schaan, Schellenberg, Triesen.
[85] Balzers, Gamprin, Mauren, Triesenberg.
[86] Vgl. oben, 3.2.
[87] Vgl. unten, 5.1.1.2.

nicht besteht.[88] Da die Volkszählungen in der Vergangenheit auf dem Statistikgesetz und einem entsprechenden Regierungsbeschluss basierte, wurde bei der Regierung die Schaffung eines **Volkszählungsgesetzes** angeregt.

Auch bei der **ZPV**, die Persönlichkeitsprofile enthält, wurden Fortschritte gemacht, was die Schaffung einer allgemeinen rechtlichen Grundlage angeht.[89]

Die Schaffung einer ausdrücklichen **rechtlichen Grundlage** für die **Gemeindedatenbank(en)** GeSoL wurde mit dem Ressort Inneres in Angriff genommen. Eine Lösung wird zur Zeit im Rahmen eines Gesetzespakets zu Art. 44 Abs. 3 DSG ausgearbeitet.

5.2. ABKLÄRUNGEN UND EMPFEHLUNGEN IM PRIVATRECHTSBEREICH

Im Privatrechtsbereich ging eine Beschwerde von zwei Personen ein, welche sich über die Versendung einer Email zu Direktmarketingzwecken aus Liechtenstein beklagt hatten. Diese beiden Personen hatten diese Email als **Spam-Mail** bezeichnet. Da diese Beschwerde erst kurz vor Jahresende einging, konnte der Sachverhalt noch nicht abschliessend festgestellt werden. Auf alle Fälle wird an Hand dieser Beschwerde eine wichtige Entscheidung zur Definition von Direktwerbung und unerwünschter Werbung (Spam)[90] zu fällen sein.

[88] Vgl. Art. 21 DSG.
[89] Vgl. oben, 4.4.
[90] Vgl. zu Spam auch Tätigkeitsbericht 2004, 7.1. und oben, 3.1.

6. Register der Datensammlungen

An dieser Stelle sei daran erinnert[91], dass das Register der Datensammlungen das Ziel hat, eine Transparenz zu schaffen, damit insbesondere sichtbar werden soll, über welche Datensammlungen die Behörden verfügen. In das Register werden zwar keine Einzeldaten über die Betroffenen, sondern nur summarische Angaben aufgenommen, welche einen Überblick über die gesamte Datenbearbeitung erlauben. Nähere Angaben können die Betroffenen beim Inhaber der Datensammlung selbst auf Grund des gesetzlichen Auskunftsrechts bekommen.

Im Dezember des Berichtsjahres wurde das Register auf der Internetseite der SDS veröffentlicht. Es umfasste 490 Datensammlungen.[92]

Die **Gemeinden** und das **Zivilstandsamt** führen nach dem Heimatschriftengesetz eine Datensammlung über Heimatscheine. Zudem nehmen die **Unfallversicherungen** im obligatorischen Versicherungsbereich die Stellung einer Behörde ein. Damit ist die Anmeldung der entsprechenden Datensammlungen eine Pflicht.[93] Die **Anmeldung** dieser **Datensammlungen** war bis Jahresende noch nicht erfolgt.

[91] Vgl. Tätigkeitsbericht 2003, 5. oder Tätigkeitsbericht 2004, 4.4.
[92] Vgl. *http://www.llv.li/amtsstellen/llv-sds-register_der_datensammlungen.htm.*
[93] Vgl. Art. 15 Abs. 2 DSG.

7. Internationales

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

Die so genannte **Art. 29 Arbeitsgruppe**, benannt nach Art. 29 der Datenschutzrichtlinie, welcher die Basis dieser Gruppe darstellt, behandelte auch 2005 Themen internationaler Relevanz, die auch für Liechtenstein Auswirkungen haben werden. In diesem Jahr wurden Dokumente vor allem zu folgenden Themen verabschiedet:

