DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Tätigkeitsbericht 2010

Datenschutzstelle des Fürstentums Liechtenstein

INHALTSVERZEICHNIS

I. VORWORT

Dies ist unser 9. Tätigkeitsbericht.

Auch vergangenes Jahr konnten wir wieder zahlreiche Anfragen von anderen Behörden, Unternehmen und Bürgern beantworten. Einige davon werden im Bericht ausführlich dargestellt, da sie aus unserer Sicht für die Öffentlichkeit von Interesse sind. Daneben waren unsere Aktivitäten von folgenden Schwerpunkten geprägt:

- Im Rahmen einer Untersuchung von Datenflüssen, insbesondere von Gesundheitsdaten, haben wir angeregt, dass die *„Analyse Sozialstaat"* als Grundlage für eine Analyse der Datenflüsse im Bereich der Sozialbeiträge herangezogen wird. Mit einer solchen kann die Abhängigkeit verschiedener Sozialbeiträge erkannt, und in Fällen von Missbräuchen von Sozialbezügen wahrscheinlich auch Kosten gespart werden (siehe 1.1).
- Bekanntermassen plant Google, weltweit Strassenansichten zu sammeln, um diese im Internet zu veröffentlichen. Vor dieser Entwicklung wird auch Liechtenstein nicht verschont. Wir standen in einem intensiven Kontakt mit Google zur Verwirklichung von *Google Street View*. Nach unserem Wissen wurden bisher aber noch keine Aufnahmen gemacht (siehe 1.2).
- Die *Vorratsdatenspeicherung* von Kommunikationsdaten im elektronischen Bereich ist ebenfalls offiziell in Liechtenstein angekommen. In Europa sehr umstritten und in Deutschland abgeschafft, wurde diese Pflicht dennoch in Liechtenstein eingeführt. Immerhin aber mit einer neuen und ausdrücklichen Kontrollkompetenz der Datenschutzstelle. Wir haben mit der Vorbereitung einer Kontrolle begonnen (siehe 1.3).
- Liechtenstein ist neu am *Krebsregister* St. Gallen-Appenzell angeschlossen. Wir konnten bei der Vorbereitung von Lösungsvorschlägen mitarbeiten. Die Sicherstellung des Datenschutzes ist zentral für ein funktionierendes Krebsregister (siehe 1.4).
- Aus Anlass des Europäischen Datenschutztages am 28. Januar 2010 haben wir wieder gemeinsam mit der Hochschule eine *öffentliche Veranstaltung* organisiert. Thema waren die Suchmaschinen im Internet (siehe 2.1).
- Die Sensibilisierung von Jugendlichen ist ein Thema, dem sich verschiedene Institutionen widmen. Wir haben im Rahmen des Präventionsprojektes *„Gateway – Abenteuer Neue Medien"* des Amtes für Soziale Dienste mitgearbeitet (siehe 2.1).
- Die Arbeiten für einen künftigen Beitritt zu *„Schengen" und „Dublin"* konnten nicht im gewünschten Masse vorangetrieben werden. Der Zeitplan wurde durch politische Entwicklungen in Brüssel bzw. im Ausland beeinflusst, sodass der Beitritt wahrscheinlich 2011 erfolgen wird. Immerhin konnten wir aber das interne Wissen zur Durchführung von Kontrollen aufbauen, die durch „Schengen" und „Dublin" gefordert werden und an den entsprechenden Sitzungen als Beobachter teilnehmen (siehe 4.2).
- In der *International Working Group on Data Protection in Telecommunications* wurde das Arbeitspapier „Mobile Verarbeitung personenbezogener Daten und Datensicherheit" angenommen, welches durch uns initiiert und massgeblich mitgestaltet wurde (siehe 4.6).
- Der Schutz der Privatsphäre kann in einer zusammenwachsenden Welt nicht in Liechtenstein isoliert angegangen werden. Gerade im Bereich der Privatsphäre gibt es zahlreiche Themen, die eine europäische, oder gar internationale, Lösung fordern. So hat die Europäische Kommission eine *Revision der Datenschutzrichtlinie* begonnen. Dieser Prozess wird einige Jahre dauern. Als EWR-Mitglied ist es wichtig, diesen Prozess, wie weitere Entwicklungen zu verfolgen, um mit technologischen Entwicklungen sowie der Tendenz zu einer sich globalen Datenbearbeitung Schritt halten zu können (siehe 5).

Der Einsatz für die Belange der Privatsphäre wäre ohne die aktive Unterstützung der Regierung, des Landtags und der Landesverwaltung nicht möglich. Deshalb möchte ich an dieser Stelle den Landtagsabgeordneten, Regierungsmitgliedern und Regierungsmitarbeitern sowie Kollegen in der Landesverwaltung, und last but not least unserem Team, meinen Dank für die gute Zusammenarbeit aussprechen. Aber auch allen anderen, die mit Anregungen, Anfragen oder Beschwerden dazu beigetragen haben, dass die Belange des Schutzes der Privatsphäre berücksichtigt und oft auch verbessert werden können, gilt mein aufrichtiger Dank.

Vaduz, im April 2011

Dr. Philipp Mittelberger
Datenschutzbeauftragter

II. BERICHTERSTATTUNG 2010

Die Zahl der Anfragen, die an uns gerichtet werden, nimmt weiterhin zu. Im vergangenen Jahr wurden *so viele Anfragen wie noch nie* an uns gestellt.[1] Im Berichtsjahr gingen insgesamt 523 Anfragen ein. Das bedeutet gegenüber dem Vorjahr eine Zunahme von 92 Anfragen. Dies kann gewiss auf ein weiterhin *steigendes Bewusstsein* für den Schutz der Privatsphäre zurückgeführt werden.

Es würde den Rahmen dieses Berichtes sprengen, alle Anfragen darzustellen. Immerhin sollen aber einige Fragen und deren Beantwortung dargestellt werden, die für die Öffentlichkeit interessant sein dürften.

1. Fälle aus unserer Beratungspraxis

1.1 Wahrnehmung gesetzlicher Rechte/Beschwerden

Die hier aufgeführten Fälle beschreiben Themen, welche auch in anderen Abschnitten behandelt werden könnten. Da es sich durchwegs um Fälle handelt, in denen sich besorgte Personen an uns wandten, sollen sie hier dargestellt werden.

Darf ein **nicht-obsorgeberechtigter Elternteil** von einem Amt **Informationen** in Bezug auf Massnahmen bekommen, die das Amt zum **Kindeswohl** getroffen hat? Das Amt gewährte zwar Akteneinsicht, kam dem Gesuch um Auskunft jedoch nicht nach. Wir empfahlen der betroffenen Person, vom Amt eine Verfügung zu verlangen, damit diese vor der Datenschutzkommission angefochten werden kann.[2] Der Fall ist noch nicht abgeschlossen.

Allgemein stellt sich die Frage, ob und inwiefern die Verfügungen von Behörden in Datenschutzfragen die **Rechtsmittelbelehrung** nach Art. 34 Buchstabe b Datenschutzgesetz (DSG) berücksichtigen. Uns ist zumindest kein Fall bekannt und dies nach acht Jahren der Geltung des Gesetzes. Dies ist erstaunlich, denn einerseits ist der Begriff der „Behörde" im DSG sehr weit und andererseits geht es aufgrund der Querschnittmaterie des Datenschutzes sehr oft um Personendaten. Wir fragten bei der Datenschutzkommission (DSK) nach der bisherigen Fallpraxis und werden diese Angelegenheit weiterverfolgen.

Bereits im Vorjahr war bei uns eine Beschwerde zur **Bekanntgabe bzw. dem Austausch von Gesundheitsdaten durch verschiedene Behörden eingegangen**. Das Thema ist sehr komplex. Wir fragten die entsprechenden Behörden nach deren Praxis. Die Antworten zeigten ein Netz von Institutionen auf, die, je nach Einzelfall, Gesundheitsdaten offenbar benötigen. Es ist schwierig, einen Überblick über die Datenflüsse im Einzelnen zu erhalten. Allgemein besteht ein **Spannungsfeld** zwischen **Amtshilfe** einerseits und **Amtsgeheimnis** andererseits. Zu diesem Spannungsfeld hatten wir ein Rechtsgutachten eingeholt.[3] Dieses geht insbesondere auf die genannte Problematik zwischen der Zusammenarbeit der Sozialhilfeorgane auf der einen und deren Schweigepflicht auf der anderen Seite ein.[4] Darüber hinaus haben wir in diesem Zusammenhang auch festgestellt, dass für die Bekanntgabe von Daten im Sozialhilfegesetz eine gesetzliche Grundlage fehlt, was bei einer Gesetzesrevision berücksichtigt werden sollte.

Darüber hinaus haben wir eine **Analyse** über die **Datenströme** im Bereich der **Sozialleistungen** angeregt. Diese könnte sich auf die „Analyse Sozialstaat Liechtenstein" der Regierung stützen.[5] Darin wurden 25 sozialstaatliche Leistungen untersucht. Ein grosser Teil der Analyse beschäftigte sich mit der Kostenentwicklung und Finanzierung der einzelnen Bereiche. Wichtige Parameter, wie gesetzliche Grundlagen, Anspruchsvoraussetzungen und Tatbestandsmerkmale für den Versicherungsschutz, wurden dabei ebenfalls unter die Lupe genommen. Die Untersuchung zeigt insgesamt klar nicht nur eine gestiegene Anspruchshaltung an den Sozialstaat, sondern kommt auch zum Ergebnis, dass der Sozialstaat selbst eine „Bedürfnishaltung" geschaffen hat.

1 523 Anfragen gegenüber 431 im Vorjahr; vgl. dazu Details im Anhang.

2 Gestützt auf Art. 34 Datenschutzgesetz. § 178 ABGB enthält zudem eine Bestimmung über die Information durch den obsorgeberechtigten Elternteil.

3 Vgl. dazu Tätigkeitsbericht 2009, 1.8.

4 Gemäss Art. 30 Sozialhilfegesetz (SHG) sind die in der Sozialhilfe tätigen Personen verpflichtet, ein Geheimnis, das in der Ausübung ihrer Tätigkeit anvertraut oder bekannt wurde, zu wahren. Sie sind zur Offenlegung des Geheimnisses nur in Erfüllung einer ausdrücklichen gesetzlichen Pflicht oder gegenüber anderen in der Sozialhilfe tätigen Personen in unerlässlichem Ausmass oder aufgrund einer Ermächtigung des Berechtigten befugt.

5 Vgl. Isabel Frommelt, Analyse Sozialstaat Liechtenstein, basierend auf der Entwicklung der Sozialausgaben des Landes 1995-2004. Die Studie wurde von der Regierung im September 2005 herausgegeben. http://www.llv.li/pdf-llv-rk-analyse_sozialstaat_liechtenstein.pdf.

Daher scheint es wenig verwunderlich, dass immer wieder Fälle von *Missbräuchen beim Bezug von Sozialleistungen* in der öffentlichen Diskussion stehen. Informationen sind eine wesentliche Voraussetzung für die Ausschüttung bzw. Inanspruchnahme von Sozialleistungen. Bedingt durch die Komplexität des Themas fällt es daher manchmal schwer, den Überblick zu behalten. Unserer Ansicht nach fehlt eine landesweite Untersuchung darüber, wie die unterschiedlichen Stellen, die wirtschaftliche Hilfe ausschütten, miteinander vernetzt sind und insbesondere, welche Informationen zwischen den einzelnen Stellen fliessen und ausgetauscht werden. Wir machten die Regierung darauf aufmerksam, dass eine solche Analyse aus unserer Sicht eine gute Basis für eine Gesamtbetrachtung bilden würde. So könnten langfristig mehr Transparenz geschaffen, allfällige Missbräuche vermieden und eventuelle Doppelgleisigkeiten reduziert werden. Dies würde nicht zuletzt auch zu einer nachhaltigen Finanzierung des Sozialstaates beitragen.

Wir wurden in diesem Jahr vermehrt mit Anfragen von Internetnutzern konfrontiert, die veröffentlichte **persönliche Daten aus dem Internet** (z.B. in Foren oder anderen Internetseiten) **gelöscht** haben wollten. Wir konnten die Betroffenen beraten und sie teilweise bei der Durchsetzung ihrer Lösch- und Berichtigungsbegehren im Internet konkret unterstützen. In den meisten Fällen waren Forenbetreiber und Webmaster in der Beantwortung von Löschbegehren kooperativ. Insbesondere bei fehlenden Zuständigkeiten bei den Plattformbetreibern, veralteten Kontaktdaten oder ungepflegten Internetauftritten können sich jedoch Probleme ergeben. Wie schon das Jahr zuvor wiesen wir darauf hin, dass die bekannten Suchmaschinen ausschliesslich die Inhalte im öffentlich verfügbaren Internet erfassen.[6] Eine *Filterung der Suchresultate und Suchtrefferlisten* ist in der Regel *nicht vorgesehen*. Durch den regelmässig wiederholten Besuch der im Suchindex erfassten Seiten im Internet werden Änderungen durch die Suchmaschinenbetreiber erkannt und der Suchindex entsprechend angepasst. Google weist z.B. darauf hin, dass die öffentlich verfügbaren Informationen im Internet zuerst auf den entsprechenden Webseiten angepasst oder entfernt werden müssen, bevor diese in den Suchtrefferlisten nicht mehr ausgegeben werden. Eine *Filterung konkreter Inhalte sei nicht möglich*.

Ein geschiedener Ehemann zahlt Unterhalt für seine Kinder. In der **Scheidungsvereinbarung** ist festgehalten, dass sich die **Höhe des Unterhalts** nach den Einkommensverhältnissen der geschiedenen Frau richtet. Wenn der Mann erfährt, dass sich ihr Arbeitspensum erhöht hat, darf er dann z.B. von der *Steuerverwaltung* erfahren, wie hoch ihr derzeitiges Einkommen ist? Nach Art. 23 Abs. 1 Buchstabe d DSG können Behörden Daten auch bekannt geben, wenn der Empfänger glaubhaft macht, dass die betroffene Person die Einwilligung verweigert oder die Bekanntgabe sperrt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren. Der betroffenen Person ist dabei vorher, wenn möglich, Gelegenheit zur Stellungnahme zu geben.[7] Im erwähnten Fall geht es um die *Klärung eines Rechtsanspruches*. Einer Bekanntgabe nach Art. 23 Abs. 1 Buchstabe d DSG steht somit nichts entgegen.

