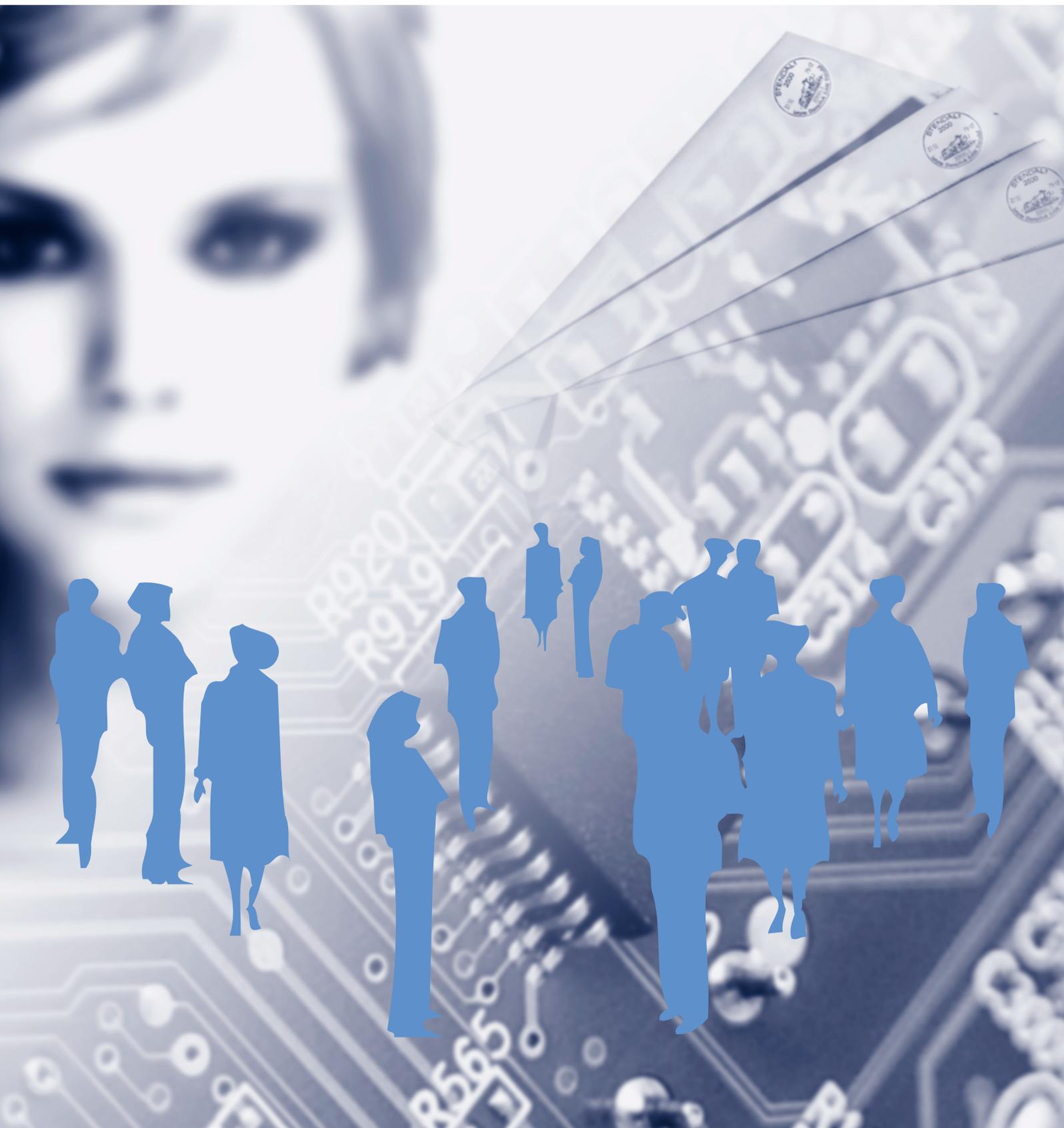


# Tätigkeitsbericht

Datenschutzbeauftragter des Fürstentums Liechtenstein

# 2004



# Inhaltsverzeichnis

<b>1. Vorwort</b> .....	<b>3</b>
<b>2. Allgemeines und Prioritäten</b> .....	<b>5</b>
<b>3. Information</b> .....	<b>6</b>
3.1. Informationspflichten des DSB .....	6
3.2. Informationspflichten von Dateninhabern .....	6
<b>4. Beratung</b> .....	<b>8</b>
4.1. Unterstützung von privaten Personen und Behörden durch allgemeine Orientierungen und Beratungen .....	8
4.2. Stellungnahmen zu Datenschutzfragen in hängigen Verfahren vor Rechtsmittelbehörden – Rechtsprechung zum DSG .....	8
4.3. Begutachtung der Gleichwertigkeit des ausländischen Datenschutzes .....	9
4.4. Stellungnahme zu Vorlagen und Erlassen .....	10
<b>5. Aufsicht</b> .....	<b>11</b>
5.1. Aufsicht über Behörden .....	11
5.1.1. <i>Datenschutzwidrige Bearbeitungen</i> .....	12
5.1.2. <i>Gesetzliche Grundlagen</i> .....	13
5.2. Abklärungen und Empfehlungen im Privatrechtsbereich .....	13
<b>6. Register der Datensammlungen</b> .....	<b>15</b>
<b>7. Internationales</b> .....	<b>16</b>
7.1. Artikel 29 Arbeitsgruppe der Richtlinie 95/46/EG .....	16
7.2. Vereinigung der Schweizerischen Datenschutzbeauftragten .....	19
7.3. Europarat .....	19
7.4. Europäische Datenschutzkonferenz .....	20
7.5. Internationale Datenschutzkonferenz .....	20
<b>8. Personelles</b> .....	<b>21</b>
<b>9. Ausblick</b> .....	<b>22</b>
<b>Anhang</b> .....	<b>23</b>



# 1. Vorwort

Der zweite Tätigkeitsbericht des Datenschutzbeauftragten (DSB) liegt hiermit vor. Das zweite Jahr nach Inkrafttreten des Datenschutzgesetzes (DSG) vom 14. März 2002, LGBl. 2002 Nr. 55, war durch zahlreiche Aktivitäten vor allem in der Liechtensteinischen Landesverwaltung geprägt. Die organisatorische Einbettung der Stabsstelle für Datenschutz (SDS) in der Landesverwaltung ermöglicht es, dass auf kurze und gut funktionierende Informationskanäle gebaut werden kann. Allgemein kann bereits nach dem zweiten Jahr gesagt werden, dass in Sachen Datenschutz einiges in der Landesverwaltung erreicht wurde.

Auch im zweiten Tätigkeitsjahr konnte die Öffentlichkeit nicht in einem befriedigenden Ausmass über den Datenschutz allgemein oder die Rechte der Einzelnen informiert werden (dazu unten, 3.1.). Noch wird der Datenschutz etwa als störend angesehen, der Einiges komplizierter mache und schliesslich auch nichts bringe, da man ja nichts zu verstecken habe. Ist dem wirklich so? Die einfache Antwort darauf lautet kurz und einfach «nein». Es braucht nicht unbedingt Horrorszenerien à la «1984», um die Nützlichkeit des Schutzes des Privatlebens, und darum geht es schlussendlich beim Datenschutz, aufzuzeigen. Dazu eine Frage: Ist Datenschutz wirklich etwas Neues in Liechtenstein? Auch hier lautet die Antwort «nein». Das Bankgeheimnis ist das wohl prominenteste und wirtschaftlich bedeutendste Beispiel für den Datenschutz im Land. Man denke auch an das Geheimnis der Stimmabgabe bei Wahlen, das Arzt-, Anwalts- oder Steuergeheimnis. Was dagegen mit dem DSG neu geschaffen wurde ist ein allgemeiner Rahmen für all diese Spezialfälle sowie die Institution des DSB, dem die Aufgabe zukommt, darauf zu achten, dass die gesetzlichen Bedingungen eingehalten werden.

Die Datenschutzkommission entschied in einem ersten Fall, der ihr vorgelegt wurde, im Sinne des Datenschutzes. Damit dürfen Baubewilligungen, die von den Gemeinden genehmigt wurden, nicht mehr im bisherigen Ausmass veröffentlicht werden (dazu unten, 4.2.).

Ein Thema, das auch 2004 im Zentrum der Tätigkeiten stand, betrifft die Zentrale Personenverwaltung (ZPV), die bei der Landesverwaltung dazu dient, administrative Abläufe zu erleichtern. Diese vor allem die ganze ständige Bevölkerung mit zahlreichen Angaben umfassende Datenbank ist wie ein Mosaik aus verschiedensten Daten zusammengesetzt, die von verschiedenen Amtsstellen eingegeben werden. Die ZPV gilt als ein zentrales Arbeitsinstrument in der Landesverwaltung.

Dieser Datenbank fehlt bisher eine rechtliche Grundlage. Immerhin wurde die Notwendigkeit der Zugriffsberechtigungen der einzelnen Amtsstellen auf die einzelnen Datenfelder überprüft (dazu unten, 5.1.1.1.).

Auch an internationalen Themen, die sich auf Liechtenstein auswirken, konnte mitgearbeitet werden. Das Bestehen eines internationalen Netzwerks kann gerade für ein kleines Land wie Liechtenstein nicht genug betont werden. Denn wie im Bericht gezeigt wird, stellen sich in verschiedenen Ländern ähnliche Probleme (dazu unten, 7.1 bis 7.5.).

Mit den Anschlägen des 11. September 2001 hat sich die Welt verändert. Das darf aber nicht dazu führen, dass unter dem Deckmantel der Terrorismusbekämpfung Neuerungen eingeführt werden, die zur Erreichung des angegebenen Zieles fragwürdig sind (dazu unten, 7.1.).

Die rasche Aufklärung der Tötung des bayrischen Modemachers Mooshammer weckt Begehrlichkeiten zur Erweiterung von staatlichen DNA-Datenbanken. Dass es bei der DNA oder bei biometrischen Daten wie Fingerabdrücken oder der Iriserkennung um höchstpersönliche Merkmale geht, ist Vielen wahrscheinlich unbewusst, weshalb die Gefahren nicht gesehen werden. Diese aufzuzeigen ist nicht zuletzt Aufgabe der Datenschutzbehörden. Deshalb wird im dritten Tätigkeitsjahr mehr darauf zu achten sein, dass das Bewusstsein für den Datenschutz in Liechtenstein gefördert wird.

Gefahren einer anderen Dimension bestehen im Rahmen der zunehmenden Datenverarbeitung in der Privatwirtschaft. Data Mining, Kundenkarten, Adresshandel. Dies nur als einige Stichworte dazu, dass in der Privatwirtschaft oft unbemerkt Kundenprofile aufgestellt und ausgewertet werden. Möglichkeiten der Überwachung sind damit gegeben. Ebenso werden vermehrt biometrische Daten verwendet und dies nicht nur zu Zwecken der Strafverfolgung, sondern auch in der Privatwirtschaft. Dabei geht es oft um unverhältnismässiges Handeln. So ist die Verwendung des Fingerabdrucks für den Zugang von Kindern zu einer Schulmensa ebenso unangemessen wie wenn in einem Lebensmittelgeschäft per Fingerabdruck oder in einem Beach Club mittels eines in die Schulter eingepflanzten Chips gezahlt wird. Das Besorgniserregende an diesen Beispielen ist der unbedachte Umgang mit persönlichen Daten, die teils höchst sensibel sind. Oder wie vor einiger Zeit in einer deutschen Zeitung zum Thema Kundenkarten treffend zu lesen war: Abends im Schlafzimmer fürchtet man sich vor

Spannern und zieht die Vorhänge zu. An der Ladentheke werden dagegen viele zu Exhibitionisten. Kritisch ist dies auch, da zunehmend die Wirtschaft Daten ohne Kenntnis der Betroffenen verarbeitet und kommerziell nutzt. Kurz: es geht um die Verhältnismässigkeit.

Ebenso wird es eine wichtige Aufgabe sein, im Zusammenhang mit wichtigen Themen wie den datenschutzrechtlichen Fragen zur Einführung des Tarmed oder der Schaffung einer rechtlichen Grundlage für die ZPV voranzukommen. Auch bei einem möglichen Beitritt Liechtensteins zu Schengen/Dublin, der nach der erfolgreichen Abstimmung in der Schweiz wahrscheinlicher geworden ist, stellen sich neue Aufgaben, die dazu dienen, das verfassungsmässige Recht auf Achtung der allzu oft bedrohten Privatsphäre zu sichern.