In einem Arbeitspapier zu **Datenschutzfragen im Zusammenhang mit Immaterialgüterrechten** beschäftigt sich die Arbeitsgruppe insbesondere mit der Bearbeitung von Personendaten beim Austausch bzw. Bezug urheberrechtlich geschützten Materials im **Internet**. Dabei wird festgestellt, dass der Zugang gerade zu Musikstücken immer häufiger von einer vorherigen Überprüfung der Identität des Benutzers abhängig gemacht wird. Neben dem erklärten Zweck der Kontrolle der individuellen Nutzung der Musikstücke wird die Kennzeichnung oft auch zur Erstellung von Benutzerprofilen und zur gezielten Werbung verwendet. Während primär der Missbrauch urheberrechtlich geschützten Materials verhindert werden soll, wird damit auch die Nachverfolgung von Benutzern und die Überwachung ihrer Vorlieben zu kommerziellen Zwecken angestrebt. Dies entspricht allerdings nicht dem Grundsatz der Zweckgebundenheit. Dazu kommt, dass eine Sammlung von Daten über Konsumgewohnheiten das Ausmass von Benutzerprofilen annehmen kann.[94] Die Arbeitsgruppe hält fest, dass personenbezogene Daten nur dann bearbeitet werden dürfen, wenn der betroffenen Person im Voraus bestimmte Auskünfte erteilt werden. Dazu zählen vor allem die Identität der bearbeitenden Stelle, das heisst des Betreibers der Internetseite, welcher für den Inhalt derselben zuständig ist, und der Verarbeitungszweck.[95] Diese Information ist eine Voraussetzung, damit die betroffene Person ihre Einwilligung zur Datenbearbeitung geben kann. Diese Informationen sollen gut sichtbar angezeigt werden, bevor der Benutzer seine Daten eingibt oder gekennzeichnetes Material bezieht. Als Ergebnis hält die Arbeitsgruppe mit Besorgnis fest, dass die rechtmässige Nutzung von Technologien zum Schutz urheberrechtlich geschützter Werke den Schutz personenbezogener Daten beeinträchtigen könnte. So lässt die Anwendung der Datenschutzgrundsätze auf die digitale Rechteverwaltung (digital rights management) erkennen, dass der Schutz des Einzelnen in der Offline-Welt und der Schutz des Einzelnen in der Online-Welt besonders vor dem Hintergrund einer Profilerstellung immer stärker auseinander klaffen. Deshalb wird die Entwicklung datenschutzgerechter technischer Instrumente gefordert und ganz allgemein die transparente Nutzung eindeutiger Identifikationen, welche dem Benutzer eine Wahlmöglichkeit bezüglich der Benutzung von solchen Internetseiten zugestehen.

In einem Arbeitsdokument zu **«Datenschutz und RFID-Technologien»** äussert sich die Arbeitsgruppe zu RFID-Funkchips (Radio Frequency Identification Technologies). Diese basieren auf einem IT-System, das über eine Antenne Funksignale empfangen und abgeben kann. Solche Funkchips werden bereits heute verbreitet eingesetzt, da sie sich grundsätzlich überall dort eignen, wo automatisiert gekennzeichnet, erkannt, registriert, gelagert, überwacht oder transportiert werden muss (Bsp.: Überwachung von Räumen, Kennzeichnung von Waren, Objekten, Tieren oder Personen, Automatisierung und Prozessoptimierung und Lieferketten). Diese neue Technologie birgt neue Möglichkeiten, aber eben auch Gefahren für das Privatleben: Die verdeckte Sammlung einer Vielzahl von Daten, die sich alle auf ein und dieselbe Person beziehen, die Lokalisierung von Personen, die sich an öffentlichen Plätzen (Flughäfen, Bahnhöfen, Geschäften) aufhalten, die Erstellung von Kundenprofilen durch Beobachtung des Verbraucherverhaltens in Geschäften, das Auslesen von Informationen über Kleidungsstücke und Accessoires, die gerade getragen, oder über Medikamente, die mitgeführt werden, sind Beispiele für das Nutzungspotenzial von RFID. Dieses Potenzial ist aus datenschutzrechtlicher Sicht fragwürdig, wenn die RFID-Technik zur Erhebung von Personendaten genützt wird, indem die RFID-Nummer eines Produktes mit den Daten des Käufers (z.B. mittels einer Kundenkarte) verknüpft wird. Das Direktmarketing-Potential wird dadurch erhöht, dass die Kunden beim Betreten des Geschäfts identifiziert und ihre Verhaltensweise im Geschäft beobachtet werden können. Wichtig ist, dass der RFID-Chip im Sinne der Datensparsamkeit nur die notwendigen Daten erheben darf. Wichtig ist auch in diesem Zusammenhang die vorgängige Information der betroffenen Person über die stattfindende Datenbearbeitung.[96] So benötigt ein Supermarkt, der seine Kundenkarten mit RFID-Tags versieht, entweder eine vertragliche Vereinbarung oder die Einwilligung der betroffenen Person. Dabei ist zu betonen, dass die Einwilligung freiwillig sein und in voller Kenntnis der Sachlage erfolgen

[94] Damit ist auch die Wahrscheinlichkeit gegeben, dass Persönlichkeitsprofile bearbeitet werden, für die sehr strenge gesetzliche Bedingungen gelten.
[95] Vgl. oben, 3.2.
[96] Informiert werden muss über den Zweck der Datenbearbeitung und den Dateninhaber (also bspw. das Kaufhaus).

muss. RFID-Chips dienen der Kennzeichnung von Waren. Diese Kennzeichnung ist aber nur so lange erforderlich als das Produkt noch nicht gekauft ist. Sobald ein Produkt gekauft ist, sollten somit die Daten gelöscht werden. Weiters hält die Arbeitsgruppe fest, dass das Problem noch dadurch verschärft wird, dass die Technik auf Grund ihrer geringen Kosten nicht nur den großen Akteuren zur Verfügung stehen wird, sondern auch kleineren bis hin zum einzelnen Bürger. Schliesslich fordert die Arbeitsgruppe auch hier eine Entwicklung einer datenschutzkonformen Technik.[97]