Eine Person beschwerte sich darüber, dass für eine **Vereinsmitgliedschaft etliche Nachweise** gefordert wurden: Einerseits wurden Kopien verschiedener Unterlagen verlangt, die sich als nicht notwendig erwiesen haben und so dem Verhältnismässigkeitsprinzip widersprachen. Anderseits wurde auch eine Einkommensbestätigung bzw. ein Lohnausweis angefordert. Diese enthielten weitere, für die Zwecke des Vereins unnötige Angaben, weshalb ein solcher Nachweis ebenfalls dem Grundsatz der „*Datensparsamkeit*" widersprach. Zur Klärung der finanziellen

6 Vgl. Tätigkeitsbericht 2009, S. 12 ff.

7 In unseren Richtlinien zur Datenbekanntgabe durch Behörden ist zu lesen (http://www.llv.li/amtsstellen/richtlinien_fuer_die_bekanntgabe_von_daten_durch_behoerden): „Bevor in einem solchen Fall…, Auskunft gegeben wird, muss sichergestellt sein, dass es tatsächlich um die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen geht. Der Antragsteller hat dies zu belegen. Telefonische Auskünfte sind in solchen Fällen sehr problematisch, es sei denn, die Person, die das Auskunftsbegehren telefonisch stellt, ist klar identifiziert. Das Gesetz sieht vor, dass der betroffenen Person vor der Bekanntgabe der Daten Gelegenheit zur Stellungnahme gegeben werden muss, wenn dies möglich ist. Auf eine Stellungnahme darf z.B. dann verzichtet werden, wenn die betroffene Person nicht erreichbar ist oder nach Ablauf einer gesetzten Frist nicht reagiert hat. Die Behörde muss aber auf alle Fälle die betroffene Person kontaktieren. Erst, wenn eine Person auch auf eine schriftliche Aufforderung nicht reagiert bzw. die Gründe, welche die betroffene Person anführt, von der Behörde nicht als stichhaltig oder genügend angesehen werden, darf bspw. der Arbeitgeber bekannt gegeben werden."

Verhältnisse benötigt der Verein jedoch gewisse Angaben, da die Mitgliedschaft einkommensabhängig ist. Der Verein sah eine lediglich auf Freiwilligkeit beruhende Angabe der Lohnhöhe als nicht ausreichend. Eine datenschutzfreundliche und gleichermassen praktikable Lösung wurde in der Verwendung eines Formulars gefunden, welches von der Gemeindesteuerverwaltung ausgefüllt und unterzeichnet wird.

Eine Person wandte sich an uns, da **Postsendungen** *wiederholt* und *versehentlich* an eine andere Person mit demselben Namen geschickt wurden. Diese Person *öffnete diese Briefsendungen offenbar bewusst* und **beschaffte** sich somit **Personendaten**, die nicht für sie bestimmt sind. Nach § 118 des Strafgesetzbuches ist mit Freiheitsstrafe bis zu 3 Monaten oder mit Geldstrafen bis zu 180 Tagessätzen zu bestrafen, wer einen nicht zu seiner Kenntnisnahme bestimmten verschlossenen Brief oder ein anderes solches Schriftstück öffnet. Somit kann dieser Sachverhalt zu einer strafrechtlichen Verurteilung führen.[8]

Das **Auskunftsrecht** gilt nach der Rechtsprechung des Europäischen Gerichtshofes (EuGH) als eine Voraussetzung für die **Geltendmachung der anderen gesetzlichen Rechte**, die auf **Sperrung, Berichtigung und Löschung**. Denn nur wenn man weiss, wer welche Daten über einen bearbeitet, können die anderen datenschutzrechtlichen Rechte wie Berichtigung, Widerspruch oder Löschung ausgeübt und durchgesetzt werden. Das Auskunftsrecht umfasst nach dieser Rechtsprechung auch Daten der Vergangenheit, wobei der Gesetzgeber eine Frist für die Aufbewahrung dieser Information sowie einen darauf abgestimmten Zugang zu ihr festlegen muss.[9] Wir erhielten verschiedene Anfragen zum *Auskunftsrecht*, die im Folgenden dargestellt werden sollen:

- Was gilt, wenn nicht die betroffene Person selbst das Auskunftsrecht geltend macht, sondern ihre *Erben oder Nachkommen*? Nach Art. 1 Abs. 7 Datenschutzverordnung (DSV) ist Auskunft über Daten von verstorbenen Personen zu erteilen, wenn der Gesuchsteller ein Interesse an der Auskunft nachweist und keine überwiegenden Interessen von Angehörigen der verstorbenen Person oder von Dritten entgegenstehen. Das Auskunftsrecht gilt nicht absolut. So kann die Auskunft nach Art. 12 DSG insbesondere *verweigert* werden, wenn dies ein Gesetz vorsieht oder wegen *überwiegender Interessen eines Dritten erforderlich* ist oder, im Fall von *Privaten*, soweit *eigene überwiegende Interessen* es erfordern und sie die Personendaten *nicht an Dritte bekannt geben*. Dies gilt selbstverständlich auch im Falle der Geltendmachung des Rechts durch Erben oder Nachkommen.
- Was ist, wenn eine Behörde auf ein Auskunftsbegehren nicht antwortet? Diese Frage ist berechtigt, denn im Gegensatz zu privaten Personen ist eine *vorsätzlich falsche oder unvollständige Auskunft bei Behörden nicht strafbar*.[10] Möglicherweise ist es einer Behörde nicht klar, dass es um die Geltendmachung eines gesetzlichen Rechtes geht. Zur Klarstellung und als Hilfestellung für die Praxis haben wir Musterschreiben erstellt, die auf unserer Internetseite abrufbar sind.[11] Wird ein formelles Auskunftsgesuch gestellt und innerhalb der vorgeschriebenen dreissig Tage[12] nicht beantwortet, kann dies unter Umständen als formelle Rechtsverweigerung interpretiert werden,[13] wodurch der Rechtsmittelweg nach dem Landesverwaltungspflegegesetz eröffnet wird.
- Neben dem Auskunftsrecht nach dem DSG gibt es in Spezialgesetzen Sonderregelungen, wie zum Beispiel in Art. 14 Abs. 2 Ärztegesetz, wonach die Patienten jederzeit Kopien der sie betreffenden Krankenunterlagen verlangen können.[14]
- Eine weitere Sonderregelung des Auskunftsrechts findet sich in Art. 34h *Polizeigesetz* bezüglich der Bearbeitung von Personendaten im Rahmen des Staatsschutzes oder zur Vorbeugung von Straf-

8 Der Tatbestand von § 118 ist bereits mit dem Öffnen des Briefes erfüllt. Es ist nicht nötig, dass der Täter sich oder einem anderen Unbefugten Kenntnis vom Inhalt verschaffen wollte, siehe dazu auch Ernst Fabrizy: Strafgesetzbuch – Kurzkommentar, 10. Aufl., Wien 2010, S. 379. Eine allgemeine Regelung enthält Art. 39 DSG: Danach ist ein unbefugtes Beschaffen von Personendaten aus einer Datensammlung nur strafbar, wenn es sich um besonders schützenswerte Personendaten und/oder Persönlichkeitsprofile handelt.

9 Vgl. Tätigkeitsbericht 2009, Fussnote 41.

10 Art. 40 Abs. 1 DSG.

11 http://www.llv.li/form-llv-dss-musterschreiben.

12 Art. 1 Abs. 4 DSV.

13 Vgl. Hugo Vogt: Das Willkürverbot und der Gleichheitsgrundsatz in der Rechtsprechung des liechtensteinischen Staatsgerichtshofes, Liechtenstein Politische Schriften (LPS), Band 44, Schaan 2008, S. 362 ff und Andreas Kley: Grundriss des liechtensteinischen Verwaltungsrechts, LPS, Band 23, Vaduz 1998, S. 246 ff.

14 Im Fall von Gesundheitsdaten sieht Art. 11 Abs. 3 DSG vor, dass der Inhaber der Datensammlung der betroffenen Person diese durch einen von ihr bezeichneten Arzt mitteilen lassen kann.

taten. Dabei geht es um ein nur *indirektes* Auskunftsrecht: Das Auskunftsbegehren müssen interessierte Personen an uns stellen, wir leiten das Begehren in Stellvertretung für die betroffenen Personen an die Landespolizei weiter.[15]

Nach der Praxis des Bundesgerichtes in der Schweiz (die für Liechtenstein aufgrund der Parallelen im Persönlichkeitsrecht wichtig ist) ist die *Verletzung des Rechts am eigenen Bild* bereits zu bejahen, wenn jemand ohne Zustimmung um seiner Person willen fotografiert oder eine bestehende Aufnahme ohne seine Einwilligung veröffentlicht wird. In bestimmten Fällen ist eine Einwilligung nicht unbedingt erforderlich. Voraussetzung ist, dass die abgebildete Person für Dritte erkennbar, also identifizierbar ist.[16] Dabei dürfen aber in den Gemein- oder Öffentlichkeitsbereich fallende Tatsachen von jedermann nicht nur ohne Weiteres wahrgenommen, sondern grundsätzlich auch weiterverbreitet werden.[17] Dies dürfte bedeuten, dass ein solches Recht, zumindest in Bezug auf die *Veröffentlichung* von Fotos, besteht, ausser, wenn sich das Kind im Gemein- oder Öffentlichkeitsbereich aufhält.[18] Ob es für die generelle Aufnahme von Fotos gilt, muss offenbleiben.

15 Vgl. Tätigkeitsbericht 2008, 2.4. und 6, Tätigkeitsbericht 2007, 4.4.
16 BGE 136 III 413 (mit Hinweisen auf die Rechtsprechung).
17 BGE 136 III 413 (mit weiteren Hinweisen auf die Rechtsprechung).
18 Die Geheim- oder Intimsphäre umfasst laut BGE 97 II 101 Tatsachen und Lebensvorgänge, die der Kenntnis aller andern Leute entzogen sein sollen, mit Ausnahme jener Personen, denen diese Tatsachen besonders anvertraut wurden. Zur Privatsphäre gehört der übrige Bereich des Privatlebens; es sind ihr also alle jene Lebensäusserungen zuzurechnen, die der Einzelne mit einem begrenzten, ihm relativ nahe verbundenen Personenkreis teilen will, so mit Angehörigen, Freunden und Bekannten, jedoch nur mit diesen. Was sich in diesem Kreis abspielt, ist zwar nicht geheim, da es von einer grösseren Anzahl von Personen wahrgenommen werden kann. Im Unterschied zum Geheimbereich handelt es sich jedoch um Lebenserscheinungen, die nicht dazu bestimmt sind, einer breiteren Öffentlichkeit zugänglich gemacht zu werden, weil die betreffende Person für sich bleiben und in keiner Weise öffentlich bekannt werden will. Diese Unterscheidung verschiedener Lebenskreise ist zweckmässig, da sie die Abgrenzung des rechtlich geschützten Bereiches der Persönlichkeit erlaubt: Die Privatsphäre gehört zusammen mit der Geheimsphäre zum rechtlich geschützten Persönlichkeitsbereich. Während die in den Gemein- oder Öffentlichkeitsbereich fallenden Tatsachen von jedermann nicht nur ohne Weiteres wahrgenommen, sondern grundsätzlich auch weiterverbreitet werden dürfen, geniessen die zur Privatsphäre gehörenden Tatsachen mindestens den Schutz vor öffentlicher Bekanntmachung; sie dürfen nur im engeren Lebenskreise des Privatbereichs Drittpersonen zur Kenntnis gebracht werden, dies im Unterschied zu den in die Geheimsphäre fallenden Lebensäusserungen, die überhaupt nicht weiterverbreitet werden dürfen.

1.2 Technologischer Datenschutz

Der Suchmaschinenbetreiber **Google** betreibt im Internet den Service **„Street View"**.[19] Wir standen in intensivem Kontakt mit Google, wobei konkrete Rahmenbedingungen für die Durchführung der Fahrten in Liechtenstein diskutiert wurden. Wir orientierten uns dabei an europäischen Entwicklungen, vor allem an der Art. 29 Datenschutzgruppe und insbesondere an Luxemburg, Österreich, Deutschland oder Griechenland.[20] Zusätzlich ging dazu eine Meldung[21] der Regierung bei uns ein. Diese war gegenüber dem Vorhaben von Google sehr kritisch und bei unseren Abklärungen entsprechend zu berücksichtigen.

Google Street View wurde von den Datenschutzbehörden in *Europa nicht einheitlich bewertet*. Die Besonderheit bei Google Street View liegt unserer Meinung nach darin, dass nicht einzelne Strassenansichten im Internet veröffentlicht werden. Es geht um die Strassenzüge des ganzen Landes, die systematisch erfasst und anschliessend veröffentlicht werden sollen. Dabei ist zu berücksichtigen, dass einzelne Personen an Orten wiedererkannt werden können, an denen sie nicht gesehen werden möchten oder sich in Situationen wiederfinden, die ihnen unangenehm sind. Dies gilt auch für die Erkennbarkeit von Autokennzeichen, die Rückschlüsse auf die Aufenthaltsorte von Fahrern oder Haltern zulassen. Es ist kritisch, wenn Ansichten von Wohnungen oder (privaten) Häusern veröffentlicht werden. Möglicherweise könnten Kriminelle örtliche Gegebenheiten zu Einbruchsversuchen einfach am Computer auskundschaften. Aber auch eine Beurteilung der wirtschaftlichen und sozialen Verhältnisse der Bewohner ist über diesen Weg nicht auszuschliessen. Wir wiesen darauf hin, dass Liechtenstein sehr klein ist und ländliche Strukturen aufweist. Eine Anonymität ist im Vergleich zu anderen Ländern nur schwierig zu gewährleisten. Liechtenstein kann also gewiss als ein Sonderfall bezeichnet werden.