Vaduz, im Juni 2005

*Dr. Philipp Mittelberger*  
*Datenschutzbeauftragter*

# 2. Allgemeines und Prioritäten

Im ersten Tätigkeitsbericht wurden folgende Prioritäten für 2004 festgelegt:

- Abschluss des Aufbaus und Veröffentlichung des Registers;
- Überprüfung der Datenbank «Zentrale Personenverwaltung» (ZPV) auf Datenschutzkonformität;
- Durchführung einer verwaltungsinternen Schulungsveranstaltung über den Datenschutz und möglicherweise ein Angebot für die Öffentlichkeit;
- Erstellung einer Broschüre «Datenschutz in der Schule»;
- Vermehrte Stellungnahmen zu Gesetzesvorhaben, insbesondere im Rahmen von Vernehmlassungsverfahren;
- Ständiger Ausbau und Aktualisierung der Internetseite als Informationsinstrument für die Öffentlichkeit.

Das Ziel der vermehrten **Stellungnahmen im Rahmen von Vernehmlassungsverfahren** wurde mit 23 Stellungnahmen im Vergleich zu acht im Jahr 2003 klar erreicht.

Auch der ständige Ausbau und die Aktualisierung der **Internetseite** der Stabsstelle für Datenschutz erfolgte plangemäss.<sup>1</sup>

Die folgenden Vorhaben konnten nicht abgeschlossen werden:

Der Aufbau des **Registers der Datensammlungen**<sup>2</sup> ist zwar abgeschlossen; doch ist das Register noch nicht auf der Inter-

netseite der Stabsstelle für Datenschutz einsehbar. Obwohl die rechtlichen Grundlagen dazu inzwischen geschaffen wurden,<sup>3</sup> konnten die technischen Vorbereitungen noch nicht abgeschlossen werden.

Die Überprüfung der Zugriffe diverser Amtsstellen auf Felder der **ZPV** im Hinblick auf **Datenschutzkonformität** wurde ebenfalls verzögert. Dies hat auch damit zu tun, dass bis Ende Jahr nicht alle Rückmeldungen der Amtsstellen vorlagen.

Eine verwaltungsinterne **Schulungsveranstaltung** konnte aus Termingründen nicht durchgeführt werden. Eine Veranstaltung für die Öffentlichkeit scheiterte an den Ressourcen.

Es ist noch offen, ob die Erstellung einer Broschüre «**Datenschutz in der Schule**», welche die bestehenden Texte der kantonalen Datenschutzbeauftragten des Kantons Zug<sup>4</sup> und Baselland<sup>5</sup> ergänzen und erweitern soll, abgeschlossen wird.

Insgesamt wurden die als prioritär qualifizierten Vorhaben nicht in einem befriedigenden Ausmass umgesetzt. Dafür gibt es verschiedene Gründe, die teils bei der Stabsstelle für Datenschutz, teils bei anderen Beteiligten liegen. Auf Prioritäten für 2005 wird am Ende des Berichtes eingegangen.

<sup>1</sup> Vgl. unten, 3.1.

<sup>2</sup> Vgl. dazu unten, 6.

<sup>3</sup> Vgl. unten, 4.4.

<sup>4</sup> [http://www.llv.li/pdf-llv-sds-schule\\_leitfaden.pdf](http://www.llv.li/pdf-llv-sds-schule_leitfaden.pdf)

<sup>5</sup> <http://www.baselland.ch/docs/jpd/ds/prak/prak-019.pdf>

# 3. Information

## 3.1. INFORMATIONSPFLICHTEN DES DSB

Wie schon angetönt, konnte auch im zweiten Berichtsjahr auf Grund der mangelnden Ressourcen keine grössere Veranstaltung durchgeführt werden, um die Öffentlichkeit über ihre Rechte und aktuelle Themen zu informieren. Eine solche Information war lediglich punktuell und in kleineren Kreisen möglich.

Deshalb wurde diese gesetzliche Aufgabe der Information der Öffentlichkeit über Fälle von allgemeinem Interesse<sup>6</sup> vor allem über einen relativ regelmässigen Ausbau der **Internetseite** der Stabsstelle wahrgenommen. Damit wurde über aktuelle und/oder wichtige Themen informiert. Dabei werden bereits auf der Startseite die **Rechte des Einzelnen nach dem Datenschutzgesetz** genannt.

Von diesen Themen sind vor allem die Folgenden kurz zu nennen:

**Datenschutz in der Schule:**<sup>7</sup> hier wurden vor allem datenschutzrechtliche Aspekte erörtert, die auftauchen, wenn eine Schule ans Internet angeschlossen wird; **datenschutzgerechtes eGovernment:**<sup>8</sup> hier geht es um Themen wie datenschutzgerechte Eingaben des Bürgers an die Verwaltung oder die Frage, inwiefern Identifizierungsdaten von Verwaltungsangestellten auf der Internetseite einer Verwaltungsstelle zu veröffentlichen sind; **Sicherheit im Internet:** diese Problematik ist allgemein bekannt. Der offene Raum des Internets ist unsicher. Es bestehen verschiedene Möglichkeiten, sich zu schützen; **Kinder und Internet:** Auch hier geht es um Gefahren und Möglichkeiten, wie man Kinder beim Umgang mit dem Internet am Besten schützen kann; **Spam-Mails:**<sup>9</sup> die Plage der Spam-Mails ist auch bekannt. Ein Dokument der Europäischen Kommission stellt geplante Massnahmen vor; **Videoüberwachung:**<sup>10</sup> die Videoüberwachung ist ein Mittel, auf das häufig zurück gegriffen wird, um Eigentum zu schützen. Damit Videoüberwachung überhaupt erlaubt ist, müssen verschiedene Voraussetzungen erfüllt sein; **Bearbeitung genetischer Daten:** genetische Daten sind Gesundheitsdaten und somit als besonders schützens-

werte Daten einzustufen, für deren Bearbeitung ein gewisser Rahmen zu beachten ist;<sup>11</sup> **Ergänzungen zu den Richtlinien für Datenbekanntgabe der Einwohnerkontrollen:** die ursprünglich erstellten Richtlinien durch die Stabsstelle für Datenschutz erwiesen sich als zu allgemein. Auf Grund verschiedener Nachfragen wurden dieselben ergänzt.

Daneben wurde über die folgenden für Liechtenstein wichtigen Gegebenheiten informiert:

- Ratifikation und Inkrafttreten des Europaratsabkommens,
- Tätigkeitsbericht des Datenschutzbeauftragten (DSB),
- Inkrafttreten des revidierten Datenschutzgesetzes,
- Inkrafttreten der revidierten Datenschutzverordnung,
- Entscheidung der Datenschutzkommission.<sup>12</sup>

Anlässlich einer Informationsveranstaltung der Sektion Informatik und Büromatik der Gewerbe- und Wirtschaftskammer (GWK) zum Thema **Internetsicherheit** wurde die Stabsstelle für Datenschutz angefragt, einen Beitrag zum Thema zu verfassen. Ein Auszug aus diesem schriftlichen Beitrag wurde in der Folge auf der Internetseite der Stabsstelle verfügbar gemacht.<sup>13</sup>

## 3.2. INFORMATIONSPFLICHTEN VON DATENINHABERN

In einem Richtungsweisenden Urteil schuf das deutsche Bundesverfassungsgericht bereits im Jahre 1983 das **«Recht auf informationelle Selbstbestimmung»**. Nach diesem Urteil, das internationale Anerkennung fand, umfasst das Recht auf Datenschutz das Recht jeder Person, selbst bestimmen zu können *«wer was wann und bei welcher Gelegenheit über sie weiss.»*<sup>14</sup> Eine Bedingung der Ausübung dieses Rechtes ist eine vorgängige Information der betroffenen Personen darüber, dass ihre Daten bearbeitet werden. Aus Gründen der Fairness und der Rechtmässigkeit der Datenerhebung soll die betroffene Person bestimmte Informationen erhalten, die es ihr ermöglichen, die Lage einzuschätzen und ihr Verhalten vernünftig zu bestimmen.<sup>15</sup> In diesem Sinne bestimmt das DSG, dass der betroffenen Person vom Inhaber der Datensammlung zumindest

<sup>6</sup> Vgl. Art. 31 Abs. 2 DSG.

<sup>7</sup> [http://www.llv.li/llv-sds-spezialthemen-datenschutz\\_in\\_der\\_schule.htm](http://www.llv.li/llv-sds-spezialthemen-datenschutz_in_der_schule.htm)

<sup>8</sup> <http://www.llv.li/llv-sds-spezialthemen-egovernment.htm>

<sup>9</sup> Vgl. zu den letzten drei genannten Themen: <http://www.llv.li/llv-sds-spezialthemen-informationssicherheit-internetsicherheit.htm>

<sup>10</sup> <http://www.llv.li/llv-sds-spezialthemen-videoeuberwachung.htm> und unten, 7.1.

<sup>11</sup> Vgl. zu Spam-Mails, Videoüberwachung und Bearbeitung genetischer Daten weiter unten, 7.1.

<sup>12</sup> Vgl. unten, 4.2.

<sup>13</sup> Vgl. [http://www.llv.li/pdf-llv-sds-zusammenfass\\_internesicherheit.pdf](http://www.llv.li/pdf-llv-sds-zusammenfass_internesicherheit.pdf)

<sup>14</sup> BVerfGE 65, 1 – Volkszählung: <http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm>

<sup>15</sup> Vgl. Ulrich Dammann / Spiros Simitis, EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997, Randnummer 1 zu Artikel 10 der Richtlinie 95/46/EG.

die Identität des Inhabers (das heisst die Person, die ihre Daten bearbeitet) und der Zweck der Bearbeitung zu erteilen ist, sofern ihr diese Informationen noch nicht vorliegen.<sup>16</sup> Diese Informationspflicht von Dateninhabern ist ein Kernstück des Datenschutzes, das Wesentliche zur Verwirklichung des Rechtes auf informationelle Selbstbestimmung beiträgt.

Dieses wichtige Recht, das für den Bearbeiter eine gesetzliche Informationspflicht darstellt, soll im Folgenden an **konkreten Fällen** erläutert werden:

Der DSB wurde darauf aufmerksam gemacht, dass ein Optikergeschäft den Inhaber gewechselt hatte, die Kunden jedoch nicht über diesen Umstand informiert wurden. Datenschutzrechtlich wechselte durch diese Geschäftsübernahme der Inhaber der Kundendaten. Wie oben dargelegt, hätten die betroffenen Personen über den Geschäftswechsel informiert werden müssen und dies zum Voraus. Dies umso mehr, als es sich um ein Optikergeschäft handelte, das naturgemäss Gesundheitsangaben bearbeitet, die nach dem DSG als besonders schützenswert gelten.

Dieses Beispiel ist nur eines von vielen anderen: Man denke nur an das Anbringen von Hinweistafeln bei der Installation von **Videokameras**, der «**Erstklässleraktion**» der Landeszeitungen,<sup>17</sup> **Datenschutzhinweise auf Internetseiten** oder die **Übermittlung von Flugpassagierdaten in die USA**.<sup>18</sup>

Ziel ist, wie angetönt, die Verwirklichung von Transparenz gegenüber den betroffenen Personen, damit diese selbst über ihre Daten bestimmen können. Oft wird dieser Pflicht in der Privatwirtschaft dadurch nachgekommen, dass die Allgemeinen Geschäftsbedingungen (AGBs) einen Hinweis auf die stattfindende Datenbearbeitung enthalten.<sup>19</sup> Solche Hinweise sind aber nicht immer so aussagekräftig wie es das DSG wünscht. Wenn der Kunde trotz unpräzise formulierter AGBs eine Geschäftsbeziehung mit dem betreffenden Unternehmen eingeht, heisst dies aber nicht unbedingt, dass er seine Einwilligung zu einer Datenbearbeitung gegeben hat.<sup>20</sup>

Grenzen für diese Informationspflicht werden einzig da gesetzt, wo es um Zwecke der Statistik oder der historischen oder wissenschaftlichen Forschung geht, wenn die Information der betroffenen Person unmöglich ist, unverhältnismässigen Aufwand erfordert oder die Speicherung oder Weitergabe gesetzlich ausdrücklich<sup>21</sup> vorgesehen ist.<sup>22</sup>

<sup>16</sup> Vgl. Art. 5 DSG und 10f. der Richtlinie 95/46/EG.

Wurden die Daten nicht bei der betroffenen Person erhoben, so sind ihr nach Art.5 Abs. 3 die Angaben gemäss Abs. 1 vom Inhaber bei Beginn der Speicherung der Daten bzw. im Fall einer beabsichtigten Weitergabe der Daten an Dritte spätestens bei der ersten Bekanntgabe zu erteilen.

<sup>17</sup> Vgl. unten, 5.2.

<sup>18</sup> Zur Anbringung von Hinweistafeln bei stattfindender Videoüberwachung vgl. Tätigkeitsbericht 2003, 4.2 und zu den beiden letztgenannten Fällen, unten, 7.1.