Schon im letzten Tätigkeitsbericht[98] wurde auf die Einführung von **biometrischen Merkmalen in Ausweispapieren** hingewiesen. Die Relevanz für Liechtenstein wurde damals im Zusammenhang mit einem Beitritt zu den Abkommen von Schengen und Dublin gesehen, da erst mit einem Beitritt Liechtensteins zu diesen Abkommen eine rechtliche Verpflichtung zur Einführung biometrischer Pässe besteht. Diese Annahme erwies sich als falsch. Obwohl rechtlich dazu nicht verpflichtet, entschied die Regierung, dass die biometrischen Pässe bis Ende Oktober 2006 eingeführt werden sollen. Somit gewann das Thema Biometrie für Liechtenstein an Bedeutung.[99] Die Arbeitsgruppe nahm eine Stellungnahme zu **Normen für Sicherheitsmerkmale und biometrische Daten in Pässen und Reisedokumenten** an. Ausgehend vom «Arbeitspapier über Biometrie»[100] wird festgestellt, dass die Aufnahme biometrischer Merkmale in Pässe weit reichende Folgen für die Inhaber der Reisedokumente haben wird, da in Zukunft die Bürger ihre biometrischen Daten in digitalisierter Form zur Verfügung stellen müssen.[101] Somit können die biometrischen Merkmale in Datenbanken gespeichert und für zahlreiche nicht vorhersehbare Zwecke verfügbar gemacht werden. Ethische Bedenken bestehen insofern, dass in Zukunft staatliche Institutionen in der Lage sein werden, riesige Mengen an Körpermerkmalen über die Bürger zu sammeln und zu speichern.[102] Menschen mit Behinderungen, die es ihnen nicht erlauben, sich den biometrischen Prüfungen zu unterziehen, könnten stigmatisiert werden. Gesetzliche Bedenken bestehen darin, dass die Schaffung einer zentralen Datenbank mit biometrischen Daten aller Bürger gegen den Grundsatz der Verhältnismässigkeit verstossen könnte. Denn dadurch würde das Risiko des Missbrauchs und der widerrechtlichen Aneignung sowie der Zweckentfremdung erhöht.[103] Was die technischen Anforderungen an einen biometrischen Pass betrifft, ist zu sagen, dass ein kontaktloser Chip (RFID-Chip)[104], der die gespeicherten biometrischen Merkmale enthält, in den Pass integriert werden soll.[105] Dieser Chip birgt nach Ansicht der Arbeitsgruppe zahlreiche Risiken für die betroffenen Personen, schon weil die Kommunikation zwischen dem Chip und dem Lesegerät über Funk abläuft und deshalb abgehört und die Daten von Unbefugten ausgelesen werden können. Daher ist die Notwendigkeit einer geeigneten Sicherheitsarchitektur[106] zwingend. Allerdings kann auch mit einer solchen Sicherheitsarchitektur ein Missbrauch nicht ausgeschlossen werden. Auch in anderen Bereichen und insbesondere in der Privatwirtschaft, ist eine zunehmende Anwendung der Biometrie zu beobachten. Daher fordert die Arbeitsgruppe unter anderem[107] eine umfassende Debatte über die sich stellenden ethischen, rechtlichen und technischen Fragen.

Ausserdem nahm die Arbeitsgruppe eine Stellungnahme zur **Nutzung von Standortdaten** zur **Ortung von Personen** an. Durch die explosionsartige Entwicklung der Nutzung satellitengestützter Standortdaten und die rasante Verbreitung des Mobilfunks werden Spuren hinterlassen, welche es ermöglichen, dass der Standort einer Person ermittelt werden kann (insbesondere durch Fahrkartenautomaten, GPS, Bankkarten, elektronische Börsen oder Mobiltelefone). Während es in einer ersten Phase um eine Ortung eines Standortes z.B. mittels

[97] Vgl: *http://www.llv.li/amtsstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-technisches/llv-sds-spezialthemen-rfid_funkchips.htm.*
[98] Tätigkeitsbericht 2004, 7.1
[99] Vgl. oben, 4.4.
[100] *http://www.llv.li/pdf-llv-sds-biometrie_wp80_de.pdf.*
[101] Zwar waren bisher schon mit dem Lichtbild und Angaben zu Geschlecht, Grösse oder Augenfarbe biometrische Merkmale in den Pässen enthalten, doch waren diese nicht digitalisiert für den Staat verfügbar.
[102] In diesem Zusammenhang ist zu erwähnen, dass z.B. Fingerabdrücke bislang vor allem in Bezug zu einer Straftat erfasst wurden.
[103] Zusätzlich könnten biometrische Identifikatoren als Zugangsschlüssel zu anderen Datenbanken verwendet werden, um so Datensätze miteinander zu verknüpfen.
[104] Der RFID-Chip entspricht der ISO-Norm 14443.
[105] Der Pass muss über genügende Speicherkapazität aufweisen und einen hohen Sicherheitsstandard erfüllen, der die Integrität, Echtheit und Vertraulichkeit der gespeicherten Daten abdeckt.
[106] Gefordert wird eine globale PKI um ein höheres Mass an Vertraulichkeit der ausgetauschten Daten (mittels Zertifikaten) zu erreichen. Jedes digitale Zertifikat lässt sich jedoch eindeutig auf eine Person zurückverfolgen. Daraus können für den Zertifikatsinhaber verschiedene Nachteile wie die Nachverfolgung von Reisegewohnheiten entstehen. Zum Schutz vor solchen Nachteilen wird ein Schutzprofil (Protection Profile, PP: IT-Sicherheitskonzept, das vollständig, konsistent und kohärant ist) vorgeschlagen, das den «Common Criteria for Information Technology Security Evaluation (Common Criteria – CC: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik als ISO-Standard) vers. 2.1.» entspricht.
[107] Vgl. auch weitere Forderungen der Internationalen Datenschutzkonferenz unten, 7.5., welche sich auf Forderungen der Arbeitsgruppe beziehen.