19 Vgl. auch Tätigkeitsbericht 2009, 1.2. S. weiters http://maps.google.com/help/maps/streetview/.
20 Zu Österreich: http://www.dsk.gv.at/site/6733/default.aspx, zu Luxemburg: http://www.cnpd.public.lu/de/actualites/national/2009/09/google-street-view/index.html?highlight=Google%22Street%22View und zu Griechenland: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/DECISION%2091-2009.PDF.
http://www.edoeb.admin.ch/themen/00794/01124/01595/index.html?lang=de.
21 Im Sinne von Art. 30 DSG.

Wir forderten verschiedene Massnahmen, insbesondere in Bezug auf die Information der Bevölkerung über den Zeitpunkt und die Fahrtroute sowie über die Aufschaltung der Bilder im Internet. Auch die automatisierte Unkenntlichmachung *(engl. blurring)* von Gesichtern und Autonummern war ein Thema, da gerade in der Anfangsphase der Veröffentlichung zahlreiche Gesichter und Autokennzeichen ohne Einschränkung klar erkenn- und somit identifizierbar sind. Die Kameras befinden sich bei der Aufnahme in einer Höhe von 2.75 m. So wird über natürliche Hindernisse und Hecken von Privatgrundstücken gesehen und die dortigen Verhältnisse werden aufgezeichnet. Einem Fussgänger bleibt dieser Einblick verwehrt.

Diese Aspekte sind auch Gegenstand eines laufenden Gerichtsverfahrens in der Schweiz. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) kam nach eingehender Prüfung von Google Street View zum Schluss, dass dem Schutz der Privatsphäre trotz zahlreicher Massnahmen vonseiten des Anbieters nicht in allen Fällen Genüge getan wird. Aus diesem Grund richtete er mehrere Empfehlungen an Google. Da diese Empfehlungen durch Google nicht fristgerecht umgesetzt worden waren, zog der EDÖB den Fall vor das Bundesverwaltungsgericht, dessen Entscheidung noch aussteht. Aufgrund der Nähe des liechtensteinischen Persönlichkeitsrechts zu dem der Schweiz dürfte das Urteil für Liechtenstein sehr wichtig sein. Wir erhielten mehrere Anrufe und Anfragen von Hausbesitzern sowie Personen, die sich gegen die Erfassung ihrer Grundstücke und Häuserfassaden ausgesprochen hatten. Eine *Entfernung der Bilder* im Nachhinein würden sie nicht akzeptieren. Wir informierten die Öffentlichkeit über die Medien zum Thema.[22] In Beantwortung der Meldung der Regierung machten wir darauf aufmerksam, dass gesetzgeberische Massnahmen getroffen werden sollten. Damit wäre das Ergebnis des Verfahrens in der Schweiz nicht ganz so wichtig. Zentral wird das Recht des einzelnen Betroffenen sein, sich gegen das Vorhaben bei Google zu wehren; denn Widerspruchserklärungen sind empfangsbedürftige Willenserklärungen. Mit anderen Worten sind sie nur gültig, wenn sie Google gegenüber geltend gemacht werden.[23] Bis zum

22 Auch über unsere Internetseite: http://www.llv.li/llv-portal-informationen/aktuelles.htm?reference=141833&checkSum=6B7333CE0810CBDAA9E22C8D86969DE5.

23 David Rosenthal/Yvonne Jöhri: Handkommentar zum Datenschutzgesetz, Zürich 2008, Randnummer 29 zu Art. 12. Dem Hamburgischen Datenschutzbeauftragten, der für Google Street View in Deutschland zuständig ist, machte Google folgende verbindliche Zusagen:

- Google hat verbindlich zugesichert, eine Technologie zur Verschleierung von Gesichtern vor der Veröffentlichung von derartigen Aufnahmen einzusetzen. Google hat verbindlich zugesichert, eine Technologie zur Verschleierung von Kfz-Kennzeichen vor der Veröffentlichung derartiger Aufnahmen einzusetzen.
- Google hat verbindlich zugesichert, Widerspruchsmöglichkeiten zur Entfernung bzw. Unkenntlichmachung eines Gebäudes durch einen Bewohner oder Eigentümer vorzuhalten und derartige Widersprüche zu bearbeiten.
- Google hat verbindlich zugesichert, dass Widersprüche zu Personen, Kennzeichen und Gebäuden bzw. Grundstücken bereits vor der Veröffentlichung von Bildern in einer einfachen Form berücksichtigt werden, mit der Folge, dass die entsprechenden Bilder vor der Veröffentlichung unkenntlich gemacht werden. Voraussetzung ist eine Identifizierung des Grundstücks, der Person oder des Fahrzeugs.
- Google hat verbindlich zugesichert, die geplanten Befahrungen mit einem Hinweis auf die Widerspruchsmöglichkeit im Internet rechtzeitig vorher bekannt zu geben. Die vorhandenen Befahrungspläne werden bis zu 2 Monate im Voraus veröffentlicht und ständig aktualisiert. Google hat die verbindliche Zusage gemacht, die Liste genauer zu gestalten und auf Landkreise und kreisfreie Städte zu erstrecken. Dies wurde zwischenzeitlich umgesetzt.
- Google hat verbindlich zugesagt, dass die Widerspruchsmöglichkeit auch nach der Veröffentlichung noch besteht.
- Die Rohdaten werden nach Aussage von Google zum Zwecke der Weiterentwicklung und Verbesserung der von Google entwickelten Technologie zur Unkenntlichmachung von Gesichtern, Kfz-Kennzeichen und Gebäudeansichten benötigt. Google hat verbindlich zugesichert, die Löschung/Unkenntlichmachung der Rohdaten vorzunehmen, indem die Ergebnisse aus dem Prozess zur Unkenntlichmachung von Gesichtern und Kfz-Kennzeichen in die Rohdaten übernommen werden, sobald die Speicherung und Verarbeitung der Rohdaten nicht mehr für die genannten Zwecke erforderlich ist.
- Google hat verbindlich zugesichert, die Löschung oder Unkenntlichmachung der Rohdaten von Personen, Kfz und Gebäudeansichten vorzunehmen, die aufgrund eines Widerspruchs zu entfernen sind. Die Löschung oder Unkenntlichmachung dieser Daten in den Rohdaten wird bereits vor der Veröffentlichung vorgenommen, wenn der Widerspruch bis zu einem Monat vor Veröffentlichung der Bilder bei Google eingeht. Später oder auch nach Veröffentlichung eingehende Widersprüche führen zu einer Löschung in den Rohdaten binnen 2 Monaten.
- Google hat die Erstellung eines Verfahrensverzeichnisses zugesichert.
- Im Falle von Verknüpfungen des Dienstes durch andere Anbieter behält sich Google in den Nutzungsbedingungen das Recht vor, bei offensichtlicher Verletzung anwendbarer Gesetze, die Schnittstelle zu unterbinden.
- Google hat zugesichert, eine Beschreibung der Datenverarbeitungsprozesse und der technischen und organisatorischen Maßnahmen für Google Street View vorzulegen. Insbesondere gehört hierzu auch eine deutliche Beschreibung des Umgangs mit den widersprechenden Daten von der Entgegennahme des Widerspruchs bis zur endgültigen Löschung bzw. Unkenntlichmachung.
- Widerspruch kann eingelegt werden im Internet unter http://maps.google.de/intl/de/help/maps/streetview/faq.html#q7 oder schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg. Der Link mit dem Text: „FAQ

jetzigen Zeitpunkt sind uns keine Fahrten durch Google in Liechtenstein bekannt. Der Hamburgische Datenschutzbeauftragte spricht von „schwierigen Verhandlungen" mit Google. Dies wird durch unsere bisherigen Erfahrungen bestätigt. Der Hamburgische Datenschutzbeauftragte spricht auch davon, dass das Datenschutzgesetz sich „als eine wenig taugliche Regulierungsgrundlage erweist".[24] Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz schreibt in einer sehr ausgewogenen Stellungnahme: „Es ist so, als würde der juristische Kompass versagen."[25] Bisher hat die Regierung nicht auf unser Anliegen zur Änderung der rechtlichen Grundlagen reagiert. Man darf auf alle Fälle auf den Fortgang dieser Angelegenheit gespannt sein.

Eine Person meldete uns, dass sie beim Ausfüllen der **elektronischen Steuererklärung** in einem Firmennetzwerk **unbeabsichtigt Zugriff** auf **persönliche** und **vertrauliche** Daten eines **Arbeitskollegen** hatte. Eine Überprüfung des Vorfalls ergab Folgendes: Bei der Entwicklung der Applikation war offensichtlich davon ausgegangen worden, dass diese ausschliesslich auf Computern im privaten Umfeld zum Einsatz kommt. Dort greifen die jeweiligen Sicherheitsmassnahmen des Anwenders (Benutzerkennwort, Virenschutz, usw.) und die vom Benutzer eingegebenen und auf der lokalen Festplatte abgespeicherten Daten sind grundsätzlich vor fremdem Zugriff geschützt.

In einem Firmennetzwerk kann es jedoch vorkommen, dass einzelne Arbeitsplätze und somit auch die jeweilige lokale Dateiablage durch mehrere Personen *gemeinsam genutzt* werden. Die Applikation sah jedoch keinen entsprechenden Zugriffsschutz bzw. Trennung von Datenbeständen in einem solchen Mehrbenutzerumfeld vor, wodurch der oben beschriebene Zugriff auf persönliche Daten des Arbeitskollegen möglich war. Von unserer Seite wurde vorgeschlagen, die Benutzerdialoge und Programmhinweise klarer bzw. unmissverständlicher zu gestalten. Insbesondere sollten bei der Nutzung der Software in einem Umfeld, in welchem mehrere Personen sich einen Computer teilen, erweiterte Schutzmassnahmen implementiert werden. Dies können technische Massnahmen (z.B. die Vergabe eines persönlichen Passworts, Verschlüsselung der Daten, usw.) oder begleitende andere Massnahmen (z.B. Hinweise auf die Gefahr der Einsichtnahme durch andere Nutzer bei der Ablage von vertraulichen Daten auf einem gemeinsam genutzten Laufwerk) sein.

Die Verwendung der eindeutigen **Personenidentifikationsnummer** (PEID) sorgt seit Jahren für Diskussionen.[26] Wir erhielten eine Anfrage zur Verwendung der PEID in Systemen ausserhalb der Landesverwaltung: Bei der Durchführung einer Studie, geleitet durch das Amt für Gesundheit, wurde erstmals vor der Datenübermittlung an ein Drittunternehmen zur Auftragsdatenbearbeitung ein alternativer bereichsspezifischer und eindeutiger Personenidentifikator erstellt. Eine Verwendung der landesinternen PEID selbst war nicht zur Erfüllung der Auftragsdatenbearbeitung notwendig. Für die Datenbearbeitung entstanden dadurch keinerlei Einschränkungen. Im Gegenteil: Diese Vorgehensweise hat den Vorteil, dass mit Hilfe eines alternativen Personenidentifikators die Verknüpfung von Daten verschiedener Datensammlungen und -quellen wesentlich erschwert wird.

1.3 Telekommunikation

Mit der letzten **Revision des Kommunikationsgesetzes** (KomG) wurde die Richtlinie zur Vorratsdatenspeicherung in Liechtenstein übernommen. Die **Vorratsdatenspeicherung** von Verkehrsdaten erfolgt verdachtsunabhängig.[27] Deshalb wird bis

Street View (inkl. Widerspruchsmöglichkeiten)" ist nunmehr direkt auf der ersten Seite der Hilfeseiten für Google Maps Deutschland erreichbar. Diese Hilfeseiten erreicht jeder Nutzer direkt aus dem Produkt Google Maps Deutschland, wenn er oben rechts auf den Link „Hilfe" klickt.

- Die bei Google eingelegten Widersprüche werden zeitnah bestätigt. E-Mails mit Widersprüchen werden bereits bestätigt, alle entsprechenden Briefe werden fortlaufend beantwortet.

24 Die Stellungnahmen des Hamburgischen Datenschutzbeauftragten sind derzeit nicht elektronisch verfügbar.

25 http://www.datenschutz.rlp.de/de/aktuell/2010/images/20100415_Stellungnahme_Google_Street_View.pdf

26 Zur PEID vgl. auch Tätigkeitsbericht 2009, 1.2 auf S. 15, Tätigkeitsbericht 2008, 3.1 und Tätigkeitsbericht 2007, 5.1.2, mit dem Hinweis auf das Rechtsgutachten von Giovanni Biaggini, Professor für Staats- und Verwaltungsrecht an der Universität Zürich, Ein Personenidentifikator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes (Art. 13 BV, Dezember 2002), abzurufen unter: http://www.edoeb.admin.ch/themen/00794/01189/index.html?lang=de.