<sup>19</sup> Zu den AGBs der Lie-Card vgl. unten, 5.2.

<sup>20</sup> Ein Beispiel von ausführlichen AGBs, die teilweise mit der Stabsstelle für Datenschutz abgesprochen wurden: [http://www.inode.li/unternehmen\\_agb.html](http://www.inode.li/unternehmen_agb.html)

<sup>21</sup> Das bedeutet, dass die gesetzliche Bestimmung gewissen Anforderungen hinsichtlich ihres Inhalts und ihrer Präzision genügen muss. Mit anderen Worten genügt die Existenz von gesetzlichen Bestimmungen als Information der betroffenen Personen nur, wenn diese Bestimmungen eine vergleichbare Transparenz schaffen (vgl. *Ulrich Dammann / Spiros Simitis*, EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997, Randnummer 7 zu Artikel 11 der Richtlinie 95/46/EG).

<sup>22</sup> Vgl. Art. 5 Abs. 4 DSG.

# 4. Beratung

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

Während 2003 insgesamt 243 Anfragen registriert wurden beläuft sich diese Anzahl für 2004 auf 378.<sup>23</sup> Dies macht eine Steigerung von 56% aus. Davon stammten 178 von den Gemeinden, die fast alle die Datenbekanntgabe betrafen.<sup>24</sup> Von diesen 378 Anfragen wurden 68 mündlich und 297 schriftlich eingereicht. Die schriftlichen Anfragen reichen von kurzen Anfragen per Email bis zu Anfragen der Regierung, z.B. im Rahmen von Vernehmlassungsverfahren.

Eine Darstellung sämtlicher Anfragen sowie der Antworten würde den Rahmen dieses Berichtes sprengen. Erwähnt sei an dieser Stelle immerhin das breite Spektrum der Anfragen: Neben allgemein bedeutenden Anfragen wie z.B. zur Zulässigkeit der Überwachung des Arbeitnehmers am Arbeitsplatz,<sup>25</sup> der Bearbeitung von Personalakten<sup>26</sup> oder der Zulässigkeit eines Krebsregisters in Liechtenstein wurden andere Fragen gestellt wie die Zulässigkeit des Einstellens von Personendaten auf verschiedene Internetseiten, der Bekanntgabe von Elternnamen von Kindergartenkindern an andere Eltern bis zur Bekanntgabe von Autohaltern an Privatpersonen im Ausland.

Auf einzelne bedeutendere Anfragen z.B. im Rahmen von Vernehmlassungsvorlagen wird weiter unten eingegangen.<sup>27</sup>

Speziell sei noch Folgendes erwähnt: In der Schweiz wurde ab Anfang 2004 ein neuer Arzttarif eingeführt (**Tarmed**). Aus Datenschutzsicht wurde vor allem die systematische Weitergabe von Diagnosen durch die Leistungserbringer an die Krankenkassen bemängelt. Der Eidgenössische Datenschutzbeauftragte (EDSB) stellte fest, dass das Krankenversicherungsgesetz eine solch systematische Bekanntgabe nicht vorsieht<sup>28</sup> und dass demgemäss eine nicht verhältnismässige Datenbearbeitung gegeben sei.

Ein Regierungsbeschluss von Dezember 2003 sah vor, dass dieser Tarif auch in Liechtenstein eingeführt werden sollte. Das mit

der Umsetzung des Regierungsbeschlusses beauftragte Ressort Gesundheit wurde schon früh auf die sich stellenden Datenschutzfragen in der Schweiz hingewiesen. Zudem wurde vorgeschlagen, eine Lösung im Sinne einer **Anonymisierung oder Pseudonymisierung** zu suchen. Denn von Seite der Krankenkassen wird geltend gemacht, die Daten über die Patienten würden sie kaum interessieren. Ihr gesetzlicher Auftrag bestehe in einer Überprüfung insbesondere der wirtschaftlichen Behandlung durch die Leistungserbringer. Dazu ist es aber in der Tat nicht nötig zu wissen, ob ein Patient z.B. an AIDS erkrankt ist. Im Gegenteil, eine so heikle Information kann sich gerade in so kleinen Verhältnissen, wie sie in Liechtenstein bestehen, sehr rasch zum Nachteil des Patienten auswirken, wenn dies ohne dessen Willen bekannt wird. Im November 2004 beschloss die Regierung, die Einführung des Tarmed um ein Jahr zu verschieben. Damit wurde aus Sicht des Datenschutzes Zeit gewonnen, damit eine Lösung gefunden werden kann.

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

2004 erfolgte keine Stellungnahme zu einem hängigen Verfahren.

Dennoch wurde die Rechtslage zum Datenschutz in Liechtenstein etwas geklärt und schliesslich auch gestärkt, indem die Datenschutzkommission (DSK) eine Empfehlung des DSB an die Gemeinden stützte und entschied, dass die liechtensteinischen Gemeinden in Zukunft genehmigte Baubewilligungen nicht mehr ohne weiteres bekannt geben dürfen. Vielmehr sind die Bedingungen des DSG einzuhalten.<sup>29</sup>

Der DSB hatte den Gemeinden empfohlen, die generelle Veröffentlichung von Baubewilligungen zu unterlassen. Nachdem die Konferenz der Gemeindevorsteher diese Empfehlung nicht angenommen hatte, wurde die Angelegenheit der DSK zur Entscheidung vorgelegt. Dabei ging es im Einzelnen um Folgendes:

<sup>23</sup> Vgl. Anhang.

<sup>24</sup> Diese Anfragen bezogen sich auf Einzelfälle, die ab und zu an Einwohnerkontrollen gestellt wurden. Die Antworten auf diese Anfragen führten zusammen mit den ergänzten Richtlinien zur Datenbekanntgabe für die Einwohnerkontrollen dazu, dass seither praktisch keine Anfragen durch Einwohnerkontrollen mehr bei der Stabsstelle für Datenschutz eingehen.

<sup>25</sup> <http://www.llv.li/amtstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-arbeitsplatz.htm>

<sup>26</sup> <http://www.llv.li/amtstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-personalakten.htm>

<sup>27</sup> Vgl. unten 4.4.

<sup>28</sup> Vgl. dazu Datenschutz und Tarmed, Bericht des EDSB, abrufbar unter: [http://www.edsb.ch/d/themen/gesundheit/tarmed-bericht\\_d.pdf](http://www.edsb.ch/d/themen/gesundheit/tarmed-bericht_d.pdf)

<sup>29</sup> Vgl. Art. 23 DSG.

Die von den Gemeinden bewilligten Baugesuche wurden bisher durch diese im Sinne der Transparenz veröffentlicht und dies über verschiedene Kanäle wie das Anschlagbrett beim Rathaus, das Beschlussprotokoll der Gemeinderatssitzungen, den Gemeindekanal, die Informationsbroschüre der Gemeinde oder deren Internetseite. Das Informationsgesetz sieht zwar vor, dass die Behörden über die Tätigkeiten von allgemeinem Interesse informieren; jedoch nur soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen. Ein allgemeines Interesse liegt vor, wenn eine Information zur Wahrung der demokratischen Rechte und zur Sicherstellung der Meinungsbildung über das Geschehen im Fürstentum Liechtenstein von Bedeutung ist. Nach Ansicht der DSK ist die Veröffentlichung von Baubescheiden nicht durch ein solches allgemeines Interesse gedeckt. Dem Argument der Vorsteherkonferenz, dass verschiedene Gemeinden regelmässig öffentliche Gemeinderatssitzungen abhalten würden, entgegnete die DSK, dass nach dem Gesetz Gemeinderatssitzungen in der Regel nicht öffentlich sind, was im Übrigen auch bei anderen Traktanden, z.B. bei Personalfragen, so gehandhabt wird. Auch Beschlussprotokolle der Gemeinderatssitzungen dürfen nur so weit offen gelegt werden, als nicht überwiegende öffentliche oder private Interessen entgegenstehen. In jedem Fall sind nach dem DSB und der DSK die Bestimmungen des Datenschutzgesetzes einzuhalten. Danach gibt es für Veröffentlichungen der Baubewilligungen im in Frage stehenden Ausmass – das heisst eine periodische Veröffentlichung von allen Baubewilligungen ohne Anfrage – keine Rechtsgrundlage. Während Eingaben zu Baugesuchen auf Grund des Einspracherechts nach dem Baugesetz veröffentlicht werden müssen, ist dies nicht der Fall, wenn der Gemeinderat ein Baugesuch bewilligt hat. Diese Entscheidung hat aber nicht zur Folge, dass bewilligte Baugesuche gar nicht mehr veröffentlicht werden dürfen: Liegt die Einwilligung der betroffenen Person vor, und wurde diese objektiv und umfassend von der

Gemeinde informiert, steht einer Veröffentlichung nichts im Wege.

Durch diese erste Entscheidung der Datenschutzkommission werden die Anliegen des Datenschutzes in Liechtenstein gestärkt und ein Umdenken in gewissen Bereichen wird nötig sein.

### 4.3. BEGUTACHTUNG DER GLEICHWERTIGKEIT DES AUSLÄNDISCHEN DATENSCHUTZES

Die Gleichwertigkeit des Datenschutzes in Drittländern wurde in Bezug auf **Guernsey**<sup>30</sup>, die **Isle of Man**<sup>31</sup> und den USA im Rahmen der Art. 29 Arbeitsgruppe wahr genommen. Dabei war das Ergebnis in den ersten beiden Fällen positiv. Die Gleichwertigkeitsfrage des Datenschutzes in den USA betraf die Übermittlung von Flugpassagierdaten in die USA.

Die **Übermittlung von Flugpassagierdaten an die USA** war in den letzten Jahren eines der Hauptthemen der Art. 29 Arbeitsgruppe.<sup>32</sup> Im Mai 2004 anerkannte die Europäische Kommission die Gleichwertigkeit des Datenschutzes in den USA in Bezug auf diese Daten. Dieser Beschluss, der im Widerspruch zur Meinung der Art. 29 Arbeitsgruppe gefasst worden war, war in der Folge in den EWR zu übernehmen.

Liechtenstein verfügt zwar über keine nationale Fluglinie, die gezwungen ist, den US-amerikanischen Zollbehörden Zugriff auf die Passagierdaten zu gestatten. Dennoch sind auch in Liechtenstein wohnhafte Personen betroffen, da auch deren Daten in die USA übermittelt werden.<sup>33</sup>

Fragen in diesem Zusammenhang können an die Stabsstelle für Datenschutz gerichtet werden. Für die Fallbehandlung zuständig ist aber je nach Abflugland die zuständige Datenschutzbehörde.

<sup>30</sup> Die Kanalinseln sind eine Gruppe von Inseln, Eilanden und Felsen vor der Küste Nordwestfrankreichs in der St.-Malo-Bucht im Ärmelkanal. Die Inseln sind zwar Teil der Britischen Inseln, gehören jedoch nicht zum Vereinigten Königreich. Sie sind unterteilt in die Bailiwicks (Selbstverwaltungsgebiete) Guernsey und Jersey. Die Inseln unterstehen der Krone (ohne zum Vereinigten Königreich zu gehören oder Kolonien zu sein) und geniessen volle Unabhängigkeit, mit Ausnahme der Aussenbeziehungen und der Verteidigung, wofür die Regierung des Vereinigten Königreichs zuständig ist. Guernsey, Alderney und Sark werden jeweils von eigenen, gewählten gesetzgebenden Versammlungen regiert. Vgl. dazu: [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2003/wp79\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp79_de.pdf) An dieser Stelle sei noch erwähnt, dass die Internetseite der Art. 29 Arbeitsgruppe gewechselt hat. Sie befindet sich nun auf: [http://europa.eu.int/comm/justice\\_home/fsj/privacy/index\\_de.htm](http://europa.eu.int/comm/justice_home/fsj/privacy/index_de.htm)

<sup>31</sup> Die Isle of Man liegt im Zentrum der Britischen Inseln. Das Land untersteht der Britischen Krone, geniesst jedoch Autonomie für innere Angelegenheiten. Es ist nicht Teil des Vereinigten Königreichs, wohl aber Mitglied des British Commonwealth. Die Isle of Man unterhält besondere Beziehungen zur Europäischen Union. Die Isle of Man gehört zum Zollgebiet der Union. Deshalb gilt der Grundsatz des freien Warenverkehrs für den Austausch von Industrie- und Agrarerzeugnissen zwischen der Insel und der Union. Vgl. dazu: [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2003/wp82\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp82_de.pdf)

<sup>32</sup> Vgl. Tätigkeitsbericht 2003 und unten, 7.1.