einer Navigationshilfe auf Wunsch einer betroffenen Person ging, ist mittlerweile eine zweite Phase eingetreten, in der der Standort von Personen über ihr Mobiltelefon bestimmt werden kann, sogar wenn kein Gespräch geführt wird; es reicht, dass das Gerät eingeschaltet ist. Ein wichtiges Beispiel stellt die **Kinderortung** mittels Mobiltelefonen dar. Die Möglichkeit der Ortung des eigenen Kindes über ein Mobiltelefon erleichtert es Eltern, sich jederzeit über den Standort ihrer Kindern vergewissern zu können, ohne diese direkt anrufen zu müssen. Dies mag praktisch sein, birgt aber auch gewisse Risiken: Ein solches Ortungssystem mag den Eltern das Gefühl geben zu wissen, wo sich ihr Kind gerade befindet. Dies kann zu einer Vernachlässigung der Verantwortung gegenüber den Kindern führen. Für die Kinder ist es aber ein Leichtes, dieses Spiel zu durchschauen.[108] Zentral muss das Wohl des Kindes sein. In diesem Sinne stellt sich insbesondere die Frage der Einwilligung der Minderjährigen in die Bearbeitung dieser Daten. Ein weiterer praktischer Fall besteht in der **Ortung von Arbeitnehmern**. Es gibt Systeme, die es Unternehmen ermöglichen, den geografischen Standort ihrer Beschäftigten zu einem bestimmten Zeitpunkt oder kontinuierlich zu ermitteln, indem der Standort von Gegenständen, die sie mit sich führen (Dienstausweis, Mobiltelefon, usw.) oder benutzen (Fahrzeuge) bestimmt wird. Eine Bestimmung des Standorts von Arbeitnehmern wirft die Frage der Trennungslinie zwischen Arbeits- und Privatleben auf und welchem Grad an Kontrolle und dauerhafter Überwachung ein Arbeitnehmer unterworfen werden darf.[109] Standortdaten über einen Arbeitnehmer dürfen zudem nur so lange gespeichert werden, wie es für den als vorgesehenen Zweck angemessen ist. Dabei sollten zwei Monate nicht überschritten werden. Zentral bei der Nutzung von Standortdaten wie in den angegebenen Beispielen ist die Einwilligung der betroffenen Person und die Informationüber eine solche Bearbeitung, welche im Voraus zu folgen hat.[110] Schliesslich sind die Betreiber elektronischer Kommunikationsnetze und die Anbieter von auf Standortdaten gestützte Dienste darauf hinzuweisen, dass Sicherheitsmassnahmen eingeführt werden müssen, die die Vertraulichkeit und Unversehrtheit der bearbeiteten Daten sicher stellen. Als wichtigster Grundsatz gilt, dass eine solche Bearbeitung von Aufenthaltsinformationen nur dann statt finden sollte, wenn nicht mit einem anderen Mittel oder mit einer anderen Methode derselbe Zweck erreicht werden kann.

Die **Vorratsdatenspeicherung von Verkehrsdaten im Telekombereich** war wiederum[111] ein Thema. Als Massnahme gegen den Terrorismus war durch die EU vorgesehen, dass prinzipiell alle Verbindungs- und Standortdaten, die beim Telefonieren, Versenden von SMS, Emails, Surfen oder Filesharing anfallen, gespeichert werden sollen. Von Datenschutzseite wird kritisiert, dass die Schwelle zum digitalen Überwachungsstaat überschritten wird, wenn über Monate hinweg minutiös nachvollzogen werden kann, wer, wo im Internet gesurft hat, wer, wann, mit wem per Telefon, Handy oder Email kommuniziert hat, wer, wann, welche Onlinedienste in Anspruch genommen hat.[112] Dies führt zu einem Paradigmenwechsel im Strafrecht in Form eines Generalverdachts auch gegenüber Unschuldigen.[113] Der Sinn und Zweck dieser neuen Richtlinie zur Bekämpfung des Terrorismus wird bereits dadurch in Frage gestellt, dass z.B. mit dem Gang zur Telefonzelle das Fahndungsnetz leicht umgangen werden kann. In der erwähnten Stellungnahme wiederholt die Arbeitsgruppe ihre bisherige Meinung und stellt fest, dass der Gegenstand der Richtlinie für alle Bürger von erheblicher Bedeutung ist. Der Richtlinienentwurf stellt Europa vor eine historische Entscheidung, da erstmals europaweit die Pflicht eingeführt werden soll, Milliarden von Daten über die Kommunikationsvorgänge aller Bürger zur Ermittlungszwecken zu speichern. Die Arbeitsgruppe stellt fest, dass heikle Fragen in Bezug auf das Berufs- und/oder Untersuchungsgeheimnis oder

[108] Damit kann den Eltern fälschlicherweise der Eindruck gegeben werden, dass sich das Kind am Ort x befindet, während sich dort nur das Mobiltelefon befindet, das Kind aber am Ort y.