27 Vgl. zur verdachtsunabhängigen Datenspeicherung die Entscheidung der Datenschutzkommission zur Videoüberwachung in der Fussgängerzone Vaduz, Erwägung 4: http://www.llv.li/entscheidung_der_datenschutzkommission_zur_videoueberwachung_in_der_fussgaengerzone_in__vaduz.pdf.

heute heftig über sie diskutiert. Von Datenschutzseite wurde schon früh 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 E-Mail* kommuniziert hat, *wer, wann, welche Onlinedienste* in Anspruch genommen hat.[28] Dies führt zu einem Paradigmenwechsel im Strafrecht in Form eines Generalverdachts – auch gegenüber Unschuldigen.[29] In Deutschland wurde sie vom Bundesverfassungsgericht zu Fall gebracht.[30] In Österreich ist sie bis heute nicht eingeführt. In Liechtenstein wurde sie, wie erwähnt, bereits eingeführt. Immerhin wurde aber unsere gesetzliche Kompetenz ausgebaut: Nach dem neuen Art. 52b des KomG haben wir die Befugnis, den Datenschutz bei der Vorratsdatenspeicherung zu kontrollieren. In den Materialien äussert sich die Regierung hierzu wie folgt: *„Die gegenständliche Bestimmung dient der Regelung der Kontrolle des Datenschutzes betreffend die Datenbearbeitung im Zusammenhang mit der Überwachung einer elektronischen Kommunikation bzw. der Mitwirkung daran und geht insoweit über den sachlichen Anwendungsbereich der Richtlinie 2006/24/EG hinaus, als die Datenschutzstelle nicht nur als Kontrollstelle im Sinne des Art. 9 dieser Richtlinie fungieren soll, sondern – im Interesse einer bürger- und grundrechtsfreundlichen Ausgestaltung des Datenschutzes im Bereich der Überwachung einer elektronischen Kommunikation – jede Form der Datenbearbeitung im Zusammenhang mit der Überwachung einer elektronischen Kommunikation bzw. der Mitwirkung daran nach Art. 52 ff KomG kontrollieren kann und soll.“*[31] Wir waren bei der Revision gegen die Einführung der Vorratsdatenspeicherung in Liechtenstein. Die Regierung hat sich zwar dafür entschieden, aber auch „im Interesse einer bürger- und grundrechtsfreundlichen Ausgestaltung des Datenschutzes“ gehandelt. Der Landtag ist diesem Ansatz gefolgt. Da die Vorratsdatenspeicherung verdachtsunabhängig erfolgt (und deshalb so umstritten ist) und somit jede Person in Liechtenstein betrifft, haben wir mit der Vorbereitung einer entsprechenden Kontrolle begonnen.

Die Lehre in Liechtenstein bezeichnet die voraussetzungslose Vorratserfassung von Verkehrsdaten trotz der strengen Kriterien für den Zugriff auf solche Daten *„grundrechtlich jedenfalls als problematisch. Ob sie der Staatsgerichtshof als verfassungswidrig qualifizieren wird, dürfte auch wesentlich von der zukünftigen einschlägigen ausländischen Grundrechtsprechung abhängen.“*[32] Mit der Entscheidung des deutschen Bundesverfassungsgerichts liegt eine solche Grundrechtsprechung vor. Die Vorratsdatenspeicherung wurde dabei nicht per se als unverhältnismässig beurteilt. Vielmehr bestand das Problem darin, dass keine genügenden Schutzmassnahmen getroffen worden waren für diesen *„besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“*. Diese Schutzmassnahmen, die nun in Folge des Urteils geschaffen werden müssen, bestehen vorwiegend in Folgendem: Es bedarf der gesetzlichen Gewährleistung eines besonders hohen Standards der Datensicherheit,[33] Anforderungen an die unmittelbare Datenverwendung,[34] an die Trans-

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

29 Vgl. bereits Tätigkeitsbericht 2004, 7.1., Tätigkeitsbericht 2005, 7.1. und Tätigkeitsbericht 2006, 7.1.

30 http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html. Das Bundesverfassungsgericht bestätigt in Randnummer 210, dass „es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite [handelt], wie sie die Rechtsordnung bisher nicht kennt: Erfasst werden über den gesamten Zeitraum von sechs Monaten praktisch sämtliche Telekommunikationsverkehrsdaten aller Bürger ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten, eine – auch nur abstrakte – Gefährlichkeit oder sonst eine qualifizierte Situation. Die Speicherung bezieht sich dabei auf Alltagshandeln, das im täglichen Miteinander elementar und für die Teilnahme am sozialen Leben in der modernen Welt nicht mehr verzichtbar ist. Grundsätzlich ist keine Form der Telekommunikation prinzipiell von der Speicherung ausgenommen.“

31 BuA 2009 / 110, S. 125 ff.

32 Vgl. Hilmar Hoch: Die Regelung des staatlichen Zugriffs auf Fernmeldedaten im Kommunikationsgesetz aus grundrechtlicher Sicht, in LJZ 4 / 2009, S. 103: http://www.juristenzeitung.li/papers/showpdf/LJZ_2009_04.pdf.

33 In Randnummer 222 wird dies wie folgt begründet: „Dieses gilt besonders, weil die Daten bei privaten Diensteanbietern gespeichert werden, die unter den Bedingungen von Wirtschaftlichkeit und Kostendruck handeln und dabei nur begrenzte Anreize zur Gewährleistung von Datensicherheit haben. Sie handeln grundsätzlich privatnützig und sind nicht durch spezifische Amtspflichten gebunden. Zugleich ist die Gefahr eines illegalen Zugriffs auf die Daten groß, denn angesichts ihrer vielseitigen Aussagekraft können diese für verschiedenste Akteure attraktiv sein. Geboten ist daher ein besonders hoher Sicherheitsstandard, der über das allgemein verfassungsrechtlich gebotene Maß für die Aufbewahrung von Daten der Telekommunikation hinausgeht. Solche Anforderungen der Datensicherheit gelten dabei sowohl für die Aufbewahrung der Daten als auch für deren Übermittlung; ebenso bedarf es effektiver Sicherungen zur Gewährleistung der Löschung der Daten.“

34 Hier wird insbesondere eine absschliessende Definition der Straftatbestände gefordert, die als „schwere Straftat“ einzustufen sind (Randnummer 228).

parenz der Datenübermittlung, an den Rechtsschutz und an Sanktionen.[35] Soweit ersichtlich sieht das KomG in Liechtenstein – ausser dem umfassenden Richtervorbehalt und unserer erwähnten Kontrollmöglichkeit – keine entsprechenden Anforderungen vor. Dies erstaunt insofern nicht, als der Inhalt des Karlsruher Urteils bei der Landtagsdebatte wohl auch aus Zeitgründen nicht im Detail diskutiert wurde.[36] Auf alle Fälle sind uns keine Zahlen bekannt, welche bestätigen, dass die Vorratsdatenspeicherung in Liechtenstein nötig ist.

Es bleibt abzuwarten, ob der Staatsgerichtshof eine Gelegenheit haben wird, hierzu Stellung zu nehmen. Die Europäische Kommission arbeitet derzeit an einer Revision der Richtlinie. Diese Revision wird auch voraussichtlich eine Änderung des KomG zur Folge haben. Damit wird auch der Gesetzgeber gefordert sein.

Das **Aufzeichnen** bzw. das **Abhören nichtöffentlicher Gespräche** gibt immer wieder Anlass für Anfragen.[37] Die Gesetzesbestimmungen, die das Aufzeichnen bzw. Abhören von Telefonaten regeln, finden sich in dem Gesetz über den strafrechtlichen Schutz des persönlichen Geheimbereichs:[38] Demnach bedarf es für die Aufnahme von nichtöffentlichen Telefongesprächen grundsätzlich der Einwilligung der daran Beteiligten. Ausnahmen von diesem Grundsatz sind explizit im Gesetz geregelt.[39] Insbesondere ist eine *Aufzeichnung von nichtöffentlichen Gesprächen ohne Einwilligung nur Hilfs-, Rettungs- und Sicherheitsdiensten im Falle von Notrufen gestattet.*[40] Gerade im Falle eines Notrufs ist es unabdingbar, dass die Notrufzentrale erkennen kann, von welchem Teilnehmer der Anruf erfolgt. Aus diesem Grund ist z.B. eine Unterdrückung der Rufnummer nicht möglich.[41] In der Schweiz gibt es das sogenannte *Notverzeichnis*, auf das von den Notrufstellen zugegriffen werden kann. Ein Zugriff der Landespolizei auf dieses Verzeichnis in der Schweiz ist auf längere Sicht nicht die bestmögliche Lösung: Es erfordert einen grenzüberschreitenden Datenverkehr. Zudem ist davon auszugehen, dass in dem Schweizer Notverzeichnis nicht alle liechtensteinischen Telefonanschlüsse erfasst werden. Eine landesinterne Lösung wäre daher zu bevorzugen und anzustreben. Aus datenschutzrechtlicher Sicht jedenfalls stehen keine grundsätzlichen Bedenken einem solchen Notverzeichnis entgegen, da die Bestimmbarkeit der betroffenen Person im Notfall im ureigensten Interesse des Anrufers sein dürfte, womit die Datenbekanntgabe gerechtfertigt wäre.[42]

Ausserdem war in diesem Zusammenhang eine andere Frage zu klären: In welchen Fällen handelt es sich um einen sogenannten *Hilfs-, Rettungs- und Sicherheitsdienst*? Dann dürfen Telefonate auch ohne vorherige Einwilligung der Gesprächspartner aufgezeichnet werden. Die Stellen, die in dem offiziellen Notrufnummerverzeichnis Liechtensteins aufgelistet sind, zählen sicherlich dazu.[43] Fraglich ist, ob auch andere Stellen dazu zählen, die in dem Verzeichnis zwar nicht erscheinen, aber allein für die Kommunikation in Notfällen gedacht sind, also den selben Zwecken dienen.

Daten aus **sozialen Netzwerken** werden immer wieder von Nichtnutzern gebraucht, da die Einstellungen dies teils zulassen. Wie ist es, wenn eine Schule durch einen *„Freund"* einer Person gewisse Dinge erfährt, die nicht im Sinn der Schule sind? Darf die Schule diese Informationen, die an sie herangetragen wurden, auswerten und unter Umständen gegen diese Person verwerten? Aus unserer Sicht geht es bei sozialen Netzwerken nicht um ein geschlossenes Netzwerk, sondern um ein quasi öffentliches Netz. Mit anderen Worten muss eine Person dafür

35 Randnummer 252 ff: „Schließlich setzt eine verhältnismäßige Ausgestaltung wirksame Sanktionen bei Rechtsverletzungen voraus. Würden auch schwere Verletzungen des Telekommunikationsgeheimnisses im Ergebnis sanktionslos bleiben mit der Folge, dass der Schutz des Persönlichkeitsrechts … angesichts der immateriellen Natur dieses Rechts verkümmern würde.., widerspräche dies der Verpflichtung der staatlichen Gewalt, dem Einzelnen die Entfaltung seiner Persönlichkeit zu ermöglichen … . Dies kann insbesondere der Fall sein, wenn unberechtigt gewonnene Daten weitgehend ungehindert verwendet werden dürften oder eine unberechtigte Verwendung der Daten mangels materiellen Schadens regelmäßig ohne einen der Genugtuung der Betroffenen dienenden Ausgleich bliebe. Der Gesetzgeber hat diesbezüglich allerdings einen weiten Gestaltungsspielraum. Dabei kann er insbesondere in den Blick nehmen, inwieweit sich entsprechende Regelungen in die allgemeine Systematik des Strafprozessrechts oder des geltenden Haftungsrechts einfügen."

36 An der 2. Lesung vom 17. März 2010 erwähnten die Abgeordneten Peter Büchel, Günther Kranz sowie der zuständige Regierungschef-Stellvertreter, Martin Meyer, dieses Urteil, vgl. Landtagsprotokoll, S. 198 ff.

37 Vgl. Tätigkeitsbericht 2009, S. 22. Vorbehalten bleiben natürlich die einschlägigen Kompetenzen der Strafverfolgung von Behörden.

38 LGBl. 1969 Nr. 34, LR 311.3.

39 Art. 4; vgl. BuA 104/2005, Z. 5.5 zu Art. 4.

40 S. BuA Nr. 104/2005, S. 120 ff.

41 Gemäss Art. 57 der Verordnung über elektronische Kommunikationsnetze und –dienste.

42 Vgl. Art. 17 DSG.

43 Vgl. http://www.llv.li/pdf-llv-azslv-notrufnummern_a6.pdf.

sorgen, dass gewisse negative Aussagen, die sie unter Umständen belasten können, nur auf einem entsprechend geschützten Netzwerk stehen. Ihre Einstellungen in einem sozialen Netzwerk sollten so konfiguriert sein, dass gewisse Aussagen nicht sichtbar sind. Oder noch besser ist es, wenn solche Aussagen überhaupt nicht auf einer Internetseite gemacht werden. Denn: Das Internet vergisst ja nicht.

1.4 Gesundheit und Soziales

Anfang 2010 wurde ein **neues Formular** für die **Überweisung** an einen nicht zur OKP zugelassenen Leistungserbringer eingeführt. Dieses sieht vor, dass bei der Angabe des Überweisungsgrundes „medizinischer Notfall" eine ausführliche Begründung angegeben werden muss, warum ein medizinischer Notfall vorliegt. Umfasst die Beantwortung die Angabe von konkreten Gesundheitsdaten? Mit Vertretern der Ärztekammer, des Ressorts Gesundheit und des Krankenkassenverbandes konnte diese Frage geklärt werden: Eine Diagnose ist keinesfalls anzugeben. Vielmehr ist eine Beschreibung der Umstände gefordert, weshalb es sich um einen medizinischen Notfall handelt (z.B. eine Wartezeit für eine erforderliche Behandlung, welche aus medizinischer Sicht nicht vertreten werden könne).

Liechtensteinisches Krebsregister: Schon Ende 2007 wurde das Amt für Gesundheit gesetzlich beauftragt, für Zwecke der Krebsbekämpfung und -forschung ein elektronisches Register zu führen oder sich einem ausländischen anzuschliessen. Wir konnten bei der Erarbeitung von Lösungsvorschlägen einen massgebenden Beitrag leisten. Die Sicherstellung des Datenschutzes ist zentral für die Akzeptanz eines Krebsregisters. Was ist ein Krebsregister eigentlich? Ein Krebsregister ist eine systematische Sammlung von Informationen zu Krebserkrankungen. Diese Informationen bilden die Basis für die Erforschung von Krebserkrankungen und deren Behandlung. Mit ihrer Hilfe wird beispielsweise ersichtlich, wie häufig bestimmte Krebserkrankungen in bestimmten Gebieten auftreten oder es können Behandlungserfolge verglichen werden. Erhoben werden allgemeine Angaben zur Person (z.B. Name, Vorname, Geburtsdatum, Adresse), zur Krebserkrankung sowie zu deren Verlauf.