<sup>33</sup> Der Vollständigkeit halber sei angefügt, dass das Europäische Parlament den Beschluss der Europäischen Kommission vor dem Europäischen Gerichtshof (EuGH) angefochten hat. Der Fall ist noch hängig. Ähnlich fordern auch Australien und Kanada Flugpassagierdatensätze. Diese beiden Länder gehen in ihren Forderungen jedoch nicht so weit wie die USA.

#### 4.4. STELLUNGNAHME ZU VORLAGEN UND ERLASSEN

Bereits im zweiten Jahr der Geltung des DSG und der DSV wurden dieselben teilweise revidiert. Dazu wurde auch die Stellungnahme des Stabsstelle für Datenschutz als primär betroffene Behörde eingeholt.

Das **DSG** wurde anlässlich der Junisitzung des Landtages teilweise revidiert. Diese Revision bestand in drei Punkten: erstens wurde eine Möglichkeit geschaffen, damit das Register der Datensammlungen<sup>34</sup> über das Internet eingesehen werden kann. Damit wird eine moderne Kommunikationsart gewährleistet und gleichzeitig die Stabsstelle administrativ entlastet. Zweitens wurde die Frist nach Art. 44 Abs. 3 um drei Jahre verlängert. Die neue Bestimmung sieht vor allem vor, dass Behörden noch bis zum 1. August 2007 Persönlichkeitsprofile und besonders schützenswerte Daten bearbeiten können, ohne dass eine ausdrückliche gesetzliche Grundlage dafür besteht. Eine solche Massnahme war nötig, da die nötigen Gesetzesrevisionen bis zum 1. August 2004 nicht abgeschlossen werden konnten. Drittens wurde in Art. 15 ein redaktionelles Versehen korrigiert.

Auch die **DSV** wurde angepasst: Nach dem neuen Art. 28 ist das Register nicht mehr periodisch zu veröffentlichen, sondern, wie oben beschrieben, über das Internet einsehbar. Nach Art. 31 ist der DSB nicht mehr gehalten, stets mit der Regierung über das Ressort Justiz zu kommunizieren, sondern nur wenn die Kollegialregierung betroffen ist. Zudem wurde Art. 5 über die Datenübermittlungen ins Ausland der Richtlinie 95/46/EG angepasst, indem deren Art. 25 Abs. 2 übernommen wurde. Schliesslich wurde die Liste der im Anhang zur Verordnung genannten gleichwertigen Länder um Argentinien und Guernsey erweitert, Ungarn gestrichen, da Ungarn inzwischen der EU beigetreten war und die Gleichwertigkeit des Datenschutzes der USA präzisiert.<sup>35</sup>

Bei den Revisionen des **Wohnbauförderungs-, Mutterschaftszulagen- und Wirtschaftsprüfergesetzes** wurde eine Stellungnahme abgegeben und angeregt, dass eine allgemeine Datenschutzbestimmung eingeführt wird,<sup>36</sup> 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<sup>37</sup> geschaffen wird.

Zu Vorentwürfen in Bezug auf das **Waffengesetz, das Polizeigesetz und eine Staatsschutzverordnung** wurde in einem informellen Rahmen Stellung genommen.

Im Rahmen von verschiedenen **Vernehmlassungsverfahren**<sup>38</sup> wurden konkrete Anliegen des Datenschutzes eingebracht.

Wie im letzten Tätigkeitsbericht erwähnt, sieht das neue Krankenversicherungsgesetz (KVG) eine Versichertenkarte vor.<sup>39</sup> Dabei erhielt die Regierung eine Verordnungskompetenz, die zur Ausarbeitung einer **Krankenversichertenkartenverordnung** führte. Die vorbereitenden Arbeiten an dieser Verordnung, an denen die Stabsstelle für Datenschutz eng beteiligt war, waren bis Ende des Jahres noch nicht abgeschlossen.

Auf Gemeindeebene konnte zu einem Entwurf eines **Kundmachungs-, Schriftgut- und Archivreglements** der Gemeinde Eschen Stellung genommen werden.

Last but not least ist zu erwähnen, dass ein **Staatsvertrag zwischen der Schweiz und Liechtenstein über die gemeinsame Benutzung von Datenbanken über Fingerabdrücke und DNA-Profile** geschaffen werden sollte. Eine solche gemeinsame Benutzung ist zwar nicht neu. Doch entstand das Bedürfnis, hierfür eine Rechtsgrundlage zu schaffen aus Gründen der Rechtssicherheit und des Datenschutzes. Auch hierzu wurde eine Stellungnahme abgegeben, wobei die meisten Anliegen berücksichtigt wurden.

<sup>34</sup> Vgl. unten, 6.

<sup>35</sup> Demnach gelten die USA nicht als allgemein gleichwertig, sondern nur im Rahmen des Abkommens über den so genannten «sicheren Hafen».

<sup>36</sup> Eine solche Regelung sollte den Grundsatz der Datenbearbeitung, allenfalls die Datenbekanntgabe, technische und organisatorische Massnahmen sowie möglicherweise die Löschung der Daten erfassen.

<sup>37</sup> Zu den angesprochenen ausdrücklichen Grundlagen vgl. unten, 5.1.2.

<sup>38</sup> Bei diesen Vernehmlassungsberichten ging es um eine Revision bzw. ein Schaffung des Arbeits-, des Gewerbe-, des Kommunikations-, des Konsumkredit-, des Investmentunternehmens-, des Mediations-, des Medien-, des Opferhilfe- und des Vermessungsgesetzes. Dazu erfolgte eine Stellungnahme zu Anpassungen in der Heilmittelgesetzgebung. Die Anregungen der Stabsstelle für Datenschutz wurden meist aufgenommen, teils nicht und teils ist die Ausmass der Aufnahme der Anregungen noch unklar.

<sup>39</sup> Vgl. Tätigkeitsbericht 2003, 3.6.

# 5. Aufsicht

Neben Informations- und Beratungsaufgaben kommen dem DSB auch Aufsichtsaufgaben zu, damit sichergestellt werden kann, dass den Anforderungen des Datenschutzes auch wirklich nachgekommen wird.

Diese Aufsicht ist nach dem DSG unterschiedlich geregelt. Geht es um Behörden, fallen dem DSB Aufsichtsfunktionen zu, auch wenn es um Datenschutzbestimmungen geht, die in anderen Gesetzen als dem DSG vorgesehen sind. Demgegenüber ist die Aufsichtsfunktion im privatrechtlichen Bereich nicht ganz so umfassend.<sup>40</sup>

In einem Problemfall wird immer erst versucht, den für eine Bearbeitung Verantwortlichen durch Information und Beratung zu einem datenschutzkonformen Umgang zu bewegen. Erst wenn sich trotz Information und Beratung Widerstände beim Verantwortlichen ergeben, beginnt die eigentliche Phase der Aufsicht. Ein solch gestuftes Vorgehen empfiehlt sich in der Regel allein schon, da das DSG noch relativ jung ist und teils das Bewusstsein für Verantwortlichkeiten fehlt.

## 5.1. AUFSICHT ÜBER BEHÖRDEN

### 5.1.1. DATENSCHUTZWIDRIGE BEARBEITUNGEN

#### 5.1.1.1. Datenbanken

Die Landesverwaltung führt seit Ende der Achtziger Jahre eine zentrale Datenbank, in der vorwiegend die gesamte ständige Bevölkerung des Landes erfasst wird. Da diese **Zentrale Personenverwaltung (ZPV)** genannte Datenbank vor Inkrafttreten des DSG geschaffen worden war, wurde sie nicht datenschutzkonform eingerichtet.<sup>41</sup> Die Regierung schuf Anfang des Berichtsjahres eine Arbeitsgruppe, welche die Aufgabe hat, dies nachzuholen.

Aufgabe der Arbeitsgruppe, die zwischen März und Ende Dezember 13 Sitzungen abhielt, ist es, in verschiedenen Schritten die Vereinbarkeit dieser umfassenden Datenbank mit dem Datenschutz herzustellen. Dazu war in einem ersten Schritt eine Bestandsaufnahme vorzunehmen. Dabei stellte sich heraus, dass etliche Amtsstellen bis zu 47 Personendaten insbesondere der gesamten ständigen Wohnbevölkerung Liechtensteins bearbeiten. Der Zugriff auf die Daten war im

Grossen und Ganzen bei allen Amtsstellen derselbe, egal welche Aufgaben sie einnehmen. Immerhin war bereits die Möglichkeit gegeben, dass Zugriffe zu einzelnen Feldern technisch verunmöglicht und Datenfelder gesperrt werden konnten. Diese Amtsstellen wurden gebeten, dem DSB mitzuteilen, aus welchen Gründen sie welche Felder benötigten und die gesetzlichen Grundlagen dazu anzugeben. Auf Grund dieser Rückmeldungen wurde zusammen mit dem Zuständigen der Abteilung Informatik des für die ZPV insgesamt verantwortlichen Amtes für Personal und Organisation und der jeweiligen Amtsstelle das Gespräch gesucht und versucht, diese zu einem Verzicht auf aus Datenschutzgründen nicht benötigte Felder zu bewegen. Ein gutes Beispiel eines Amtes, das nur einen beschränkten Zugriff zur ZPV benötigt, ist die Landeskasse. Deren Aufgabe besteht darin, Rechnungen für die Landesverwaltung zu verschicken. Dazu benötigt sie die aktuelle Adresse der betroffenen Person. Es müssen auch Verwechslungen mit anderen gleichnamigen Personen ausgeschlossen werden können. Angaben über einen Arbeitgeber, das Heiratsdatum oder die Staatsbürgerschaft der betroffenen Person sind für die Aufgaben der Landeskasse nicht nötig. Nach diesem Muster – Zugriff zu Personendaten nach dem entsprechenden gesetzlichen Auftrag – wurde vorgegangen.

Das Ziel, den Bedarf bei sämtlichen ZPV-Amtsstellen bis Ende des Jahres zu eruieren und auszuwerten, konnte nicht ganz erreicht werden. Von 28 eingegangenen Anträgen, welche durch den DSB auf ihre Datenschutzkonformität zu untersuchen waren, konnten 8 Anträge abgeschlossen werden, während es bei 19 Anträgen noch offene Fragen gab. Einzelne Anträge wurden bis Ende des Jahres noch nicht eingereicht.

Eine andere, damit zusammen hängende Frage, besteht in der **Schaffung einer gesetzlichen Grundlage** für die ZPV. Vorbereitungen hierzu sind im Gange und obwohl es nicht Aufgabe des DSB ist, solche Grundlagen zu schaffen, gab er doch auf Grund eines Rohentwurfes den konkreten Anstoss zur Inangriffnahme dieses komplexen Vorhabens. Damit eng verbunden ist auch die **Schaffung eines Bearbeitungsreglements** nach Art. 21 DSV, da es sich um eine automatisierte Datensammlung handelt, welche Persönlichkeitsprofile beinhaltet. Auch diese Aufgabe konnte durch die Arbeitsgruppe ZPV noch nicht abgeschlossen werden. Es ist überhaupt fraglich, ob diese Arbeitsgruppe der komplexen Aufgabe, eine rechtliche Grundlage für die ZPV zu schaffen, innert nützlicher Frist nach-

<sup>40</sup> Vgl. Art. 29 und 30 DSG.

<sup>41</sup> Vgl. dazu Tätigkeitsbericht 2003, 4.1.2.

kommen kann. Die Dringlichkeit der Schaffung einer rechtlichen Grundlage ist auch deshalb gegeben, da teils Daten in die ZPV eingegeben werden, die in einem juristischen Graubereich liegen.

Neben dieser umfassenden Datenbank gibt es etliche **spezifische Fachapplikationen**, die mit der ZPV zusammen hängen (wie sie z.B. in Bezug auf direkte und indirekte Steuern vorkommt. Weiters ist die Datenbank «Bistrada» der Motorfahrzeugkontrolle, das Gewerberegister, das Gesundheitsnetz Liechtenstein (GNL), die Datenbank Terris und das Liechtensteinische Unternehmensregister (LUR), zu nennen. Auch das Amt für Umweltschutz, das Ausländer- und Passamt, das Zivilstandsamt, das Schulamt (Stipendien), das Amt für Wohnungswesen, die Landeskasse und das Amt für Zollwesen weisen eigene Applikationen auf, die mit der ZPV zusammenhängen. Dazu kommen die Programme «Winschule» und möglicherweise die Datenbank «Juris» des Landgerichtes und der Staatsanwaltschaft, die ebenfalls für eine Überprüfung in Frage kommen. Diese Liste könnte noch verlängert werden.