[109] So kann die Bearbeitung von Standortdaten gerechtfertigt sein, wenn sie im Zusammenhang mit der Überwachung der Beförderung von Personen oder Waren oder wenn *sie zur Sicherheit* des Arbeitnehmers selbst oder der in seiner Obhut befindlichen Waren oder Fahrzeuge dient. Dagegen ist eine Bearbeitung von Standortdaten nicht angebracht, wenn Arbeitnehmer ihre Dienstreisen selber organisieren können oder wenn sie nur zu dem Zweck erfolgt, die Arbeit eines Arbeitnehmers zu überwachen, und dies auch mit anderen Mitteln geschehen kann. In jedem Fall darf ein Arbeitgeber keine Standortdaten über einen Arbeitnehmer ausserhalb der Arbeitszeiten erheben. Deshalb ist zu empfehlen, dass Ausrüstungsgegenstände, insbesondere Fahrzeuge, die Arbeitnehmern auch für den privaten Gebrauch zur Verfügung gestellt werden, mit einem System ausgestattet werden, das es dem Arbeitnehmer erlaubt, die Standortbestimmungsfunktion auszuschalten.

[110] Was die Information der betroffenen Person betrifft, müssen die Personen, deren Daten bearbeitet werden, darüber informiert werden, wer für die Verarbeitung verantwortlich ist und zu welchem Zweck die Bearbeitung statt findet. Dazu muss das Recht der Nutzer, ihre Einwilligung jederzeit zurück ziehen zu können, kommuniziert werden. Solche Informationen können entweder in allgemeinen Geschäftsbedingungen für die Nutzung solcher Dienste fest gehalten werden oder unmittelbar bei jeder Inanspruchnahme der *Dienstleistung* erteilt werden. Vgl. oben, 3.2.

[111] Vgl. Tätigkeitsbericht 2004, 7.1.

[112] So Thilo Weichert, Leiter des unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein in einer Pressemitteilung vom 05.12.05.

[113] Diese Massnahmen sind in einem Richtlinienentwurf vorgesehen, der offiziell den Titel der Vorratsspeicherung von Kommunikationsdaten trägt. Der Begriff der Vorratsspeicherung impliziert, dass Daten auf Vorrat gesammelt werden. Dies ist ein eigentlicher Widerspruch gegen das Verhältnismässigkeitsprinzip.

bestimmte Tätigkeiten von unter besonderem rechtlichen Schutz stehenden Institutionen aufgeworfen werden. Obwohl die Gruppe anerkennt, dass Massnahmen gegen terroristische Bedrohungen notwendig sind, stellt sie dennoch in Frage, ob dies der richtige Weg ist. Die Arbeitsgruppe verlangt insbesondere, dass die Verhältnismässigkeit gewahrt wird, um sicher zu stellen, dass die Gesellschaft, die geschützt werden soll, nicht durch unverhältnismässige staatliche Massnahmen untergraben wird. Da der Richtlinienentwurf keine Speicherung von Inhaltsdaten vorsieht, wird gefordert, dass eine scharfe und wirksame Trennung zwischen Inhalts- und Verkehrsdaten sicher gestellt wird; und dies sowohl für den Bereich des Internets[114] als auch für den Bereich der Telefonie.[115] Zudem wird gefordert, dass die zu speichernden personenbezogenen Daten in der Richtlinie konkret aufgeleistet werden müssen. Dabei sind Verkehrsdaten zu nicht zustande gekommenen Kommunikationen nicht in die Richtlinie aufzunehmen. Zentral sind weiters der Zugang bzw. Zugriff zu den Daten die Verwendungszweck und die Schutzmassnahmen. Was den Zugang betrifft, dürfen die genannten Daten nur eigens benannten Strafverfolgungsbehörden im Rahmen der absoluten Notwendigkeit ihrer Arbeit verfügbar gemacht werden. Da sich beim besprochenen Text um einen Richtlinienentwurf handelt, wird dieser auch für Liechtenstein relevant sein, sobald er in den EWR übernommen wird. Bei der Umsetzung der Richtlinie in Liechtenstein wird darauf zu achten sein, dass die Richtlinie minimal umgesetzt wird, um das verfassungsmässige Recht auf Achtung der Privatspähre zu beachten.