All dies kann zu einer *Interessenskollision* zwischen möglichst *vollständigen und aussagekräftigen Ergebnissen des Krebsregisters* einerseits mit den *Grundrechten des Patienten auf Selbstbestimmung* andererseits führen. Dieses Selbstbestimmungsrecht bezieht sich hier auf Informationen bzw. Daten über die eigene Person. Datenschutzrechtlich besonders geschützt sind Angaben über die Gesundheit einer Person. Voraussetzung für die Bekanntgabe der Gesundheitsdaten an das Krebsregister durch den behandelnden liechtensteinischen Arzt ist die Einwilligung des Patienten. Der Arzt fragt den Patienten vor einer Bekanntgabe um Unterzeichnung einer *Einwilligungserklärung*. Mit der Einwilligung des Patienten wird der Arzt gleichzeitig zur Offenlegung seines Berufsgeheimnisses berechtigt.[44] Aufgrund der Wichtigkeit der Einwilligung haben wir, gemeinsam mit dem Amt für Gesundheit, ein entsprechendes Formular erarbeitet, welches bei den Ärzten aufliegt. Darin bestätigt der Patient mit seiner Unterschrift, ob er mit einer Weiterleitung seiner Krankheitsdaten an das Krebsregister St. Gallen-Appenzell einverstanden ist oder nicht.[45]

In einer Anfrage ging es um die **Weitergabe von Daten** an Träger der sogenannten 2. Säule. Von der AHV werden jährlich sogenannte *Lebensbescheinigungen* eingeholt, um feststellen zu können, ob Renten rechtmässig ausbezahlt werden. Diese Lebensbescheinigungen werden auch von Trägern der 2. Säule benötigt. Deshalb wurden wir angefragt, ob es zulässig sei, wenn die AHV die Kopie dieser Lebensbescheinigungen auch an die Vorsorgeeinrichtungen der obligatorischen betrieblichen Altersvorsorge übermittelt. Damit sollte verhindert werden, dass diese Einrichtungen ebenfalls diese Lebensbescheinigungen einholen müssten. Eine Weitergabe ist nach unserer Ansicht möglich, wenn in der Angabe des Zwecks ein entsprechender Hinweis erfolgt.

Bei der Einführung eines **KIinik-Informationssystems** beim Landesspital konnten wir im Rahmen der Zugriffsberechtigungen Stellung nehmen. Dabei wurde auf das Arztgeheimnis hingewiesen, da im

44 Eine Einwilligung in die Bekanntgabe der Gesundheitsdaten durch den Arzt an das Krebsregister muss zwar nicht zwingend schriftlich, immerhin aber ausdrücklich erfolgen. Dies setzt voraus, dass der Betroffene auch weiss, wozu er seine Einwilligung gibt. Das Kriterium „in Kenntnis der Sachlage" ist zentral. Die volle Kenntnis der Sachlage setzt voraus, dass die betroffene Person umfassend über die konkreten Umstände informiert ist. Sinn dieses Kriteriums ist es, dass die betroffene Person die Möglichkeit hat, Gefahren und Vorteile der Verarbeitung sie betreffender Daten zu beurteilen.

45 Das Formular sowie weitere Informationen finden Sie hier: http://www.llv.li/amtsstellen/llv-ag-krankheiten_risiken/krebsregister.htm.

System auch Gesundheitsdaten bearbeitet werden. Wie in einem Rechtsgutachten, das 2009 zum Thema Ausnahmen des Arztgeheimnisses in Auftrag gegeben worden war, festgehalten wird, gilt das Arztgeheimnis auch zwischen Ärzten und umso mehr gegenüber nicht ärztlichem Personal. Dies ist umso wichtiger, als eine *Verletzung des Arztgeheimnisses* strafbar ist.[46]

1.5 Polizei, Sicherheit und Justiz

Wie im letzten Tätigkeitsbericht bereits ausführlich dargestellt, wurden mit Inkrafttreten der letzten Teilrevision des DSG die Voraussetzungen für den rechtmässigen Betrieb einer **Videoüberwachungsanlage im öffentlichen Raum** geschaffen.[47] Dabei kann erst nach einer kritischen Prüfung der *Erforderlichkeit und Verhältnismässigkeit* abschliessend beurteilt werden, ob eine Videoüberwachung zur Erreichung eines bestimmten Zwecks zulässig ist oder nicht.

Wir bewilligten verschiedene Videokameras z.B. in Tief- und Parkgaragen. Die Erforderlichkeit begründet sich in diesen Fällen insbesondere durch die unübersichtliche Situation und die oftmals diffusen Lichtverhältnisse der Parkgaragen und das damit verbundene erhöhte Beschädigungs- und Einbruchsrisiko an den geparkten Fahrzeugen als auch des erhöhten Risikos von Übergriffen auf Personen. Die Videoaufzeichnung kann somit als geeignetes Mittel zur Abschreckung und Beweissicherung betrachtet werden, da in vergleichbaren Sachverhalten Videotechnik bereits eingesetzt wurde und sich als wirkungsvoll erwiesen hat. Untersuchungen in England haben beispielsweise ergeben, dass eine Videoüberwachung in Parkhäusern bzw. auf Parkplätzen bei der Prävention von Autodiebstählen besonders erfolgreich ist. So konnte infolge des Einsatzes von Videoüberwachungsanlagen in Parkhäusern vor allem Diebstahl von und aus Kraftfahrzeugen um ca. 41% reduziert werden.[48] Dies gilt insbesondere bei einer Kombination mit verbesserter Beleuchtung und deutlichen Hinweisen auf die Videoüberwachung.[49]

Im Zusammenhang mit der **Überwachung von Arbeitsbereichen** in Unternehmen sind zudem weitere Bestimmungen des Arbeitnehmerrechts zu berücksichtigen. Eine Überwachung des Verhaltens der Arbeitnehmenden ist nur in wenigen Ausnahmefällen zulässig.[50] Eine Videoüberwachung am Arbeitsplatz kann zulässig und ohne Bewilligung betrieben werden, wenn bestimmte Voraussetzungen erfüllt sind, die jeweils in jedem Fall einzeln und konkret zu prüfen sind. Zum Beispiel ist eine Videoüberwachung einer nicht öffentlichen Lagerstätte innerhalb eines Unternehmens, die ausschliesslich ausserhalb der Betriebs-, Öffnungs- bzw. Arbeitszeiten erfolgt, zum Zwecke des Diebstahlschutzes zulässig.

Die möglicherweise betroffenen Mitarbeiter müssen jedoch vor der Inbetriebnahme über die Videoüberwachung, dabei insbesondere über die Aufnahmezeiten, die Erfassungsbereiche der Kameras sowie den Zweck der Überwachung, *informiert* werden. Die Videoüberwachung ist in einem Überwachungsreglement zwingend mit aufzunehmen und zu regeln. Dieses Überwachungsreglement ist den betroffenen Mitarbeitern nachweislich zur Kenntnis zu bringen. Diese Information kann durch öffentlichen Aushang oder, wenn verfügbar, über das Intranet sowie auch durch persönliche Anschreiben an alle Mitarbeiter erfolgen. Zusätzlich muss die Überwachung vor Ort entsprechend ausgewiesen werden. Die technische Ausgestaltung muss eine zweckentfremdende Nutzung sowie Missbrauch verhindern. Die Bestimmungen gemäss Artikel 9 und 10 DSV gelten sinngemäss. Das DSG findet keine Anwendung, wenn eine **natürliche Person Personendaten ausschliesslich zum persönlichen Gebrauch** bearbeitet und diese nicht an Aussenstehende bekannt gibt (Art. 2 Abs. 3 Buchstabe a DSG). Mit dem Begriff *„zum persönlichen Gebrauch"* grenzt das Gesetz den Bereich persönlicher Lebensführung ab von der beruflichen und geschäftlichen Sphäre. Hier betrachtet der Gesetzgeber denjenigen, der personenbezogene Daten erhebt, verarbeitet oder nutzt, als ebenso schutzbedürftig wie

46 § 121 StGB.
47 Vgl. Tätigkeitsbericht 2009, S. 18 ff.
48 Brandon C. Welsh/David P. Farrington, Crime prevention effects of closed circuit television: a systemativ review, Home Office Research Study 252, August 2002, S. 39; Brandon C. Welsh/David P. Farrington, Effects of Closed-Circuit Television on Crime, 2009; Martin Gill/Angela Spriggs, Assessing the impact of CCTV, Home Research Study 292, Februar 2005.
49 S. Fussnote 1.
50 Vgl. dazu unsere Richtlinien: http://www.llv.li/amtsstellen/llv-dss-richtlinien/llv-dss-ueberwachung-arbeitnehmer.htm.

die Betroffenen und räumt diesen deshalb keinen rechtlichen Einfluss auf seinen Datenumgang ein. Entscheidend ist hierbei, dass eine Verwendung von Personendaten ausschliesslich im engeren Privat- und Familienleben stattfindet, ohne dass Aussenstehende auf diese Zugriff haben.[51] Kommt es bei einer Datenbearbeitung zum persönlichen Gebrauch trotzdem zu einer Persönlichkeitsverletzung, so kann sich eine in ihrer Persönlichkeit verletzte Person vor dem Landgericht mittels Art. 39 und 40 des Personen- und Gesellschaftsrechts (PGR) zur Wehr setzen. Das heisst umgekehrt: Jegliche nach aussen gerichtete, über den persönlichen und familiären Kreis hinaustretende Tätigkeit verlässt diesen Rahmen, wodurch das DSG anwendbar wird.[52]

1.6 Wirtschaft und Finanzen

Der **Finanzmarktaufsicht** (FMA) obliegt nunmehr[53] die **Aufsicht** über die **Träger einer Berechtigung nach Art. 180a PGR**. Die nach Art. 180a PGR Berechtigten müssen nun auch – neu – eine Aufsichtsgebühr gegenüber der FMA entrichten. Die Liste der Träger einer Berechtigung nach Art. 180a PGR ist jedoch nach wie vor vom Grundbuch- und Öffentlichkeitsregisteramt (GBOERA) zu führen.[54]

Durch die neue Aufgabenzuweisung ist nun folgende Situation entstanden: Dem GBOERA obliegt das Führen, die Pflege und Verwaltung der Art. 180a PGR-Liste. Es übt selbst aber keine weiteren Aufsichtsfunktionen gegenüber den in der Liste aufgeführten Personen aus. Die Ausübung der Aufsicht und Erhebung der Gebühren gegenüber den nach Art. 180a PGR Berechtigten obliegt der FMA, die ihrerseits keinen direkten Zugang zu der Liste nach Art. 180a PGR hat. Um nun ihren Aufsichtsverpflichtungen überhaupt nachkommen zu können, benötigt die FMA Zugang zu dieser Liste und stellte diesbezüglich einen Antrag. Dabei wünschte sie eine *regelmässige Bekanntgabe*.

Da eine solche Datenbekanntgabe bislang nicht gesetzlich geregelt ist, wurden wir in diesem Zusammenhang um Stellungnahme gebeten. Wir kamen hier zum Ergebnis, dass eine einmalige Bekanntgabe der aktuellen Daten gestützt auf Art. 23 Abs.1 Buchstabe a DSG zulässig ist. Diese Datenbekanntgabe musste jedoch an gewisse Voraussetzungen geknüpft werden, namentlich die Zweckgebundenheit und die Informationspflicht gegenüber den auf der Liste eingetragenen berechtigten Personen. Eine darüber hinausgehende, also wiederholte oder gar regelmässige Datenweitergabe musste hingegen als unzulässig untersagt werden, da es zum Zeitpunkt der Anfrage an der hierfür erforderlichen Rechtsgrundlage fehlte. Da es sich um eine ständige Aufgabe der FMA handelt, standen in Folge konkrete Überlegungen an, das Führen der Art. 180a PGR Liste zusammen mit entsprechenden Rechten zur Datenbearbeitung und Bekanntgabe gesetzlich neu zu regeln.

In der Schweiz gibt es einen **Verein Unternehmens-Datenschutz** (VUD), in dem grosse Unternehmen vereinigt sind und sich mit Datenschutz-Angelegenheiten befassen. Da es einige Bereiche gibt, in denen sich auch Fragen zum liechtensteinischen Datenschutzrecht stellen, wurden wir zu einem Gedankenaustausch eingeladen. Dieser war sehr fruchtbar, da er auch erlaubte, Standpunkte der Wirtschaft in Erfahrung zu bringen. In Liechtenstein gibt es nach unserem Kenntnisstand noch keinen vergleichbaren Verein. Ein den Grössenverhältnissen Liechtensteins angepasstes Austauschforum wäre aber auf alle Fälle zu begrüssen.[55]

Eine Person wandte sich in folgendem Fall an uns: Sie hatte eine *Zahlungsaufforderung* eines *angeb-*

51 Beispiele für den typischen persönlich-familiären Bereich: Freizeit, Urlaub, privater Konsum, Sport, Unterhaltung; die typische dazu gehörende Datenverarbeitung betrifft z.B. private Gespräche, Adressen, Telefonnummern, Webadressen, E-Mailadressen, Nutzung von privaten Adressverzeichnissen z.B. für Weihnachtsgrüsse, Geburtstage, weitere Angaben von Freunden, Bekannten, Verwandten, Hobby- und Tauschpartner, Favorites/Bookmarks zum Internet-Surfen, die „History" der privaten Browser-Nutzung, E-Mail-Korrespondenz, alles gleich ob im PC, Notebook, Handheld oder Telefon gespeichert oder auch auf einem Server abgelegt. Fotos oder Videoaufnahmen, die nur im familiären Umkreis aufbewahrt und gezeigt werden. Vgl. Urs Maurer-Lambrou/Simon Kunz, in: Maurer-Labrou/Vogt (Hrsg.), Basler Kommentar zum Schweizer Datenschutzgesetz, 2. Auflage, Basel 2006, Rn. 21 zu Art. 2 CH-DSG.