Ähnlich ist die Situation bei den Gemeinden. Auch diese verwenden eine sehr umfassende Datenbank für die tägliche Arbeit, welche auf einer **Gemeinde Software Lösung (GeSoL)** genannten Software beruht. Diese Datenbank ist ein sehr wichtiges Arbeitsinstrument der Gemeinden. In dieser Datenbank werden jeweils die Gemeindeglieder erfasst und ihre Daten bearbeitet. Dabei werden im Unterschied zur ZPV nicht nur Persönlichkeitsprofile sondern auch (teils) besonders schützenswerte Daten über die religiösen Ansichten bearbeitet. Auch diese Gemeindegliederdatenbank entbehrt einer ausdrücklichen rechtlichen Grundlage wie sie das DSG fordert.<sup>42</sup> Die Schaffung einer solchen Grundlage wurde ebenfalls bei der Regierung angeregt.

### 5.1.1.2. Anderes

Wie bereits beschrieben, wurden die vom Gemeinderat **bewilligten Baugenehmigungen** datenschutzwidrig bekannt gegeben.<sup>43</sup> Nachdem eine Abklärung der Sachlage durch den DSB durch die Vorsteherkonferenz nicht akzeptiert wurde, blieb nichts anderes übrig, als die Datenschutzkommission anzurufen. Diese entschied schliesslich im Sinne des DSB.<sup>44</sup> Bei ver-

schiedenen Gemeinden ist es ausserdem üblich, auch Stellungnahmen oder Entscheide zu **Einbürgerungsgesuchen** zu veröffentlichen. Diese Bekanntgaben erfolgen teils über die Internetseite der Gemeinde. Abgesehen davon, dass Bekanntgaben über das Internet eine ausdrückliche gesetzliche Grundlage benötigen,<sup>45</sup> ist eine Bekanntgabe von behandelten Einbürgerungsgesuchen in der Regel spezialgesetzlich nicht vorgesehen. Deshalb wurde den Gemeinden über die Vorsteherkonferenz empfohlen, von solchen Bekanntgaben abzusehen. Eine Antwort der Gemeinden war bis Ende des Jahres noch nicht eingegangen.

Auch die Bearbeitung und insbesondere die interne **Bekanntgabe von privaten Daten der Angestellten der Landesverwaltung** innerhalb derselben ist hier zu nennen. Dabei umfasste insbesondere das verwaltungsinterne Intranet auch private Daten wie Geburtsdatum, private Adresse und ein Foto der Mitarbeiter der Verwaltung. Zwar wurde die Möglichkeit geschaffen, diese Daten zu sperren. Doch führte dies dazu, dass die betreffenden Daten der anderen Mitarbeiter auch nicht mehr einsehbar waren, auch wenn diese die Daten nicht gesperrt hatten. Das Sperrecht nach Art. 24 DSG sieht allerdings keine derartige Bedingungen oder Sanktionen der Ausübung des Sperrechts vor. Zudem wurden gewisse private Angaben ins Intranet eingestellt, ohne dass die Betroffenen davon wussten. Der DSB wies in einer formellen Empfehlung auf diesen Missstand hin und das Amt für Personal und Organisation verpflichtete sich, der Empfehlung nachzukommen und die Sperrung der Bekanntgabe von privaten Daten auch auf andere Veröffentlichungen des Amtes für Personal und Organisation auszudehnen. Die Einwilligung der betroffenen Mitarbeiter zur Bekanntgabe der erwähnten privaten Daten war insbesondere deshalb nötig, da für solche Bekanntgaben keine gesetzliche Grundlagen bestehen.

Ein weiterer Fall der Datenbekanntgabe betrifft die listenweise **Bekanntgabe von Arbeitslosen** durch die Abteilung Arbeit des Amtes für Volkswirtschaft **an das Ausländer- und Passamt**. Anfangs umfassten solche Bekanntgaben auch liechtensteinische Staatsangehörige, obwohl dies für das Ausländer- und Passamt nicht relevant war, da das Ausländer- und Passamt nur zu überprüfen hat, ob eine Ausländergenehmigung verlängert werden kann. Die gesetzlichen Regelungen sehen eine

<sup>42</sup> Vgl. Art. 21 Abs. 2 DSG.

<sup>43</sup> Vgl. dazu bereits Tätigkeitsbericht 2003, 4.1.1.

<sup>44</sup> Vgl. dazu oben, 4.2.

<sup>45</sup> Vgl. Art. 23 Abs. 3 DSG. Eine solche ist in Ausarbeitung.

Listenbekanntgabe im Sinne von Art. 23 Abs. 1 nicht vor. Da solche Angaben aber für die Arbeit des Ausländer- und Passamtes notwendig sind, ist eine Einzelbekanntgabe nach Art. 23 Abs. 1 Buchstabe a erlaubt. Dies aber erst, nachdem eine arbeitslose Person während einer Dauer von sechs Monaten arbeitslos war.<sup>46</sup> Diese Einhaltung der Frist wurde nicht respektiert, sodass auch Einzelmeldungen von arbeitslosen Ausländern an das Ausländer- und Passamt ergingen, wenn diese vor Ablauf der Sechsmonatsfrist wieder eine Arbeit fanden. Für solche Fälle gibt es aber keine Rechtsgrundlage. Deshalb wurde der Abteilung Arbeit des Amtes für Volkswirtschaft empfohlen, solche Meldungen erst nach Ablauf der genannten Frist vorzunehmen. Dem wurde nachgekommen. Da es aber auch Gründe für eine frühzeitige Meldung an das Ausländer- und Passamt gibt (insbesondere um den Betroffenen frühzeitig darauf hinzuweisen, dass seine Bewilligung möglicherweise nicht mehr verlängert wird) wurde die Rechtslage mit der letzten Revision der Personenverkehrsverordnung (PVO) dahin gehend abgeändert,<sup>47</sup> dass das Ausländer- und Passamt die Möglichkeit erhält, die Betroffenen frühzeitig anzuschreiben.

Nachdem die Frage der Bearbeitung von **Religionsdaten** durch die Landesverwaltung gelöst werden konnte,<sup>48</sup> stellte sich diese Frage auch auf der Ebene der **Gemeinden**. Deswegen wurden die Gemeinden über die Vorsteherkonferenz gebeten, anzugeben welchem Zweck die bei den Gemeinden vorhandenen Daten über die Religionsangehörigkeit der Gemeindeeinwohner dienen. Ein genannter Zweck bestand in den laufenden Verhandlungen über das Verhältnis von Staat und Kirche. Das revidierte DSG verlängerte die Frist zur Möglichkeit einer Bearbeitung von besonders schützenswerten Daten, und somit von Religionsangaben, bis zum 1. August 2007.<sup>49</sup> Vor diesem Hintergrund wurde die Untersuchung dieser Frage bis zum Ablauf dieser Frist unterbrochen.

### 5.1.2. GESETZLICHE GRUNDLAGEN

Die Bearbeitung von Daten benötigt wie jedes staatliche Handeln eine gesetzliche Grundlage. Da das DSG noch sehr

jung ist, aber an andere Gesetze gewisse Ansprüche stellt, kann es sein, dass solche Gesetze aus Datenschutzgründen geändert werden müssen.<sup>50</sup>

Nach Art. 44 dürfen insbesondere Behörden bestehende Datensammlungen, die **besonders schützenswerte Daten und Persönlichkeitsprofile** enthalten, neu bis am 31. Juli 2007 benutzen<sup>51</sup> ohne dass eine ausdrückliche gesetzliche Grundlage für die Bearbeitung existiert. Die Verlängerung dieser Übergangsfrist wurde nötig, da die nötigen Grundlagen nicht bis am 31. Juli 2004 geschaffen werden konnten. Somit wären gewisse Tätigkeiten innerhalb der Behörden ab dem letzt erwähnten Datum als gesetzeswidrig einzustufen gewesen. Wie schon 2003 wies der DSB die Regierung darauf hin, wenn solche gesetzliche Grundlagen insbesondere für Behörden nicht existierten. Ein solcher Handlungsbedarf wurde in Bezug auf folgende Gesetze festgestellt: Arbeitslosen-, Arbeitsvermittlungs-, Flüchtlings-, Investmentunternehmens- und Polizeigesetz sowie im AHV-Bereich.

Auch im Rahmen der ZPV und der Gemeindedatenbanken (Gesol)<sup>52</sup> werden Persönlichkeitsprofile bearbeitet. Die Schaffung einer ausdrücklichen gesetzlichen Grundlage ist auch in diesen Fällen geboten.

### 5.2. ABKLÄRUNGEN UND EMPFEHLUNGEN IM PRIVATRECHTSBEREICH

Die polnische Datenschutzbehörde machte den DSB darauf aufmerksam, dass eine in Liechtenstein ansässige Gesellschaft beabsichtige, ein **Telefonbuch über Einwohner in Polen** herauszugeben. Die genannte Behörde ersuchte um verschiedene Stellungnahmen zu konkret gestellten Fragen. Dem DSB war diese Gesellschaft und deren Tätigkeit und Vorhaben unbekannt. Insbesondere war keine Datensammlung angemeldet und registriert worden. Dies wäre aber nötig gewesen, da die betroffenen Personen in Polen über diese Datenbearbeitung nicht informiert waren.<sup>53</sup> Auch der vorgängigen Informationspflicht, nach der über den Dateninhaber und den Zweck der Datenbearbeitung zum Voraus informiert werden muss, wurde

<sup>46</sup> Vgl. Art. 94 Abs. 1 Buchstabe f der alten Personenverkehrsordnung.

<sup>47</sup> Vgl. Art. 20 Abs. 5 PVO.

<sup>48</sup> Vgl. Tätigkeitsbericht 2003, 4.1.1.

<sup>49</sup> Vgl. oben, 4.4.

<sup>50</sup> Vgl. auch in der Schweiz z.B. das Bundesgesetz über die Schaffung und die Anpassung gesetzlicher Grundlagen für die Bearbeitung von Personendaten vom 24. März 2000.

<sup>51</sup> Vgl. oben, 4.4.

<sup>52</sup> Vgl. zur ZPV und zur Gesol-Datenbank oben, 5.1.1.

<sup>53</sup> Vgl. Art. 15 Abs. 3 DSG.

gegenüber den Betroffenen nicht nachgekommen. Die Betroffenen wurden auch nicht darauf aufmerksam gemacht, dass sie ein unentgeltliches und sofort wirksames Widerspruchsrecht hatten, das ihnen ermöglicht hätte, nicht im geplanten Telefonbuch aufzuscHEINEN.<sup>54</sup> Angesichts dieser Konstellation wurde der Gesellschaft empfohlen, das Versäumte nachzuholen, und insbesondere die Betroffenen zu informieren, oder die Datenbearbeitung einzustellen. Auf Grund der grossen Anzahl von betroffenen Personen in Polen entschied sich das Unternehmen dazu, von ihrem Vorhaben abzusehen.

Wie schon im Vorjahr führten die beiden Landeszeitungen auch 2004 wieder eine Fotoaktion durch, um die **neuen Erstklässler** bildlich mit Angabe von Vor- und Nachname in den Zeitungen, und teils auch auf dem Internet, darzustellen. Nachforschungen ergaben, dass die Empfehlungen des Vorjahres<sup>55</sup> nicht berücksichtigt worden waren. Um die angebliche Beliebtheit dieser Fotoaktion nicht grundsätzlich in Frage zu stellen, wurde den beiden Zeitungen ein Weg aufgezeigt, wie die Erstklässler auch in Zukunft namentlich und mit Foto vorgestellt werden können – aber eben unter Berücksichtigung des Datenschutzes. Dieser wird sichergestellt, indem den Eltern die Gelegenheit gegeben wird, sich gegen eine Darstellung ihres Kindes in einer Zeitung zu wehren. Haben die Eltern nichts dagegen einzuwenden, kann aus Datenschutzsicht vom Vorliegen einer stillschweigenden Einwilligung ausgegangen werden.<sup>56</sup>

Die Gewerbe- und Wirtschaftskammer (GWK) schuf 2004 mit der **LieCard** eine Kundenkarte, die jedoch nicht mit anderen Kundenkarten wie der Cumulus- oder der Supercard vergleichbar ist. Auf Initiative des DSB wurden die allgemeinen Geschäftsbedingungen (AGBs) der LieCard angepasst, um die Kundenbesitzer ausführlich zu informieren, welche Daten gesammelt und zu welchen Zwecken sie bearbeitet werden. Schliesslich wird in den AGBs auch festgehalten, dass die Daten nicht weiter verkauft, oder sonst wie kommerziell ausgenutzt werden. Interessierte werden somit über die Datenbearbei-

tung, die mit der LieCard verbunden ist, ausreichend informiert.<sup>57</sup>

Im Anschluss an einen Fall versteckter **Videoüberwachung**<sup>58</sup> wurden die drei Grossbanken angeschrieben und um Auskunft gebeten, wie die Videoüberwachung gehandhabt wird. Die Rückmeldungen ergaben keine datenschutzrechtlichen Bedenken.