Schliesslich ist erwähnenswert, dass sich die Gruppe in einer Stellungnahme zu den künftigen Informationssystemen in Zusammenhang mit **Schengen (SIS II)** und der Erteilung von **Visa (VIS)** äusserte. Da der Bezug zu Liechtenstein aber derzeit (noch) nicht gegeben ist, soll an dieser Stelle ein Hinweis auf die Fundstelle dieser Dokumente genügen.[116]

7.2. VEREINIGUNG DER SCHWEIZERISCHEN DATENSCHUTZBEAUFTRAGTEN

Im Rahmen der Vereinigung der Schweizerischen Datenschutzbeauftragten, in dem der EDSB und die kantonalen DSB vertreten sind, wurde an der Frühjahrstagung über neue Tendenzen des Datenschutzes im Gesundheits- und Sozialversicherungsbereich informiert und eine **«Erklärung zum Datenschutz im Gesundheits- und Sozialversicherungsbereich»** angenommen. In dieser Erklärung[117] wurde mit Besorgnis auf verschiedene Entwicklungen im Gesundheits- und Sozialversicherungsbereich eingegangen und von den Beteiligten verschiedene Massnahmen gefordert. Bekanntermassen stützt sich das Gesundheits- und Sozialversicherungssystem in Liechtenstein auf dem der Schweiz. Es wird wichtig sein zu untersuchen, ob sich dieselben Probleme auch in Liechtenstein stellen und Lösungen aufzuzeigen.[118]

An der Herbsttagung wurde speziell über die Auswirkungen eines Beitritts zu den Abkommen von **Schengen** und **Dublin** informiert. Neben einem gesetzgeberischen Handlungsbedarf wurde dabei festgehalten, dass personelle Veränderungen gerade bei den kantonalen Datenschutzbeauftragten unausweichlich sind. Bei einigen Kantonen war ein Ausbau des Personals bereits ersichtlich oder gar beschlossen. Da der Personalbestand in Liechtenstein mit verschiedenen Kantonen vergleichbar ist, wird bei einem Beitritt Liechtensteins zu Schengen/Dublin ein Personalausbau auch in Liechtenstein unausweichlich sein.

Ausserdem wurde über das **Violent Crime Linkage Analysis System** (ViCLAS) informiert. Dabei geht es um ein Analysesystem, das bei den Kantonspolizeien und seit 2003 auch bei der Landespolizei zur Verknüpfung von Gewaltdelikten gebraucht wird. Dieses polizeiliche Informationssystem soll durch eine weltweit standardisierte Datenerfassung[119] insbesondere überprüfen, ob eine Straftat Teil einer Serie darstellt.

[114] Beschränkung auf Anmelde- und Abmeldedaten oder sonstige Informationen wie Mailserver und Webcash-Protokolle und Aufzeichnungen eines IP-Verkehrs.
[115] Konferenzschaltungen, Fax, SMS, Sprachtelefonie.
[116] Zum Visa-Informationssystem: «Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt»
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_de.pdf
und zum Schengen-Informationssystem: *http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp116_de.pdf.*
Vgl. zum Ganzen auch Tätigkeitsbericht 2004, 7.1.
[117] *http://www.dsb-cpd.ch/d/publikationen/050609.pdf.*
[118] Vgl. oben, 4.1.
[119] ViCLAS ist in verschiedenen Staaten in Europa im Einsatz. Die relevanten Daten werden mittels eines 168 Fragen umfassenden Erhebungsbogens erfasst.

Erfasst werden u.a. alle ungeklärten Tötungsdelikte, alle geklärten Tötungsdelikte mit sexuellem oder unbekanntem Motiv, bestimmte sexuelle Gewaltdelikte unter Anwendung oder Androhung von Gewalt, verdächtiges Ansprechen von Kindern und Jugendlichen, wenn ein sexuelles Motiv vermutet werden kann und mögliche konkrete Anhaltspunkte für eine geplante schwerwiegende Straftat vorliegen.

Aus Sicht des Datenschutzes wurde die Nützlichkeit eines solchen Systems akzeptiert. Doch wurden auch Fragen zur Rechtsgrundlage und insbesondere zum Umstand gestellt, dass auch strafrechtlich nicht relevante Verhaltensweisen wie Voyeurismus und Exhibitionismus erfasst werden.

Schliesslich wurde auch an der Arbeitsgruppe **«Einwohnerkontrollen»** teilgenommen. Dabei kam man zur Feststellung, dass sich zahlreiche Fragen stellen (von den Rechtsgrundlagen bis zur Praxis). Eine Fortsetzung dieser Tätigkeit war bei Jahresende noch offen, da sich die Sache als sehr komplex erwies. Dennoch konnten verschiedene Schlussfolgerungen für Liechtenstein gezogen werden: So wurde unter anderem eine Anpassung des Gemeindegesetzes initiiert, damit die Praxis der Einwohnerkontrollen und der Datenbearbeitungen durch die Gemeinden allgemein auf eine rechtliche Basis gestellt werden kann.[120]

7.3. EUROPARAT

Nach dem allgemeinen Arbeitspapier zur Biometrie und einer Stellungnahme zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel durch die Art. 29 Arbeitsgruppe[121] nahm auch der Datenausschuss des Europarats ein Dokument zum Thema Biometrie an.[122] Daneben wurde die Arbeit an einem Dokument über die Anwendung von Grundsätzen des Datenschutzes auf das **Internet** fortgesetzt und die Ergebnisse einer Konferenz über die **Rechte und Verantwortlichkeiten** von Betroffenen diskutiert.