52 Beispiele für nicht mehr (rein) persönliche, also berufliche Bereiche: eine Datenverarbeitung im Zusammenhang mit einem Familienbetrieb oder Heimarbeit; Adressen des persönlichen Freundeskreises, die – wenn auch nur einmal – zugunsten eines Dritten für eine Direktwerbeaktion zur Verfügung gestellt oder genutzt werden (z.B. gewerbliche Produktwerbung, Hinweis auf eine erwünschte Unterstützung wohltätiger Organisationen oder kommunaler Anliegen); Fotos oder Videoaufnahmen, die über das Internet Aussenstehenden frei zugänglich gemacht werden (z.B. Soziale Netzwerke, Fotoalben).

53 Aufgrund von Änderungen des Sorgfaltspflichtgesetzes (SPG) und des FMA-Gesetzes.

54 Vgl. Art. 3 der Verordnung vom 8. April 2003 über die Ausübung von Tätigkeiten nach Art. 180a PGR.

55 Vgl. Tätigkeitsbericht 2009, II.1.

lichen Rechtsanwaltes aus Deutschland per E-Mail bekommen, in der es darum ging, dass sie offenbar **illegal Musik vom Internet** bezogen hatte. Es ist bekannt, dass das illegale Herunterladen von Musik zu grossen finanziellen Nachteilen in der Musikindustrie führt.[56] Wir haben darauf hingewiesen, dass es sehr merkwürdig ist, dass ein in Deutschland tätiger Rechtsanwalt in einer blossen E-Mail auf einen möglichen Verstoss hinweist. Zudem haben wir auch darauf hingewiesen, dass der Anwalt, sollte es sich in der Tat um einen solchen handeln, in Liechtenstein tätig werden muss. D.h. der ausländische Anwalt kann in Liechtenstein klagen. Im gegenständlichen Fall war auffällig, dass zur einfachen Lösung zwar eine Zahlung von EUR 100.- angeboten wurde, die Anwaltskanzlei jedoch nicht eindeutig zu identifizieren war. Vor diesem Hintergrund rieten wir zur Vorsicht.

1.7 Arbeitsbereich

Im vergangenen Jahr hatten wir angekündigt, bei der **Überwachung der Arbeitnehmer am Arbeitsplatz** mit dem Amt für Volkswirtschaft (AVW), Fachbereich Arbeitssicherheit zusammenarbeiten zu wollen, um Synergien zu nutzen. Soweit eine Überwachung am Arbeitsplatz stattfindet, bei der auch Personendaten bearbeitet werden, bestehen unsere Zuständigkeiten und die des AVW parallel. Als typisches Beispiel sind hier die Schalterhallen von Banken oder Post zu nennen: Schalterhallen sind meistens für jedermann öffentlich zugänglich und gleichzeitig befinden sich dort *permanente Arbeitsplätze* (z.B. Schalterpersonal, Kassier). Aus diesem Grund erachteten wir ein gemeinsames Vorgehen für sinnvoll und führten daher erste gemeinsame Überprüfungen durch. Diese Vorgehensweise hat für die Betroffenen den Vorteil, dass nur ein Verfahren läuft, es nur einen Ansprechpartner gibt und die ergehenden Entscheidungen sowohl vom AVW als auch von uns mitgetragen werden. Diese Überprüfungen standen in der Regel im Zusammenhang mit einem Antrag auf Bewilligung einer Videoüberwachung.[57]

Im Rahmen der Zusammenarbeit mit dem AVW haben wir ausserdem *„Richtlinien zur Überwachung der Arbeitnehmer am Arbeitsplatz"* erarbeitet, die auf unserer Internetseite abgerufen werden können.[58]

1.8 Bildung/Forschung

Immer wieder stellt sich im Rahmen von **Forschungsprojekten** die Frage, wie mit Personendaten umzugehen ist.[59] Das DSG sieht hierzu für Behörden in Art. 26 eine Sondervorschrift vor. Behörden dürfen unter bestimmten Voraussetzungen für die Zwecke der Forschung, Planung und Statistik Personendaten bearbeiten. Diese müssen *anonymisiert* werden, sobald der Zweck des Bearbeitens dies erlaubt, der Empfänger darf die Daten nur mit Zustimmung des Inhabers weitergeben und schliesslich sind die Ergebnisse so zu veröffentlichen, dass die betroffenen Personen nicht bestimmbar sind. Kann im Rahmen des Forschungsprojekts diesen Voraussetzungen entsprochen werden, so sind die Anforderungen an die Bearbeitung von Personendaten weniger anspruchsvoll.

Beispielsweise bedarf es zwar für die Erhebung der Daten durch Behörden einer Rechtsgrundlage, *nicht aber für die Bekanntgabe*, da es sich ja um anonymisierte Angaben handelt. Somit kann *nicht mehr von Personendaten* gesprochen werden. Ziel dieser Gesetzesbestimmung ist es, die Bearbeitung von Personendaten für solche nicht personenbezogenen Zwecke zu vereinfachen. Somit findet nur vor der Veröffentlichung eine Bearbeitung von Personendaten statt. Insofern empfiehlt es sich, dass sich die Projektleitung gegenüber den betroffenen Personen in dieser ersten Phase ausdrücklich zur Beachtung der datenschutzrechtlichen Bestimmungen verpflichtet. Hierzu gehören unter anderem die Zweckbindung, eine Löschung der erhobenen Daten nach Zweckerreichung, keine Weitergabe an Dritte sowie

56 In der Schweiz sammelte ein Unternehmen im Auftrag von Urheberrechtsinhabern in „Peer-to-Peer- Netzwerken (darin ist jeder angeschlossene Computer gleichberechtigt) IP-Adressen von Usern, die angeblich illegal urheberrechtsgeschützte Inhalte (Musik- oder Videodateien) zum Tausch anboten. Mit diesen IP-Adressen stiessen die Rechteinhaber Strafverfahren an, um mittels der dann gewährten Akteneinsicht Name und Adresse der betroffenen User zu erhalten und diese zivilrechtlich auf Schadenersatz zu verklagen. Das Bundesgericht qualifizierte in seinem Urteil (BGE 136 II 508) statische wie dynamische IP-Adressen als Personendaten unter anderem, weil die Bestimmbarkeit der betroffenen Personen die Basis des Geschäftsmodells dieses Unternehmens darstelle. Eine abstrakte Feststellung, ob es sich (insbesondere bei dynamischen) IP-Adressen um Personendaten handelt oder nicht, sei dagegen nicht möglich.

57 Vgl. zum Thema Videoüberwachung am Arbeitsplatz auch unter 1.5.

58 http://www.llv.li/amtsstellen/llv-dss-richtlinien/llv-dss-ueberwachung-arbeitnehmer.htm.; s. unter 2.2.

59 Vgl. zuletzt Tätigkeitsbericht 2009, S. 10.

ausdrückliche Stillschweigeverpflichtungen. Auf Anfrage haben wir bei unterschiedlichen Forschungsprojekten solche entsprechenden Datenschutzerklärungen ausgearbeitet und der Öffentlichkeit zur Verfügung gestellt.[60]

Die **Veröffentlichung von Fotos von neuen Erstklässlern** ist kein neues Thema.[61] Wir wurden angefragt, ob es nicht eine ausdrückliche Einwilligung der betroffenen Eltern vor Veröffentlichung der Fotos braucht. Da es sich bei Fotos (mit oder ohne Namensangabe) nicht um besonders schützenswerte Daten und um Persönlichkeitsprofile handelt, ist eine stillschweigende Einwilligung ausreichend. Die Zeitungen haben die betroffenen Eltern auf eine mögliche Veröffentlichung von Fotos ihres Kindes aufmerksam zu machen. Wenn die Fotos von den Eltern nicht gewünscht sind, haben sich diese an die Zeitungen zu richten. Die Eltern können vor der Publikation eines Fotos somit widersprechen.

Wie ist der Fall zu beurteilen, in dem Eltern möchten, dass ihr **Kind** während der **gesamten Schulzeit** in der **Schule nicht fotografiert** wird? Das Kind soll demnach nicht nur bei der jährlichen Veröffentlichung der Erstklässler durch die Zeitungen oder auf Internetseiten (z.B. von Schulklassen) nicht erfasst, sondern es soll auch bei Schulausflügen und Ähnlichem nicht fotografiert werden – auch nicht schulintern. Diese Frage ist die des *Rechtes am eigenen Bild*: Es darf niemand ohne seine Einwilligung z.B. auf Fotos abgebildet werden.[62]

Das Schulamt führt regelmässig eine **landesweite Umfrage unter Schülern** durch, um das Leistungsniveau auf nationaler Ebene im Vergleich mit den anderen europäischen Ländern feststellen zu können. Die Erhebung läuft ähnlich ab wie bei der PISA-Studie.[63] Aus datenschutzrechtlicher Sicht ist insbesondere der Fragenkomplex zum sozialen und sozio-ökonomischen Umfeld von Bedeutung, da hier die Kinder auch Fragen, z.B. über die Bildung der Eltern, oder über Umstände zu Hause zu beantworten haben. Für die Erhebung bedarf es datenschutzrechtlich einer Rechtsgrundlage.[64] Zudem sind die Eltern darüber zu informieren, dass Kinder Fragen über sie beantworten sollen bzw. die Eltern sollten diese Fragen selbst beantworten. Mangels Rechtsgrundlage kann die Umfrage zum jetzigen Zeitpunkt nur auf freiwilliger Basis, im Einverständnis der Schüler und Eltern, durchgeführt werden.

1.9 Datenbekanntgabe im Inland

Traktandenlisten wie auch **Gemeinderatsprotokolle** sind in der Regel **öffentlich zugänglich**. Bei der Traktandierung eines Verwaltungsgerichtsverfahrens waren die Namen der Beschwerdeführer öffentlich genannt. Die Beschwerdeführer wandten sich an uns, damit nicht auch das entsprechende Gemeinderatsprotokoll ebenfalls veröffentlicht werden sollte. Während klar ist, dass der Gemeinderat die Gemeinde betreffende Angelegenheiten diskutieren können muss, heisst dies nicht, dass die Namen der Beschwerdeführer ebenfalls zu veröffentlichen sind. Was zählt, ist die Sachinformation des Verfahrens und nicht die Angabe über die beteiligten Personen. Dies ist auch der Grund, weshalb *Gerichtsurteile* in der Praxis *anonymisiert veröffentlicht* werden. Das Informationsgesetz sieht denn auch an verschiedenen Stellen vor, dass *überwiegende private Interessen zu berücksichtigen* sind.[65] Diesbezüglich ist zu erwähnen, dass nach Art. 9 Abs. 4 des Informationsgesetzes der Gemeinderat in seiner Geschäftsordnung mit Zustimmung des Vorstehers die näheren Vorschriften in Bezug auf die Vertraulichkeit der Sitzungen und die Information der Öffentlichkeit erlässt. Sollte die Geschäftsordnung einer Gemeinde diese näheren Vorschriften noch nicht enthalten, empfiehlt es sich, dem nachzukommen, damit sich ähnliche Fälle in der Zukunft nicht mehr stellen.

Die **Bekanntgabe einer Liste von Personen** fällt nicht nur unter das DSG, sondern grundsätzlich auch unter das *Amtsgeheimnis*. Der Staatsgerichtshof hat festgehalten, dass mit der Amtshilfe ein Grundrechtseingriff verbunden sein kann, wobei insbesondere

60 Vgl. Tätigkeitsbericht 2009, 2.2. und http://www.llv.li/form-llv-dss-mustervorlagen.
61 S. Tätigkeitsbericht 2003, 4.2.
62 Handbuch des Persönlichkeitsrechts, Horst-Peter Götting/Christian Schertz/Walter Seitz (Hrsg.), München 2008, Randnummer 14 zu § 67 (mit Hinweis auf die Rechtsprechung in der Schweiz).
63 Vgl. hierzu http://www.pisa.oecd.org.
64 Vgl. Art. 22 DSG.
65 Art. 3 Abs. 3, Art. 9 Abs. 2, Art. 14. Abs. 1 und Art. 25 des Informationsgesetzes. Art. 20 Abs. 2 der Informationsverordnung sieht zudem vor, dass bei der Veröffentlichung von abgeschlossenen Verwaltungsverfahren der Persönlichkeitsschutz sicherzustellen ist.

eine *Verletzung der Privat- und Geheimsphäre nach Art. 32 der Verfassung* infrage kommt.[66] Das Amtsgeheimnis ist im Staatspersonalgesetz erwähnt[67], ein Verstoss gegen das Amtsgeheimnis ist auch im Strafgesetzbuch geregelt.[68] Die Amtshilfe steht im Gegensatz zum Amtsgeheimnis. Schon im letzten Tätigkeitsbericht hatten wir hierzu festgehalten: *„Die Idee des Datenschutzes besteht darin, dass ein Schutz nur dort greifen soll, wo er gerechtfertigt ist. Mit anderen Worten sollen Daten fliessen, wenn dies notwendig ist."*[69] Da es bei der Amtshilfe um einen Grundrechtseingriff gehen kann, stellt sich somit unter anderem die Frage der Verhältnismässigkeit der Amtshilfe. Wurden im Fall einer Amtshilfe die Information oder diejenigen Personendaten mitgeteilt, die für den Zweck notwendig waren? Die Frage der Grenze zwischen *Amtshilfe und Amtsgeheimnis* kann wohl kaum abstrakt beantwortet werden. Es kommt vielmehr auf den Einzelfall an, eben darauf, ob im Falle von Personendaten, ein Schutz gerechtfertigt ist. Im Rahmen der Überarbeitung unserer Richtlinien zur Datenbekanntgabe durch Behörden beabsichtigen wir, die Frage des Spannungsfeldes *„Amtshilfe – Amtsgeheimnis"* speziell zu berücksichtigen.