<sup>54</sup> In einem ähnlichen Fall, in dem es auch um die Schaffung eines Telefonbuches, allerdings in Liechtenstein, ging, wurden die Betroffenen in den Allgemeinen Geschäftsbedingungen der Gesellschaft genügend informiert.

<sup>55</sup> Vgl. Tätigkeitsbericht 2003, 4.2.

<sup>56</sup> Die Einholung der Einwilligung setzt eine entsprechende Information der Kinder bzw. der Eltern nach Art. 5 DSG voraus; vgl. zu Informationspflichten oben, 3.2.

<sup>57</sup> Vgl. zur Informationspflicht nach Art. 5 DSG, oben, 3.2.

<sup>58</sup> Vgl. Tätigkeitsbericht 2003, 4.2.

# 6. Register der Datensammlungen

Mit LGBl. 2004 Nr. 174 wurde die rechtliche Grundlage geschaffen, damit das Register der Datensammlungen auf dem Internet veröffentlicht werden kann. Mit dieser Massnahme wurde ein modernes Kommunikationsinstrument geschaffen, da Interessierte somit nicht erst mit der Bitte an die Stabsstelle für Datenschutz gelangen müssen, einen Auszug aus dem Register zu bekommen, oder das Register vor Ort einsehen zu können. Mit dieser Massnahme wird auch der geringe Personalbestand der Stabsstelle entlastet. Die Vorbereitungen zur Aufschaltung des Registers auf die Internetseite der Stabsstelle für Datenschutz konnten bis Jahresende noch nicht abgeschlossen werden.

# 7. Internationales

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

Die Artikel 29 Arbeitsgruppe der Datenschutzrichtlinie erwies sich auch 2004 als ein interessantes Forum, in dem aktuelle Themen von internationaler Relevanz diskutiert wurden.<sup>59</sup> Von diesen Themen waren vor allem die Folgenden für Liechtenstein von Bedeutung:

Auch 2004 befasste sich die Arbeitsgruppe mit der **Übermittlung persönlicher Daten bei Flügen zwischen Europa und den Vereinigten Staaten von Amerika**.<sup>60</sup> Und dies gleich mehrmals. Dabei geht es um Folgendes: Nach den Ereignissen des 11. September 2001 hatten die USA eine Reihe von Regelungen erlassen, die Fluggesellschaften bei Flügen in die USA dazu verpflichten, den US-Behörden Personendaten über einreisende oder ausreisende Fluggäste und Besatzungsmitglieder zu übermitteln. Insbesondere müssen die Fluggesellschaften den US-amerikanischen Zoll- und Grenzschutzbehörden bei Flügen von den, in die und durch die USA elektronischen Zugang zu den im so genannten Passenger Name Record (PNR) enthaltenen Fluggastdaten gewähren. Fluggesellschaften, die diesen Forderungen nicht nachkommen, müssen mit hohen Geldstrafen oder sogar dem Entzug der Landrechte und ihre Passagiere mit Verspätungen bei der Ankunft in den USA rechnen. Diese PNR-Daten umfassen eine Vielzahl von Informationen, die während des Buchungsverfahrens angegeben werden oder den Fluggesellschaften oder Reiseveranstaltern vorliegen, so etwa Name des Fluggastes, Kontaktdaten, Details der Reiseroute (etwa das Reisedatum, Ausgangs- und Zielort, Sitznummer und Zahl der Gepäckstücke) und Details der Reservierung (etwa Reiseveranstalter und Zahlungsinformationen) oder andere Informationen (etwa Zugehörigkeit zu einem Vielfliegerprogramm).<sup>61</sup>

In einer im Januar angenommenen Meinung<sup>62</sup> wiederholte die Gruppe ihre Bedenken gegen eine Bekanntgabe der PNR-

Daten an die US-amerikanischen Zoll- und Grenzschutzbehörden. Trotz dieser Bedenken fasste die Europäische Kommission im Mai 2004 einen Beschluss, wonach ein gleichwertiger Datenschutz gegeben sei. Damit wurde der Transfer dieser Datensätze, der seit März 2003 von den europäischen Fluggesellschaften praktisch erzwungen wurde, auf eine Rechtsgrundlage gestellt, die aber durch das Europäische Parlament vor dem Europäischen Gerichtshof angefochten wurde. Im Juni nahm die Arbeitsgruppe ein weiteres Dokument zu diesem Thema an, das sich mit der Frage beschäftigte, wie der erwähnte Gleichwertigkeitsbeschluss der Europäischen Kommission am Besten umgesetzt werden kann.<sup>63</sup> An der Septembersitzung wurde sodann ein Dokument angenommen, das den Betroffenen erklären soll, wie sich die Situation gestaltet und worin ihre Rechte bestehen. Dieses Dokument, das eine Kurzbeschreibung und eine lange Version in der Form von Fragen und Antworten umfasst, wurde an die Reisebüros in Liechtenstein gesandt, um über die Einreisebestimmungen in die USA aufmerksam zu machen.<sup>64</sup>

Eine Idee zur Verbesserung der Handhabung des Datenschutzes besteht in einer einheitlicheren Anwendung der **Informationspflichten**.<sup>65</sup> Der erste Bericht der Europäischen Kommission zur Umsetzung der Datenschutzrichtlinie sah einen Handlungsbedarf in diesem Zusammenhang. Kurz gesagt geht es darum, dass die betroffene Person informiert werden muss, wenn Daten über sie bearbeitet werden; dies gilt mit kleinen Unterschieden unabhängig davon, ob die Daten bei der betroffenen Person erhoben werden oder nicht. Ein oft vorkommender Anwendungsfall betrifft **Datenschutzerklärungen auf Internetseiten**. Im Sinne einer vorgängigen Information muss der Dateninhaber den Betroffenen über die Identität des Inhabers der Datensammlung, also den Betreiber der Internetseite, informieren. Dazu muss der Zweck einer Datenbearbeitung angegeben werden. Diese Information findet man normalerweise auf der Startseite einer Internetseite z.B. unter dem Hinweis «Datenschutz» oder «Privacy». Solche

<sup>59</sup> Vgl. auch Tätigkeitsbericht 2003, 6.1. und oben, 4.3.

An dieser Stelle sei noch erwähnt, dass die Internetseite der Art. 29 Arbeitsgruppe gewechselt hat. Sie befindet sich nun auf: [http://europa.eu.int/comm/justice\\_home/fsj/privacy/index\\_de.htm](http://europa.eu.int/comm/justice_home/fsj/privacy/index_de.htm)

<sup>60</sup> Vgl. dazu bereits Tätigkeitsbericht 2003, 6.1.

<sup>61</sup> Für weitere Angaben: [http://www.llv.li/pdf-llv-sds-cbp-dhs\\_pnrundertakings5-25-04.pdf](http://www.llv.li/pdf-llv-sds-cbp-dhs_pnrundertakings5-25-04.pdf) Pkt 4ff. und Attachment A.

<sup>62</sup> Vgl. [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2004/wp95\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp95_de.pdf)

<sup>63</sup> Dieses letztgenannte Dokument wurde auch auf der Internetseite der Stabsstelle für Datenschutz verfügbar gemacht:

<http://www.llv.li/amtstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-flugpassagierdaten.htm>

Die Übernahme dieses Gleichwertigkeitsbeschlusses in den EWR war zwar bis Ende 2004 noch nicht erfolgt. Dennoch sind Flugpassagiere, die in die USA fliegen gezwungen, diese Daten bekannt zu geben. Als Alternative bleibt lediglich, dass auf eine Reise in die USA verzichtet wird.

<sup>64</sup> Vgl. Art. 5 DSGVO und oben, 3.2.

<sup>65</sup> Vgl. auch oben, 3.2.

Hinweise fehlen in Liechtenstein noch bei etlichen Internetseiten und sind somit nachzuholen.<sup>66</sup>

Eine Methode, solche Datenschutzerklärungen auf Internetseiten zu vereinfachen, besteht in der Schaffung von so genannten Layered Notices. In diesen «geschichteten Mitteilungen» wird auf der obersten Schicht eine Grundinformation gegeben.<sup>67</sup> Diese Erklärungen sollen nur einleitend erklären und ausreichende Informationen nicht ersetzen, sondern zu letzteren leiten. So wird die Qualität der Datenschutzzinformationen verbessert, wenn auf jeder Ebene die Informationen in den Vordergrund gestellt werden, die die betroffene Person benötigt, um ihre Situation zu bestimmen und gezielte Entscheidungen zu treffen. Steht für die Kommunikation nur wenig Zeit und/oder Raum zur Verfügung, kann so die Leserfreundlichkeit der Hinweise verbessert werden.

So ist auch das oben angegebene Beispiel der Information von Flugpassagieren in die USA zu verstehen.

Die **Einführung biometrischer Merkmale<sup>68</sup> in Ausweispapiere** (Pässe, Visa, Aufenthaltstitel) ist eine Reaktion auf die Terroranschläge des 11. September 2001. Dabei verspricht man sich eine erhöhte Sicherheit von Reisedokumenten. In einer vorläufigen Stellungnahme zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel unter Berücksichtigung des Aufbaus des Visa-Informationssystems VIS<sup>69</sup> wurde einleitend bemerkt, dass das VIS sowie die zweite Generation des Schengener Informationssystems<sup>70</sup> (SIS II) derzeit aufgebaut werden. Zu geplanten verbesserten Synergien zwischen bestehenden und künftigen Informationssystemen (SIS II, VIS und EURODAC<sup>71</sup>) weist die Gruppe darauf hin, dass sich alle Massnahmen in diesem Bereich erheblich auf die Grundrechte der betroffenen Personen, d.h. aller Ausländer, die ein Visum beantragen, also von Zigmillionen Menschen, auswirken dürften. Diese Stellungnahme hat, wie angetönt, vorläufigen

Charakter und ist an die Institutionen der EU gerichtet und somit für die Öffentlichkeit nicht so interessant. Bei einem Beitritt Liechtensteins zu den **Abkommen von Schengen und Dublin** dürfte das Dokument aber dennoch interessant werden. Ob und wann ein solcher erfolgen wird, ist noch offen.

In einer Stellungnahme zum Thema **Videoüberwachung<sup>72</sup>** hält die Gruppe fest, dass die Videoüberwachung verschiedene Zwecke erfüllt (wie der Schutz von Einzelpersonen, von Eigentum, des öffentlichen Interesses. Sie kann auch der Ermittlung, Verhütung und Verfolgung von Straftaten, der Beweissicherung, oder sonstigen berechtigten Interessen dienen). Es wird betont, dass der Datenschutz auch dann anwendbar sein kann, wenn Bild- und Tondateien keine Personen betreffen, deren Gesicht gefilmt wurde, aber andere Informationen enthalten, zum Beispiel Nummernschilder oder PIN-Nummern, die in Verbindung mit der Überwachung von Geldautomaten gesammelt wurden. Der Grundsatz der Verhältnismässigkeit bedeutet, dass diese Systeme nur eingesetzt werden dürfen, wenn sich andere Vorsorge-, Schutz- und/oder Sicherheitsmassnahmen physischer und/oder programmgesteuerter Art, die keine Bildaufnahmen erfordern<sup>73</sup> zweifelsfrei als unzureichend und/oder nicht anwendbar im Hinblick auf die vorgenannten legitimen Zwecke erweisen. Zum Beispiel sollte verhindert werden, dass Behörden Videoüberwachungsanlagen im Zusammenhang mit geringfügigen Verstössen installieren – etwa um einem Rauchverbot in Schulen und anderen öffentlichen Plätzen oder dem Verbot, Zigarettenstummel und Abfälle an öffentlichen Plätzen zu hinterlassen, Nachdruck zu verleihen. Mit anderen Worten: Im Hinblick auf den verfolgten Zweck muss von Fall zu Fall der **Grundsatz der Verhältnismässigkeit** angewandt werden, der eine Art Pflicht der **Datenminimierung** bei den für die Verarbeitung Verantwortlichen beinhaltet. Die Verhältnismässigkeit muss sodann auch für die Modalitäten der Verfilmmungen gewahrt werden. So ist z.B. das Bildfeld zweckgerecht

<sup>66</sup> Als Beispiele vgl. die Rechthinweise auf <http://www.fma-li.li>, <http://www.llv.li/> oder <http://www.planken.li>.

<sup>67</sup> Dabei geht es darum, dass erst in einer kurzen Information das Wesentliche über eine Datenbearbeitung ausgesagt wird. Diese Kurzinformation wird durch eine längere und ausführliche Information ergänzt und so gesehen wird die Kurzinformation überlagert (daher der Begriff «Layered Notices» d.h. geschichtete Informationen).