7.4. EUROPÄISCHE DATENSCHUTZKONFERENZ

An der jährlich stattfindenden **Europäischen Datenschutzkonferenz** ging es um Themen wie die Bewusstseinsbildung in Bezug auf den Datenschutz, die Möglichkeit der Einsetzung betrieblicher Datenschutzbeauftragter,[123] einer ersten Bilanzziehung nach 10 Jahren der DS-Richtlinie und andere Themen. Die Teilnahme an einer solchen Konferenz ermöglicht es immer wieder, sich über aktuelle Trends und Probleme zu informieren und Gedanken auszutauschen. Dies ist gerade in Liechtenstein wichtig, da es keine Ansprechspartner in diesem Sinne gibt.

7.5. INTERNATIONALE DATENSCHUTZKONFERENZ

An dieser Konferenz, an der jährlich neben Datenschutzbehörden auch viele Vertreter der Privatwirtschaft teilnehmen, wurden Themen behandelt wie Datenschutz und Terrorismusbekämpfung, Datenschutz auf dem Internet oder die Wirtschaft im Dschungel datenschutzrechtlicher Bestimmungen.

Die Konferenz nahm u.a. eine Resolution zur Verwendung der **Biometrie** in Pässen, Identitätskarten und Reisedokumenten an. Darin wird insbesondere darauf hingewiesen, dass biometrische Daten nur mit Kenntnis der betroffenen Person gesammelt werden sollten. Zudem machen biometrische Daten wegen ihrer Einmaligkeit den menschlichen Körper «maschinenlesbar». Dadurch besteht die Gefahr, dass biometrische Daten, als weltweit einheitlicher Identifikator benutzt werden könnten. Gefordert werden wirksame technische Schutzmassnahmen und eine zweckgebundene Datenbearbeitung der biometrischen Daten.

[120] Vgl. oben, 5.1.2.
[121] *http://www.llv.li/pdf-llv-sds-biometrie_wp80_de.pdf. und vgl. Tätigkeitsbericht 2004, 7.1.*
[122] Dieser Bericht ist verfügbar unter: *http://www.llv.li/pdf-llv-sds-t-pd_2005_biom0e-1.pdf.*
[123] Ein solch betrieblicher DSB sollte auch unabhängig sein und entweder im Unternehmen selbst oder extern von diesem angestellt sein. Mit dieser Institution werden behördliche DSB entlastet und das «Netz» von Datenschützern erweitert. Deutschland, Schweden, Frankreich, die Niederlande, Luxemburg und auch die Schweiz haben diese sinnvolle Institution eingeführt.
[124] Vgl. zum Thema Biometrie auch oben, 4.4. und 7.1.

8. Personelles und Organisatorisches

Die personelle Situation hat sich seit Anfang Juli dahin gehend verbessert, als der SDS seither ein unbefristetes Teilzeitsekretariat zur Verfügung steht. Damit konnte ein wichtiger Schritt erreicht werden, der zum Funktionieren der Stabsstelle einen wichtigen Beitrag leistet. Dennoch ist die Personalsituation weiterhin ungenügend: Laut einer Untersuchung im Rahmen der Europäischen Datenschutzkonferenz ist Liechtenstein das einzige Land in Europa (und nicht nur innerhalb des EWR), das über eine einzige Person verfügt, welche für inhaltliche Fragen zuständig ist. So verfügt z.B. Monaco über sieben Vollzeitbeschäftigte.[125] Es fehlt weiterhin an einem Stellvertreter, der den DSB bei Abwesenheit vertritt. Vor diesem Hintergrund ist auch erklärbar, wieso auch nach dem dritten vollständigen Berichtsjahr verschiedene allgemeine Informationsbroschüren noch nicht abgeschlossen werden konnten. Ein mangelndes Bewusstsein in der Öffentlichkeit für den Schutz der Privatsphäre ist mit Sicherheit auch auf diesen Umstand zurück zu führen. Unter den gegebenen Umständen ist eine Wahrnehmung der gesetzlichen Aufgaben nicht möglich.[126] Dies ist gerade im privaten Sektor störend, da dort Daten kommerziell, und teils ohne Kenntnis der Betroffenen und/oder zu deren Nachteil bearbeitet werden. Beim gegebenen Personalstand wird das verbindliche DSG zu einem Instrument der blossen Selbstregulierung degradiert.

Zum Thema **Datenschutzberater**[127] kann erwähnt werden, dass sich die Landespolizei (LP), das Ausländer- und Passamt (APA) und das Amt für Personal und Organisation (APO), unter Betonung ihrer beschränkten Ressourcen, bereit erklärten, einen solchen vorzusehen.

[125] Vgl. Österreichische Datenschutzkommission: Datenschutzbericht 1. Januar 2002 bis 30. Juni 2005, Seite 12, abrufbar unter: *http://www.dsk.gv.at/*.
[126] Daran ändert auch der Umstand nichts, dass ab Oktober bis Ende 2005 eine befristet angestellte Aushilfe zur Verfügung steht.
[127] Vgl. Tätigkeitsbericht 2004, 8.