66 StGH 2008/63, Ew. 9.1.

67 Nach Art. 38 Abs. 1 sind die Angestellten zur Verschwiegenheit über dienstliche Angelegenheiten verpflichtet, die nach ihrer Natur oder gemäss besonderer Vorschrift geheim zu halten sind. Art. 31 der Staatspersonalverordnung bestimmt: „Die Befreiung der Amtsstellenleiterinnen und Amtsstellenleiter von der Schweigepflicht gemäss Art. 38 des Gesetzes obliegt dem jeweils zuständigen Regierungsmitglied." Der Begriff der „dienstlichen Angelegenheit" wird dabei nicht näher definiert.

68 § 310 Absatz 1 bestimmt: „Ein Beamter oder ehemaliger Beamter, der ein ihm ausschliesslich Kraft seines Amtes anvertrautes oder zugänglich gewordenes Geheimnis offenbart oder verwertet, dessen Offenbarung oder Verwertung geeignet ist, ein öffentliches oder ein berechtigtes privates Interesse zu verletzen, ist, wenn die Tat nicht nur eine Bestimmung mit strengerer Strafe bedroht ist, mit Freiheitsstrafe bis zu drei Jahren zu bestrafen." Nach der Literatur ist Objekt der Tat ein Geheimnis, also Tatsachen, Gegenstände, Erkenntnisse oder Pläne, die höchstens einem kleinen Kreis bekannt und anderen nicht oder nur schwer zugänglich sind. Der Beamte muss nicht Sachbearbeiter im engeren Sinn gewesen sein. Auch eine spezielle Geheimhaltungsverpflichtung ist nicht erfordert. Geheimnis ist, was ohne Rücksicht auf eine allfällige Bezeichnung als Geheimnis durch die zuständigen Stellen zur Vermeidung der Verletzung öffentlicher oder privater Interessen geheim gehalten werden muss (vgl: Ernst Fabrizy: Strafgesetzbuch – Kurzkommentar, 10. Aufl., Wien 2010, Randnummer 3 zu § 310.

69 Vgl. Tätigkeitsbericht 2009, 1.8.

1.10 Datenbekanntgabe mit Auslandsbezug

Die **Europäische Kommission** erliess am 5. Februar 2010 eine **neue Entscheidung** zu **Standardvertragsklauseln**.[70] Standardvertragsklauseln können in den Fällen eingesetzt werden, in denen Personendaten in sogenannte Drittländer übermittelt werden sollen, in denen also kein angemessener Datenschutz gewährleistet ist. Für diesen Fall geben die Standardvertragsklauseln die technischen und organisatorischen Sicherheitsmassnahmen vor, die Datenverarbeiter in einem Drittland ohne angemessenes Schutzniveau anwenden sollten, um einen Schutz zu gewährleisten, der den durch die Verarbeitung entstehenden Risiken und der Art der zu schützenden Daten angemessen ist.[71]

Der Beschluss 2010/87/EG dient vor allem dazu, klarzustellen, dass die aufgeführten Vertragsklauseln von einem für die Datenverarbeitung Verantwortlichen, der in der Europäischen Union niedergelassen ist, auch verwendet werden können, um angemessene Garantien für die Übermittlung personenbezogener Daten an einen **Auftragsverarbeiter**, der in einem Drittland niedergelassen ist, zu gewährleisten.[72] Der Schwerpunkt der Entscheidung liegt also darin, dass insbesondere die Auftragsdatenbearbeitung besser geregelt werden sollte, um der „rasch expandierenden Datenverarbeitungstätigkeit weltweit Rechnung zu tragen".[73] Diese Entscheidung wurde im Berichtsjahr noch nicht in liechtensteinisches Recht umgesetzt.[74]

Deshalb sind *Standardvertragsklauseln*, die unmittelbar auf der Entscheidung 2010/87/EG vom 05. Februar 2010 basieren, – noch nicht – von der Genehmigungspflicht gemäss Art. 8 Abs. 3 DSG befreit.[75]

70 Entscheidung Kommission 2010/87/EG vom 05. Februar 2010; ftp://ftp.freenet.at/privacy/ds-eu/eu-standardvertragsklauseln-3.pdf.

71 Vgl. Erwägung (12) der Entscheidung 2010/87&EG, a.a.O.

72 Erwägung (8) der Entscheidung 2010/87/EG, a.a.O.

73 Erwägung (7) der Entscheidung 2010/87/EG, a.a.O.

74 Ebenso noch nicht umgesetzt wurde die Entscheidung über die Angemessenheit des Datenschutzes auf den Färöer Inseln und in Andorra. Solange eine Umsetzung in liechtensteinisches Recht noch nicht erfolgt ist, gilt ein grenzüberschreitender Datentransfer von und nach den Färöer Inseln bzw. Andorra daher noch als ein solcher in einen Drittstaat entsprechend den gesetzlichen Vorgaben.

75 Vgl. Art. 6 Abs. 5 DSV.

Denn eine Genehmigung von Standardvertragsklauseln ist dann nicht notwendig, wenn Daten unter der Verwendung von Standardvertragsklauseln nach Anhang 1 der DSV übermittelt werden. In diesen Fällen sind wir vom Inhaber der Datensammlung über die Datenbekanntgabe unter Verwendung dieser Standardvertragsklauseln lediglich zu informieren. Im Verlauf des Berichtsjahres reichte nur ein international tätiges Unternehmen bei uns eine solche Meldung ein. Diese niedrige Quote zeigt uns, dass hierzulande von den Standardvertragsklauseln noch kaum Gebrauch gemacht wird, obwohl diese einen sehr guten datenschutzrechtlichen Standard gewährleisten würden. Dies gilt auch für den Einsatz von *Binding Corporate Rules* (BCR).[76] Europaweit laufen zur Zeit viele Verfahren zur Anerkennung von BCRs, während in Liechtenstein ansässige bzw. vertretene Unternehmen nach unserer Kenntnis nur in ganz vereinzelten Fällen über die Schaffung und Genehmigung solcher verbindlicher unternehmensinterner Datenschutzvereinbarungen nachdenken oder diese gar beantragen. So wurde 2010 auch nur ein einziger Antrag auf Genehmigung von BCRs gestellt, dessen Bearbeitung zum Jahresende jedoch noch nicht abgeschlossen werden konnte.

2. Öffentlichkeitsarbeit

Die Sensibilisierung der Öffentlichkeit für Themen rund um den Schutz der Privatsphäre gehört zu unseren **Kernaufgaben**. Nicht zuletzt unsere Online-Umfrage vom vergangenen Jahr hat gezeigt, dass der Informationsbedarf gemeinhin nach wie vor gross ist.[77] Um möglichst weite Kreise der Bevölkerung zu erreichen, nutzen wir *unterschiedliche Kanäle* und setzen auf ein *Bündel von Massnahmen*. Neben Veranstaltungen, Schulungen, Publikationen und unserer Internetseite gehört auch der gegenständliche Tätigkeitsbericht zu den zentralen Informationsmassnahmen.[78]

2.1 Veranstaltungen

Der **4. Europäische Datenschutztag** am 28. Januar 2010 stand ganz im Zeichen von Suchmaschinen. Wir organisierten in Zusammenarbeit mit der Hochschule einen Vortragsabend zum Thema **„Einblicke in die Welt von Google & Co: Von Informationsjägern und Datensammlern"**. Wie gross das Interesse am Thema Suchmaschinen und Datenschutz ist, zeigten die über 150 Anmeldungen zur Veranstaltung. Kein Wunder: Das Internet ist heutzutage aus unserer Gesellschaft nicht mehr wegzudenken. Im Dickicht des Informationsdschungels sind daher Suchmaschinen, allen voran Google, von zentraler Bedeutung. Bei unserer Einführung wiesen wir auf die verschiedenen Aspekte bei der Nutzung von Suchmaschinen hin: So können im Sinne einer „multiple identity" mehrere Suchmaschinen verwendet werden, wodurch die Ergebnisse nicht von einer einzigen Suchmaschine zusammengeführt werden können. Eine andere, wohl einfachere, Möglichkeit besteht in einer Nutzung der Meta-Suchmaschine Ixquick, die 2008 den ersten Europäischen Datenschutzgütesiegel gewann. Ixquick gibt an, keine Nutzungsdaten zu speichern.[79] Schliesslich haben Technologien eines gemeinsam: Sie sind an sich weder gut noch schlecht. Es kommt immer darauf an, wie man sie nützt. Und das liegt in der Hand jedes Einzelnen.

Organisiert vom Amt für Soziale Dienste nahmen wir am Auftakt des **Projekts „Gateway"** teil, der als Impulstag für Fachleute aus dem Bereich der Jugend und Sozialarbeit veranstaltet wurde. „Gateway" soll Erwachsenen eine Orientierungshilfe im Medienkonsum der jüngeren Generation geben, da die digitale Kluft zwischen Eltern und Kindern stetig grösser wird. Wir hatten bei dieser Veranstaltung die Möglichkeit, auf die Datenschutzproblematik in sozialen Netzwerken (am Beispiel „Facebook") aufmerksam zu machen.[80] Ausserdem nahmen wir im Rahmen dieses Projektes auch an der LIHGA teil.

Zusammen mit dem Amt für Soziale Dienste wollten wir insbesondere Jugendliche sensibilisieren. Dabei wurde vor Ort eine *Prüfung der Einstellungen zur Privatsphäre* des – auch in Liechtenstein – sehr beliebten *Internetportals Facebook* angeboten. Daneben konnte auch an einem Datenschutzquiz teilgenommen werden. Dabei ging es jedoch nicht um einen eigentlichen Wettbewerb, der darauf abzielt, den Teilnehmern danach Werbematerial zu schi-

76 Vgl. Tätigkeitsbericht 2009, S. 24, mit Hinweisen.
77 Vgl. Tätigkeitsbericht 2009, Anhang, 2.
78 Gemäss Art. 31 DSG.
79 http://eu.ixquick.com.
80 http://www.llv.li/amtsstellen/llv-asd-publikationen/llv-asd-publikationen-3.htm.

cken. Man konnte sich mittels einer Passworteingabe pseudonymisiert anmelden und zeigte damit gleichzeitig, dass ein Wettbewerb auch datenschutzfreundlich organisiert werden kann.

Gleichzeitig war damit ein *Passwort-Check* verbunden,[81] bei dem die Qualität eines Passworts vor Ort durchgeführt wurde. Schliesslich bestand die Möglichkeit, sich selbst zum Thema *Datendiebstahl*[82] zu prüfen. Bei diesem Test, der uns vom deutschen Bundesbeauftragten für Datenschutz und Informationssicherheit zur Verfügung gestellt wurde, geht es um die Prüfung von elf Sachverhalten im Rahmen eines möglichen Risikos von Identitätsdiebstahl. Bei diesem Test wird beispielsweise danach gefragt, ob man die Telefonnummern von Kreditkartengesellschaften für den Fall bereithält, wenn die Karte gestohlen wird, ob im Falle einer Abwesenheit Postsendungen zurückgehalten oder der Briefkasten durch den Nachbarn geleert wird.[83]

Im Rahmen der **Erwachsenenbildung** hielten wir einen **Vortrag** zum Thema **„Spuren im Internet – Ein Blick hinter die Kulissen"**: Durch neue technische Entwicklungen und immer leistungsfähigere Computer wandelte sich auch die Rolle des Internet-Nutzers in jene eines Mitgestalters. In dieser Veranstaltung wurden die Vor- und Nachteile sowie Gefahren für die Privatsphäre der Benutzer dargestellt. Es wurde aufgezeigt, wie Betreiber von sogenannten Internet-Shops ihre Besucher identifizieren und wie zielgruppenorientierte Werbung bekannter Internet-Suchdienste funktioniert. Der Blick hinter die Kulissen sollte helfen, sich vor nicht notwendigen oder allzu übertriebenen *„Spurenlesern"* im Internet zu schützen. Dabei wurden neben der „Macht" der Suchmaschinen auch einfache Anonymisierungsdienste vorgestellt.

81 https://passwortcheck.datenschutz.ch/check.php?lang=de.
82 http://gsb.download.bva.bund.de/BFDI/id_theft/index.html.
83 Weitere Fragen sind z.B., ob Dokumente, die persönliche Informationen enthalten, wie zum Beispiel Rechnungen und Bankauszüge, „geschreddert" werden, bevor sie weggeworfen werden; ob alle personenbezogenen Daten vom eigenen PC gelöscht werden, bevor er verkauft, abgegeben oder weggeworfen wird; ob beim Online-Shopping nur Artikel von seriösen Firmen, denen vertraut wird, gekauft werden; ob die Handy-Rechnung kontrolliert wird, um sicherzustellen, dass sie richtig ist; ob ein Passwort, das schwer zu erraten ist, gewählt wird; ob nur Angaben zur eigenen Kreditkarte am Telefon preisgegeben werden, wenn man selbst angerufen hat, etc.

Neben der seit Jahren üblichen **Datenschutz-Schulung** in der **Landesverwaltung** führten wir wiederum eine **Schulung** an der **Hochschule** des Master-Studiengangs **Business Process Engineering der Wirtschaftsinformatik** durch.[84] Neben einer juristischen Einleitung zur Vorstellung und Anwendung des DSG im betrieblichen Umfeld wurden den Studenten insbesondere die technischen Aspekte wie die Unterschiede zwischen IT-Sicherheit und Datenschutz, Standards und Leitfäden, Privacy Enhancing Technologies (PETs) und deren Anwendung in einem Unternehmen aufgezeigt.

2.2 Neuigkeiten auf der Internetseite

Auf unserer Internetseite „www.dss.llv.li" informieren wir regelmässig über aktuelle Themen, die für die Öffentlichkeit relevant sind.