<sup>68</sup> Zu biometrischen Merkmalen im Allgemeinen vgl.: [http://www.llv.li/pdf-llv-sds-biometrie\\_wp80\\_de.pdf](http://www.llv.li/pdf-llv-sds-biometrie_wp80_de.pdf)

<sup>69</sup> [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2004/wp96\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_de.pdf)

<sup>70</sup> Innerhalb des Schengen-Systems wurde ein automatisiertes Netz (SIS) geschaffen, um allen Polizeidienststellen und konsularischen Vertretern der dem Schengen-Raum angehörenden Staaten Daten über gesuchte Personen, Gegenstände oder Fahrzeuge zu übermitteln. Das VIS ist gegenwärtig noch im Aufbau.

<sup>71</sup> EURODAC dient dem Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens in Bezug auf Asylanträge.

<sup>72</sup> Das Dokument ist mit weiteren Informationen auf folgender Adresse eingestellt:

<http://www.llv.li/amtstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-videoeberwachung.htm>

<sup>73</sup> Wie z. B. die Verwendung von Türen mit Sicherheitsbeschlägen zur Bekämpfung von Vandalismus, den Einbau von automatischen Toren und Freigabegeräten, von Alarmsystemen mit Fernübertragung, stärkere und umfassendere Beleuchtung von Straßen usw.

einzustellen (bei der Überwachung eines Hauseingangs ist es irrelevant, wer auf dem Trottoir am Hauseingang vorbei geht). Weiters sind die Bild- und gegebenenfalls Tonaufnahmen **gesichert aufzubewahren** und zu löschen, wenn sie ihren Zweck erfüllt haben. Schliesslich sind die Betroffenen über eine Videoüberwachung zu **informieren** selbst wenn sich diese auf öffentliche Ereignisse, Veranstaltungen oder Werbemassnahmen (Webcams) bezieht. Sie sind ausführlich darüber zu informieren, welche Stellen überwacht werden. Es ist nicht notwendig, den genauen Standort des Überwachungsgeräts anzugeben, aber die Umstände der Überwachung müssen eindeutig bekannt gemacht werden. Die Auskünfte müssen in einem vernünftigen Abstand zu den überwachten Plätzen angebracht werden. Zu nennen sind schliesslich v.a. die **Rechte der Betroffenen**, insbesondere das Recht auf Einspruch gegen eine Verarbeitung der in Frage stehenden Bild- und allenfalls Tonaufnahmen. Die Richtlinie 95/46/EG gestattet den Betroffenen, gegen die Verarbeitung sie betreffender Daten jederzeit aus stichhaltigen, sich aus ihrer besonderen Situation ergebenden Gründen Widerspruch einzulegen.

Die Arbeitsgruppe behandelte auch die wichtige Frage der **Vorratsdatenspeicherung von Verkehrsdaten im Telekommunikationsbereich**.<sup>74</sup> Elektronische Kommunikationsnetze und -dienste werden zunehmend im Alltag genutzt. Die bei dieser Form der Kommunikation generierten Daten, die so genannten «Verkehrsdaten», können Informationen über Ort, Zeitpunkt und Gesprächspartner von Mobil- oder Festnetztelefonaten, Telefaxkommunikation, E-Mails, SMS und anderen Formen der Internetkommunikation enthalten und daher zunehmend die Lebensführung der Nutzer widerspiegeln. In der Stellungnahme kommt die Arbeitsgruppe unter anderem zum Ergebnis, dass die in der EU vorgesehene Verpflichtung zur routinemässigen, flächendeckenden Vorratspeicherung sämtlicher Verkehrs-, Nutzer- und Teilnehmerdaten die nur ausnahmsweise zulässige Überwachung zur Regel machen würde. Ferner würden alle versandten oder empfangenen Mitteilungen erfasst. Nicht alles, was sich für die Strafverfolgung als nützlich erweisen könnte, ist demnach wünschenswert oder kann als notwendig angesehen werden, zumal wenn es zu einer systematischen Registrierung der gesamten elektronischen Kommunikation führt. Dass eine so um-

fassende Speicherung von Verkehrsdaten der einzig gangbare Weg zur Bekämpfung der Kriminalität oder zur Wahrung der nationalen Sicherheit ist, dafür liefere der in Frage stehende Entwurf keine überzeugenden Argumente. Mit der Verpflichtung der Provider zur Speicherung von Verkehrsdaten, die sie nicht für eigene Zwecke benötigen, würde der Grundsatz der Zweckbindung in beispielloser Weise durchbrochen. Die Gruppe bezieht sich auf verschiedene Stellungnahmen von Datenschutzbehörden, in denen die systematische Speicherung aller Verkehrsdaten für die Dauer von einem Jahr oder länger eindeutig unverhältnismässig und deshalb abzulehnen wäre. Dies auch, da Untersuchungen europäischer Telefongesellschaften gezeigt haben, dass das Gros der von Strafverfolgungsbehörden abgerufenen Daten nicht älter als sechs Monate war. Das belege, dass längere Aufbewahrungsfristen eindeutig unverhältnismässig seien.

Auch wenn der in Frage stehende Entwurf eines Rahmenbeschlusses möglicherweise nicht in Kraft tritt oder nicht EWR relevant ist: Die angenommene Stellungnahme enthält gute Argumente gegen eine solche Vorratsdatenspeicherung von Telekommunikationsdaten, sollte sich die Frage einmal auch in Liechtenstein stellen.

In einem Text über **unerbetene Werbenachrichten** (besser bekannt unter dem Begriff **Spam-Mails**)<sup>75</sup> nahm die Arbeitsgruppe zu verschiedenen Begriffen<sup>76</sup> der Datenschutzrichtlinie 2002/58/EG in der elektronischen Kommunikation Stellung. Diese Richtlinie wird in Liechtenstein auf Grund der EWR-Mitgliedschaft umzusetzen sein. Dabei dürften verschiedene Punkte dieser Stellungnahme wichtig werden.<sup>77</sup>

Das angenommene Dokument zum Thema **Rechtsdurchsetzung** sowie das verabschiedete **Strategiepapier** setzen sich mit allgemeinen Bereichen auseinander, die vor allem für die Datenschutzbehörden selbst, aber auch für die Öffentlichkeit, von Interesse sind. Bei der Entschliessung zum Thema Rechtsdurchsetzung<sup>78</sup> geht es um die generelle Rolle der Datenschutzbehörden im Zusammenhang mit deren gesetzlicher Aufgabe der Aufsicht über Personen und Institutionen, welche Daten bearbeiten. In diesem Dokument verpflichtet sich die Arbeitsgruppe insbesondere dazu, proaktive Strategien

<sup>74</sup> [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2004/wp99\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_de.pdf)

<sup>75</sup> [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2004/wp90\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp90_de.pdf)

<sup>76</sup> Thematisiert wurden die folgenden Begriffe: Elektronische Post, vorherige Einwilligung des Teilnehmers, und Direktwerbung. Dazu wurde zur Ausnahme von der Opt-in-Regelung und zur Regelung für Nachrichten, die an juristische Personen gerichtet sind Stellung genommen.

<sup>77</sup> Die Vernehmlassungsfrist zu einem umfassenden Kommunikationsgesetz lief Ende Dezember 2004 ab.

<sup>78</sup> [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2004/wp101\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp101_de.pdf)

zur Rechtsdurchsetzung zu entwickeln, Durchsetzungsmassnahmen voranzutreiben und ihre Bemühungen um mehr Kooperation zu intensivieren, indem sie Amtshilfevereinbarungen fördert. Das so genannte Strategiepapier setzt sich demgegenüber mit der Rolle, den Aufgaben und Perspektiven der Arbeitsgruppe auseinander.<sup>79</sup>

Schliesslich wurde ein Arbeitspapier über **genetische Daten**<sup>80</sup> angenommen, das auch für Liechtenstein relevant sein dürfte.

## 7.2. VEREINIGUNG DER SCHWEIZERISCHEN DATENSCHUTZBEAUFTRAGTEN

Im Frühling 2004 konnte zum ersten Mal an einer Sitzung der Vereinigung «Die schweizerischen Datenschutzbeauftragten/ Les Commissaires suisses à la protection des données» teilgenommen werden. An dieser Sitzung wurde eine Datenbank des Kantons Basel-Stadt vorgestellt, die mit der liechtensteinischen ZPV vergleichbar ist.<sup>81</sup> Neben der Gestaltung dieser Datenbank war insbesondere die Frage interessant, wie die Datenschutzkonformität gewährleistet wird. Dazu gibt es ein Formular, das die entsprechenden Ämter in Basel ausfüllen müssen. Der Datenschutzbeauftragte bereitet in Basel den Entscheid, der durch die Datenschutzkommission gefällt wird, vor. Ein ähnliches Vorgehen wurde von der Arbeitsgruppe ZPV auch für Liechtenstein gewählt.<sup>82</sup>

Im Herbst 2004 waren Fragen aus dem sozialen und dem Gesundheitsbereich im Mittelpunkt der Diskussion. Neben Fragen zum Tarmed<sup>83</sup> wurden Fälle von Datenmissbrauch diskutiert, die teils durch eine mangelnde Transparenz zwischen den Sozialbehörden erleichtert wurden.

## 7.3. EUROPARAT

Die Datenschutzkonvention des Europarates wurde im Frühling 2004 durch Liechtenstein ratifiziert. Sie trat am 1. September 2004 in Kraft. Auch eine Erklärung, wonach Liechtenstein den Beitritt der Europäischen Gemeinschaften zur Konvention akzeptiert, wurde beim Europarat hinterlegt.<sup>84</sup> Wie schon im letzten Tätigkeitsbericht erwähnt,<sup>85</sup> gibt es neben der Konvention auch ein Zusatzprotokoll über Aufsichtsbehörden und die grenzüberschreitende Datenübermittlung. Eine Unterzeichnung desselben sollte ins Auge gefasst werden, da damit die gesetzliche Unabhängigkeit des DSB verstärkt wird. Dazu werden auch wichtige Fragen des internationalen Datenverkehrs geregelt. Dass auch dieser für Liechtenstein sehr wichtig ist, steht ausser Frage.

Nach dem Zusammenschluss der beiden Ausschüsse zum Datenschutz im Europarat wurde im verbleibenden Konventionsausschuss an der jährlich stattfindenden Sitzung teilgenommen. Thema dieser Sitzung war einerseits die **Anwendung von Grundsätzen des Datenschutzes auf das Internet**. Dabei wurde insbesondere die Frage von Datenspuren (Cookies, usw.) behandelt, die ein Internetbenutzer bewusst oder unbewusst hinterlässt. Solche Datenspuren, oder die Benutzung des Internets im Allgemeinen, bedrohen die Privatsphäre; denn es finden heimliche Datenbearbeitungen statt, welche die Bildung von Persönlichkeitsprofilen ermöglichen. Andererseits wurde die Frage der **Biometrie** auch<sup>86</sup> vom Konventionsausschuss aufgegriffen.<sup>87</sup>

Schliesslich fand eine Konferenz zum Thema «**Die Rechte und Verantwortlichkeiten von Betroffenen**» statt, an welcher der DSB teilnahm. Dieses Thema ist besonders wichtig, da die von

<sup>79</sup> [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2004/wp98\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp98_de.pdf)

<sup>80</sup> [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2004/wp91\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp91_de.pdf)

<sup>81</sup> Vgl. dazu Tätigkeitsbericht 2003, 6.2. und <http://www.dsb-cpd.ch/d/home.htm>

<sup>82</sup> Mehr zum Thema ZPV vgl. oben, 5.1.1.1.

<sup>83</sup> Vgl. oben, 4.1.

<sup>84</sup> Eine solche Erklärung haben bisher [Stand: 5..4.05] 24 der 31 Konventionsstaaten hinterlegt.

<sup>85</sup> Tätigkeitsbericht 2003, 6.3.

<sup>86</sup> Vgl. dazu Tätigkeitsbericht 2003, 6.1. und ein Dokument, das von der Art. 29 Arbeitsgruppe angenommen worden war: [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2003/wp80\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_de.pdf)

<sup>87</sup> [http://www.llv.li/pdf-llv-sds-t-pd\\_2005\\_biom0e-1.pdf](http://www.llv.li/pdf-llv-sds-t-pd_2005_biom0e-1.pdf)

Datenbearbeitungen betroffenen Personen im Mittelpunkt stehen. Kurz gesagt ging es um die Rechte aller, die in irgendeiner Form von einer Datenbearbeitung betroffen sind. Ebenso standen insbesondere die Bewusstseinsbildung und Sensibilisierung der Öffentlichkeit für den Datenschutz zur Diskussion. Diese Konferenz ergab wichtige Anhaltspunkte für die Schaffung einer Broschüre über den Datenschutz in Liechtenstein.<sup>88</sup>

#### 7.4. EUROPÄISCHE DATENSCHUTZKONFERENZ

Jeweils im Frühling jedes Jahres findet die Europäische Datenschutzkonferenz statt, an der 2004 zum ersten Mal teilgenommen werden konnte. An dieser Konferenz waren insgesamt 33 Länder vertreten. Dabei wurde vorwiegend die **Rolle der nationalen Datenschutzbehörden in Europa** diskutiert. Basis war ein umfassender Fragebogen, der für die Konferenz erstellt wurde. Solche Vergleiche mit anderen Datenschutzbehörden sind gerade für eine noch junge Stelle wie die Stabsstelle für Datenschutz sehr nützlich, um Hinweise für die Definition der eigenen Rolle und der Arbeitsweise zu erhalten.