9. Ausblick

Die Vorhaben, die für 2005 als prioritär qualifiziert wurden und nicht abgeschlossen werden konnten sind als Aufgaben für 2006 zu übernehmen. Es geht dabei um Folgendes:

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

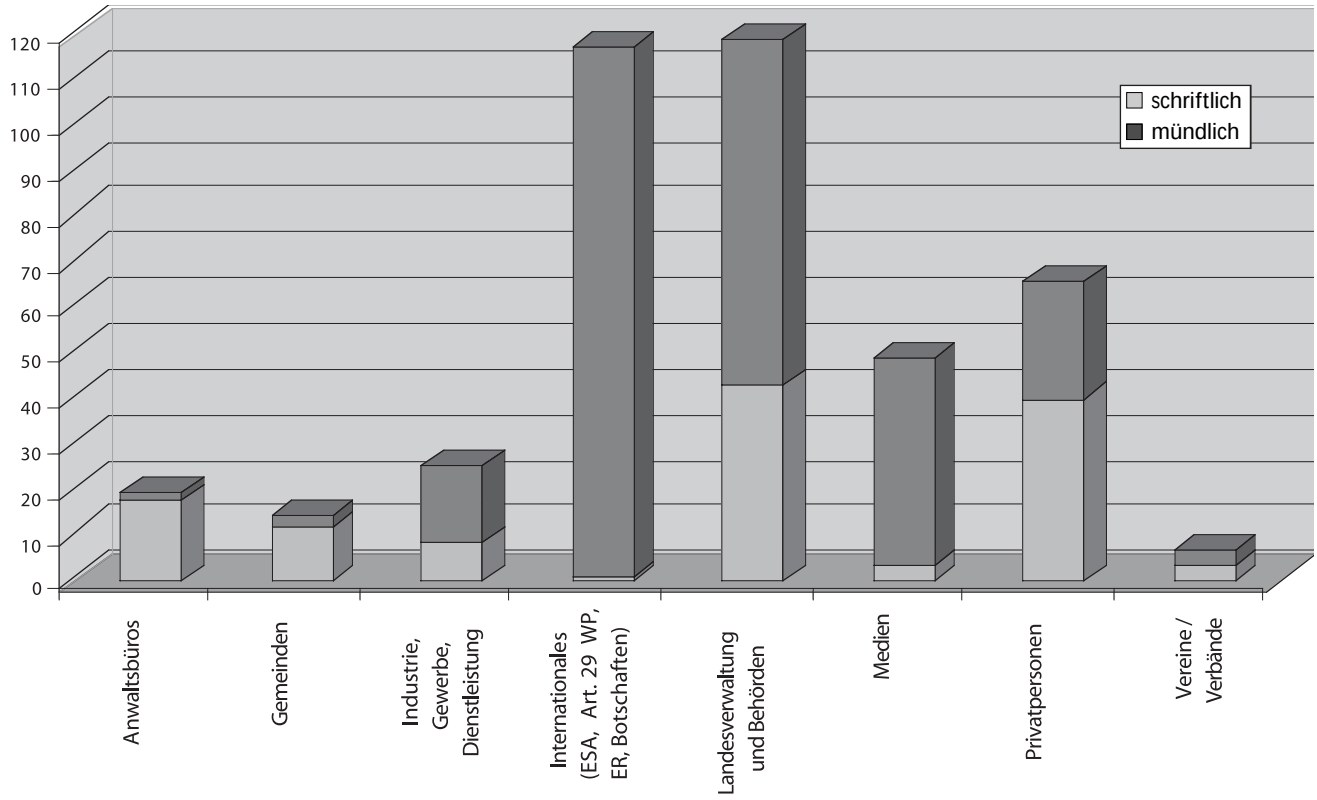
NEUE PRIORIÄTEN FÜR 2006:

Die Information der Öffentlichkeit zu Themen, welche für den Schutz der Privatsphäre wichtig sind muss fortgesetzt und intensiviert werden. In diesem Sinne soll die Internetseite der SDS ausgebaut werden.

Eine Festlegung weiterer Prioritäten für 2006 ist angesichts der gegebenen Personalsituation schwierig. Da zudem die Erfahrung gezeigt hat, dass sich auch grössere Vorhaben kurzfristig abzeichnen können, soll an dieser Stelle auf eine Erwähnung zusätzlicher prioritärer Aktivitäten verzichtet werden.

Anhang

ANFRAGEART



GESETZESTHEMEN

	Anwalts-büros	Gemein-den	Industrie, Gewerbe, Dienst-leistung	Internatio-nales (ESA, Art. 29 WP, ER, Bot-schaften)	Landesver-waltung und Behörden	Medien	Privatper-sonen	Vereine / Verbände	Gesamt-ergebnis
Anmeldung, Datensammlungen					1		1		2
Auskunftsrecht					2		4		6
Datenbekanntgabe	5	13	4		65	1	26	2	116
DS Allgemein	9	1	12	116	30	34	29	5	236
Gesetzesvorlagen					10				10
Internationales (Ausser Übermittlungen ins Ausland)					1				1
Sicherheit	1		2	1	8		6		18
Übermittlungen ins Ausland	4		4		2	1			11
Überwachung am Arbeitsplatz	2					13			13
GESAMTERGEBNIS	**19**	**14**	**25**	**117**	**119**	**49**	**66**	**7**	**416**

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