#### 7.5. INTERNATIONALE DATENSCHUTZKONFERENZ

Jeweils im Herbst jedes Jahres findet die Internationale Datenschutzkonferenz statt, an der ebenfalls erstmals eine

Teilnahme möglich war. Neben weltweiten Datenschutzbehörden nahmen auch Vertreter der Wirtschaft teil. Das Leitthema der 26. Internationalen Konferenz in Breslau, Polen, war «**Das Recht auf Privatsphäre – das Recht auf Würde**».<sup>89</sup> Dabei wurden verschiedene aktuelle Themen von grosser Bedeutung behandelt, die auch für Liechtenstein relevant sind: Eines der Hauptthemen bestand in «Privatsphäre und öffentliche Sicherheit», welches durch die traurigen terroristischen Ereignisse der jüngeren Vergangenheit sehr an Bedeutung gewonnen hat. Dabei wurde betont, dass der Schutz der Privatsphäre und die Garantie von Sicherheit für den Bürger Hand in Hand gehen müssen.

Weitere Themen waren vor allem: «Privatsphäre und die Nutzung von RFID»<sup>90</sup>, «die Privatsphäre und die Medien», «Bekämpfung der Verletzung der Privatsphäre im Internet», «Die Bedrohungen der Privatsphäre in der Zeit der e-Demokratie»<sup>91</sup>, «Die Informationen zum Datenschutz» oder «die biometrische Feststellung der Identität».<sup>92</sup>

<sup>88</sup> Vgl. dazu unten, 9.

<sup>89</sup> Sämtliche Konferenzunterlagen sind verfügbar unter: <http://26konferencja.giodo.gov.pl/program/j/ge/>

<sup>90</sup> Radio Frequency Identification Technologies. Bei dieser Technologie geht es um ein 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. Für einen datenschutzkonformen Umgang mit RFID-Funkchips fordert die deutsche Konferenz der Datenschutzbeauftragten insbesondere eine Prüfung weniger weit gehender Mittel. Bei einer Verwendung solcher Funkchips wird zudem gefordert, dass die Datenerhebung offen und transparent sein muss, die Bearbeitung nur für einen speziellen Zweck stattfindet und die Möglichkeit der Löschung oder Deaktivierung der Daten gegeben sein muss.

Das deutsche Bundesamt für Sicherheit und Informatik hat hierzu eine Studie mit dem Titel «Risiken und Chancen des Einsatzes von RFID-Systemen» herausgegeben: Die Art. 29 Arbeitsgruppe bereitet ebenfalls ein Dokument zu dieser Frage vor. Dieses Dokument sollte Anfang 2005 fertig gestellt sein. Vgl. zum Ganzen: [http://www.llv.li/amtsstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-rfid\\_funkchips.htm](http://www.llv.li/amtsstellen/llv-sds-spezialthemen/llv-sds-spezialthemen-rfid_funkchips.htm)

<sup>91</sup> Es sei daran erinnert, dass Art. 8b des revidierten Volksrechtgesetzes (VRG) eine probeweise Einführung der elektronischen Stimmabgabe vorsieht.

<sup>92</sup> Vgl. zu den beiden letzt genannten Themen oben, 7.1.

# 8. Personelles

Im letzten Tätigkeitsbericht wurde die Hoffnung ausgedrückt, dass der Stabsstelle für Datenschutz ein Teilzeitsekretariat zur Verfügung gestellt wird. Dem wurde bereits im Februar 2004 nachgekommen.

Im Dezember konnte der DSB auf eine zwei jährige Tätigkeit zurück blicken. Diese war auch durch den personalen Engpass geprägt. Das Ressort Justiz, dem der DSB administrativ zugeteilt ist, wurde in einem Schreiben, in dem Bilanz gezogen wurde, gebeten, dafür zu sorgen, dass dem DSB ein Stellvertreter zugeteilt wird. Ohne einen solchen Stellvertreter ist die Wahrnehmung der gesetzlichen Aufgaben, die dem DSB zukommen, nicht in einem befriedigenden Ausmass möglich.

Art. 23 DSV sieht vor, dass die Regierung mindestens einen Datenschutzberater ernennt. Diese Bestimmung wurde bisher noch nicht umgesetzt. Die Praxis zeigt, dass sich bei den Behörden naturgemäss sehr viele datenschutzrechtliche Fragen stellen. Die Stabsstelle für Datenschutz ist auf Grund der personellen Beschaffenheit nicht in der Lage, diesen Fragen in einem befriedigenden Ausmass nachzukommen. Deshalb wurde das Ressort Justiz bereits im August 2004 auf diese Bestimmung hingewiesen und gebeten, darauf hinzuwirken, dass Art. 23 DSV umgesetzt wird.

# 9. Ausblick

Die Vorhaben, die für 2004 als prioritär qualifiziert wurden und nicht abgeschlossen werden konnten, sind als Aufgaben für 2005 zu übernehmen. Es geht dabei um Folgendes:

- Abschluss des Aufbaus und Veröffentlichung des Registers;
- Überprüfung der ZPV auf Datenschutzkonformität;
- Durchführung einer verwaltungsinternen Schulungsveranstaltung über den Datenschutz;
- Erstellung einer Broschüre «Datenschutz in der Schule»;<sup>93</sup>

## NEUE PRIORIÄTEN FÜR 2005:

Die Öffentlichkeit konnte bisher nicht in einem befriedigenden Ausmass über den Datenschutz allgemein und die Rechte der einzelnen Personen im Besonderen informiert werden. Dies

muss sich ändern. Deshalb ist für 2005 geplant, eine erste **öffentliche Veranstaltung zum Datenschutz** durchzuführen. Dazu ist es ein weiteres Ziel, eine **Informationsbroschüre** für die Öffentlichkeit in Angriff zu nehmen.

Zudem dürften bei einem allfälligen Beitritt Liechtensteins zu den **Abkommen von Schengen und Dublin**<sup>94</sup> weitere Aufgaben auf die Stabsstelle für Datenschutz zukommen, denn der Gemeinsamen Kontrollinstanz des Schengener Durchführungsabkommens sind die nationalen Datenschutzbehörden jedes Schengenstaates vertreten.<sup>95</sup>

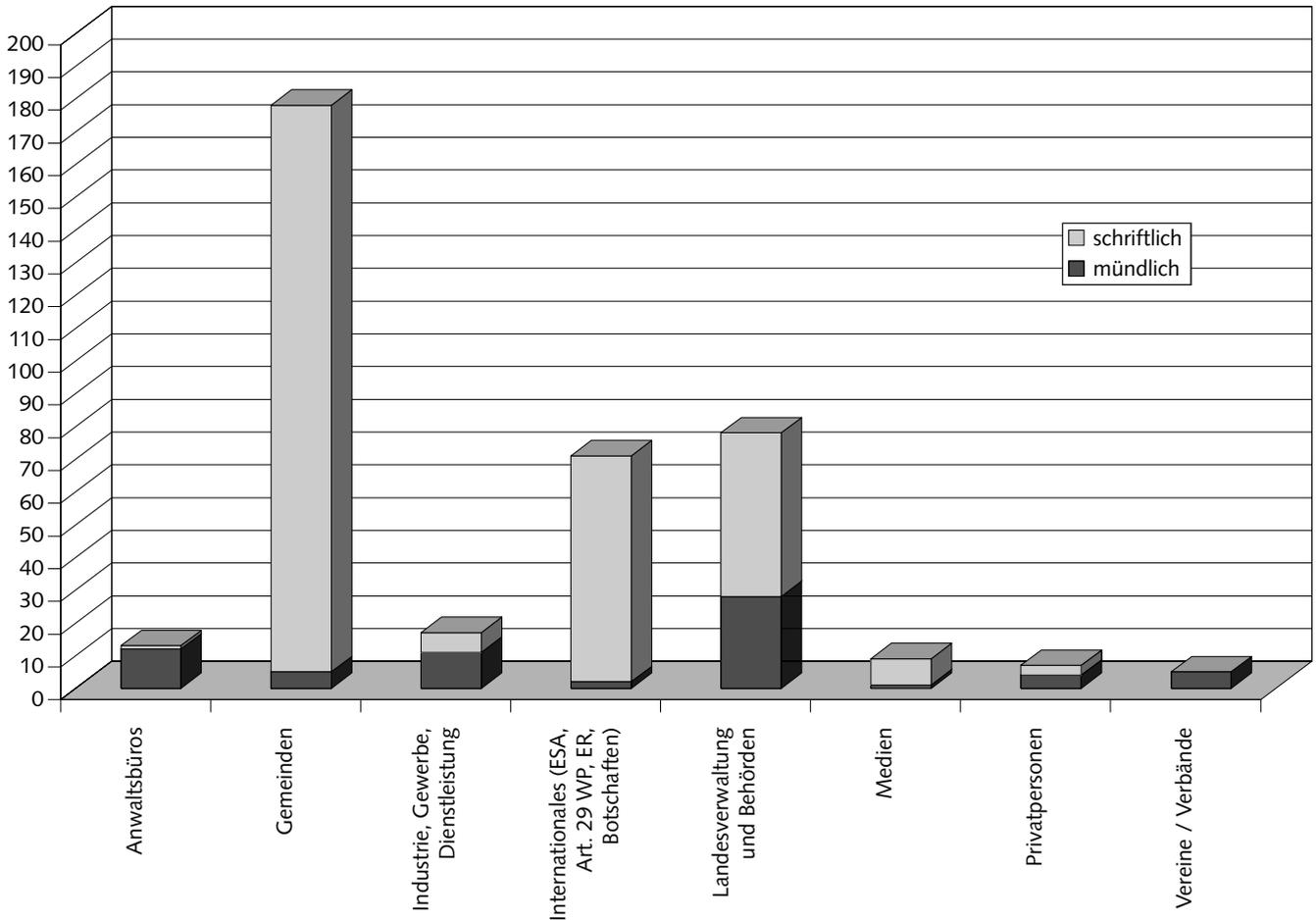
<sup>93</sup> Es sei daran erinnert, dass noch nicht definitiv fest steht, ob und in welcher konkreten Form dieses Vorhaben fort gesetzt wird.

<sup>94</sup> Vgl. dazu oben, 7.1.

<sup>95</sup> Vgl. Sechster Tätigkeitsbericht der Gemeinsamen Kontrollinstanz Schengen (2002 – 2003), Seite 5. Der EDSB hat das Abkommen aus dem Blickwinkel des Datenschutzes untersucht und kommt zum Schluss, dass der Datenschutz in der Schweiz bei einem Beitritt zum Schengener Abkommen gestärkt wird: <http://www.edsb.ch/d/doku/jahresberichte/tb9/tb9d.pdf>, 3.1.6.

# Anhang

## ANFRAGEART



## GESETZESTHEMEN

	Anwaltsbüros	Gemeinden	Industrie, Gewerbe, Dienstleistung	Internationales (ESA, Art. 29 WP, ER, Botschaften)	Landesverwaltung und Behörden	Medien	Privatpersonen	Vereine / Verbände	Gesamtergebnis
Anmeldung, Datensammlungen		1	2						3
Auskunftsrecht	1				1				2
Datenbekanntgabe	1	173	7	1	39		3	3	227
DS Allgemein	7	4	5	68	13	9	3	2	111
Gesetzesvorlagen					22				22
Internationales (Ausser Übermittlungen ins Ausland)				1					1
Sicherheit	1		2		1		1		5
Übermittlungen ins Ausland	1		1	1	2				5
Überwachung am Arbeitsplatz	2								2
<b>GESAMTERGEBNIS</b>	<b>13</b>	<b>178</b>	<b>17</b>	<b>71</b>	<b>78</b>	<b>9</b>	<b>7</b>	<b>5</b>	<b>378</b>



**Stabsstelle für Datenschutz**

Herrengasse 6

FL-9490 Vaduz

Tel. +423 236 60 90

Fax +423 236 60 99

E-Mail: [info@sds.llv.li](mailto:info@sds.llv.li)

<http://www.sds.llv.li>