Wir haben beispielsweise über unsere Veranstaltung anlässlich des Datenschutztages berichtet. Nennenswert sind auch Informationen über *Google Street View* und Werkzeuge für *Selbsttests* und andere Hilfestellungen zum Thema Datenschutz, die wir bereits an der LIHGA vorgestellt hatten. Ein Lernprogramm des Datenschutzbeauftragten des Kantons Zürich gibt nützliche Hinweise für die *Sicherheit von Daten und Dokumenten am Arbeitsplatz*. Und schliesslich kann man mithilfe von Anleitungen der deutschen Kampagne *„Watch your web" Privatsphären-Einstellungen* in den jeweiligen *Social Networking Services* vornehmen, um die persönlichen Daten zu schützen. [85]

Auf diese Werkzeuge haben wir auch mit einer **Plakat-Aktion** mit dem Titel *„Datenklau"* aufmerksam gemacht. Insgesamt wurden landesweit Plakate an öffentlich zugängliche Plätze sowie Stellen mit hoher Besucher-Frequenz verteilt.

Von unseren eigen Aktivitäten ist eine neue Richtlinie zum Thema *„Überwachung der Arbeitnehmer am Arbeitsplatz"* nennenswert. Die Überwachung der Arbeitnehmer am Arbeitsplatz wird durch den Einsatz bzw. durch die alltägliche Nutzung technischer Hilfsmittel (Arbeitsplatzrechner, Mobiltelefone, elektronische Zeiterfassungs- und Schliesssysteme, Videoanlagen, usw.) immer einfacher und es

84 Vgl. Tätigkeitsbericht 2009, 2.1.
85 http://www.llv.li/amtsstellen/llv-dss-selbstdatenschutz.htm.

stellen sich in diesem Zusammenhang viele Fragen. Aus diesem Grund haben wir zusammen mit dem AVW Richtlinien herausgegeben.[86] Neben den allgemeinen rechtlichen Grundlagen und deren Voraussetzungen werden in den Richtlinien vor allem viele konkrete Fallbeispiele aus der Praxis und weiterführende Hinweise gegeben. Weiters haben wir internationale Entwicklungen thematisiert, wie das *Arbeitspapier zur mobilen Bearbeitung personenbezogener Daten* der International Working Group on Data Protection in Telecommunications (IWGDPT), an welchem wir massgeblich mitgearbeitet haben.[87] Als Beispiele sind darüber hinaus das wegweisende Urteil des deutschen Bundesverfassungsgerichts und der Bericht der Art. 29 Datenschutzgruppe zur Vorratsdatenspeicherung zu nennen.[88]

3. Mitarbeit bei der Gesetzgebung

Die Mitarbeit bei der Gesetzgebung ist eine weitere unserer Kernaufgaben. Es hat sich sehr bewährt, wenn wir in einem *möglichst frühen Verfahrensstadion* einbezogen werden. Insgesamt gaben wir zu 26 Gesetzesvorhaben in verschiedenen Stadien des Gesetzgebungsverfahrens eine Stellungnahme ab. Exemplarisch soll im Folgenden aufgrund besonderer datenschutzrechtlicher Relevanz nur auf ein paar wenige Gesetzesvorhaben näher eingegangen werden:

Anlässlich der Totalrevision des **Gesetzes über den Konsumkredit** vom 22. Oktober 1992 wird eine „Vollharmonisierung" im Rahmen der Umsetzung der Verbraucherkreditrichtlinie 2008/48/EG angestrebt. Die Vernehmlassungsvorlage beinhaltete sehr detaillierte Informationspflichten, die ebenso wie der Verweis auf die uneingeschränkte Geltung des DSG aus datenschutzrechtlicher Sicht zu begrüssen sind. Allerdings ist das in der Vorlage vorgesehene Verfahren zur Überprüfung der Kreditwürdigkeit der Konsumenten grundsätzlich sehr kritisch zu betrachten, da ein *Kredit-Scoring* erhebliche Folgen für die Betroffenen haben kann. Denn Kredit-Scoring-Verfahren sind von einer hohen Eingriffsintensität bei den Konsumenten geprägt und können demzufolge eine weitere Beteiligung am Wirtschaftsleben erheblich einschränken: *„Eine von Wirtschaftsauskunftsdiensten festgestellte mangelhafte Bonität hat für die meisten Menschen einen dramatischen Ausschluss von wirtschaftlicher Beteiligung zur Folge. Es ist für diese Menschen praktisch unmöglich, Konten zu eröffnen, neue Kredite zu erhalten, Telefonverträge abzuschliessen oder im Versandhandel auf Rechnung zu bestellen. Auch Verschlechterungen in Zahlungszielen, Bezugskonditionen oder der Entzug von Kundenkarten können die Folge sein."*[89] Die datenschutzrechtliche Zulässigkeit einer Kreditüberprüfung ist demzufolge sehr genau zu analysieren. In unserer Stellungnahme sind wir insbesondere auf die fehlenden spezialgesetzlichen Regelungen betreffend die datenschutzrechtliche Zulässigkeit von Kredit-Scorings und von Datenbanken eingegangen. An dieser Stelle möchten wir die Gelegenheit nutzen und ein paar grundlegende Ausführungen zu Kreditüberprüfungen aus Sicht des Datenschutzes machen:

Das sogenannte Kredit-Scoring dient der Bewertung einzelner Persönlichkeitsmerkmale, die in der Regel im Rahmen einer automatisierten Bearbeitung erfolgt. Die Beurteilung der Kreditwürdigkeit wird im DSG in zwei Vorschriften explizit erwähnt.[90] Die wichtigsten datenschutzrechtlichen Anforderungen an das Kredit-Scoring können wie folgt zusammengefasst werden:[91]

- Die Informationen sind primär bei den betroffenen Personen einzuholen. Erst wenn die für die Bearbeitung notwendigen Daten nicht bei der betroffenen Person selbst erhoben werden können, können diese auch bei Dritten eingeholt werden.
- Die Kategorien der Daten müssen eindeutig festgelegt sein.
- Ausserdem müssen die Daten für die Bewertung der Kreditwürdigkeit notwendig, angemessen und relevant[92] sein.

86 Das Merkblatt „Überwachung der Arbeitnehmenden am Arbeitsplatz" ist auf unserer Internetseite abrufbar. http://www.llv.li/amtsstellen/llv-dss-richtlinien/llv-dss-ueberwachung-arbeitnehmer.htm; vgl. 1.7.

87 Näheres dazu unter 4.6. sowie http://www.llv.li/llv-dss-aktuelles.htm?reference=147393&checkSum=DBB85D2B4645D4D452833CAEFAAE11E7.

88 Vgl. 1.3. und 4.1.

89 Vgl. Michael Krenn/Hans G. Zeger, in: Lukas Bauer/Sebastian Reimer (Hrsg.), Handbuch Datenschutzrecht, Wien 2009, S. 535.

90 Art. 6 Abs. 1 und Art. 17 Abs. 2 Buchstabe c DSG.

91 Vgl. auch den Beitrag der Art. 29 Datenschutzgruppe zur öffentlichen Konsultation der GD MARKT zu dem Bericht der Expertengruppe „Kredithistorien", angenommen am 01. Dezember 2009, WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp164_de.pdf.

92 Vgl. Dr. Thilo Weichert, Datenschutzrechtliche Anforderungen an Verbraucher-Kredit-Scoring, in: Datenschutz und Datensicherheit (DuD) 29 (2005), S. 582ff., 584: „[…] Relevanz haben nur Sach-

- Der Zweck der Datenerhebung muss eindeutig definiert werden.
- Die Rechte der Betroffenen müssen gewahrt werden. Von besonderer Wichtigkeit sind ein vollumfängliches Informationsrecht sowie die Möglichkeit zur Geltendmachung der anderen gesetzlichen Rechte (Auskunfts-, Widerspruchs-, Berichtigungs- und Löschrecht). Aus diesem Grund ist es unentbehrlich, dass die Konsumenten hinreichend über das Prüfungsverfahren und auch über ihre Rechte unterrichtet sind. Denn nur bei einer umfassenden Information ist es den betroffenen Personen möglich, ihre Rechte auch auszuüben. In diesem Zusammenhang ist vor allem auf die Gefahr hinzuweisen, dass mit völlig veralteten Daten gearbeitet wird, die nicht mehr den tatsächlichen Gegebenheiten entsprechen. Hier besteht zum Beispiel ein Anspruch auf Berichtigung bzw. Löschung dieser Daten.

Das **Asylgesetz** (vormals: Flüchtlingsgesetz) wurde total revidiert, das Gesetzgebungsverfahren ist noch nicht abgeschlossen. Gründe für die Revision des Flüchtlingsgesetzes waren u.a. die fortlaufenden europäischen Harmonisierungsbestrebungen in der Asylgesetzgebung (Überarbeitung der EU- Richtlinien und Schengen/Dublin-Acquis). Wesentliche Bestimmungen betrafen beispielsweise die Schaffung einer gesetzlichen Grundlage für die Erhebung und Bearbeitung von biometrischen Daten zur Feststellung der Identität von Asylsuchenden und Schutzbedürftigen oder die Bestimmungen zur Informationspflicht der asylsuchenden Person. Das *Recht auf Information* spielt auch hier als Voraussetzung für andere Rechte (Auskunft, Berichtigung) eine wesentliche Rolle. In diesem Zusammenhang ist auch zu erwähnen, dass Grundsätze der Kommunikation im Asylverfahren neu eingeführt werden sollen. Die Eurodac Supervision Coordination Group hat im Übrigen zu diesem Thema eine koordinierte Inspektion durchgeführt und vergangenes Jahr einen Bericht darüber publiziert.[93]

Im Rahmen der Weiterentwicklung des Schengen-Besitzstandes stand die Übernahme der VIS-Verordnung[94] ins **Ausländergesetz** zur Debatte. Dazu konnten wir in einem frühen Stadium Stellung nehmen. In der VIS-Verordnung werden Zweck, die Funktionen sowie die Zuständigkeiten für das System festgelegt. Darüber hinaus werden die verschiedenen Verfahren für den Austausch von Visadaten zwischen den Schengen-Staaten beschrieben. Um eine zuverlässige Identifizierung der Antragsteller eines Visums zu ermöglichen, werden im System auch biometrische Daten (Fotografie und Abdrücke der zehn Finger) erfasst. In der Vorlage war ausserdem vorgesehen, welche Behörden zu welchem Zweck Daten des zentralen Visa-Systems online abfragen können.

Auch bei der Gesetzesvorlage zur Bekanntgabe von Umsatzdaten von Leistungserbringern nach dem **Krankenversicherungsgesetz** (KVG) gaben wir eine Stellungnahme ab. Unseres Erachtens gab es bei der Vorlage einen gewissen Widerspruch. Denn einerseits sollten *Zahlen von Leistungserbringergruppen publiziert* werden (wobei es Gruppen gibt, bei denen es nur sehr wenige oder gar nur ein Mitglied gibt), auf der anderen Seite sollte die Anonymität gewährleistet werden. Aufgrund eines Papiers der Art. 29 Datenschutzgruppe wiesen wir darauf hin, dass der Gesetzgeber eine Grenze festlegen sollte. Diese Grenze sollte definieren, ab welcher Anzahl Betroffener die Anonymität gewährleistet ist. Die Arbeitsgruppe hält hierzu am Beispiel von statistischen Erhebungen und der Kombination vereinzelter Informationen fest: „*In jeder Situation sollte ein Grenzwert festgelegt werden, unter dem die Identifizierung einzelner Personen als möglich angesehen wird. Wenn ein Kriterium die Identifizierung in einer bestimmten*

verhalte, die mit der Kreditwürdigkeit in einem unmittelbaren Zusammenhang stehen. Dazu gehören z.B. grundsätzlich nicht Erfahrungen aus anderen, nicht vergleichbaren Vertragsverhältnissen (z.B. Arbeits-, Miet-, Telekommunikationsvertrag). Zur Beurteilung der Kreditwürdigkeit erscheinen folgende üblicherweise verwendeten Daten relevant: Vermögen, Einkommen, Beruf, Dauer der Beschäftigung, Sicherheiten, Verbindlichkeiten, regelmäßige Ausgaben, Zahl und Höhe der bestehenden Kredite, Insolvenz oder andere harte Negativdaten, finanzielle Allgemeinbildung. Nicht relevant erscheinen dagegen Adresse, Wohnumfeld, Haushaltstyp, Wohndauer, Geschlecht, Familienstand, Alter, Zahl der Kinder, Kfz-Besitz, Religionszugehörigkeit. Daten Dritter haben grundsätzlich keine Relevanz für die Score-Berechnung. Dies gilt in jedem Fall für Daten, aus denen auf den Betroffenen geschlossen werden soll (z.B. Bildungsstand der Eltern). Aber auch sonstige Angaben Dritter (z.B. Alter der Kinder) sind nicht mit einzubeziehen. […]“

93 Eine Zusammenfassung des Berichts in deutscher Sprache kann von unserer Internetseite unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/09-06-24_Eurodac_report2_summary_DE.pdf heruntergeladen werden.

94 Verordnung (EG) Nr. 767/2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedsstaaten über Visa für einen kurzfristigen Aufenthalt.

Personengruppe gleich welcher Größe (z.B. nur ein Arzt in einer Stadt mit 6000 Einwohnern) zu ermöglichen scheint, sollte dieses Unterscheidungskriterium weggelassen oder andere Kriterien zur „Verschleierung" der Ergebnisse über eine bestimmte Person aufgenommen werden, um die statistische Geheimhaltungspflicht zu erfüllen."[95]

Weiters haben wir zu folgenden Gesetzesprojekten eine Stellungnahme abgegeben.

- Abkommen mit der Russischen Föderation über die Rückübernahme und Visumerleichterung;
- Arbeitslosenversicherungsgesetz;
- Dienstleistungsgesetz;
- E-Geldgesetz;
- FMA-Gesetz;
- Gewerbegesetz;
- Gesetz über die Hochschule Liechtenstein;
- Gesetz über das öffentliche Auftragswesen;
- Gesetz über das öffentliche Auftragswesen im Bereich der Sektoren;
- Gesetz über das Zentrale Personenregister;
- Gesetz über die Staatsanwaltschaft;
- Öffentlichkeitsregisterverordnung;
- Polizeigesetz;
- Steueramtshilfegesetz;
- Steueramtshilfegesetz-UK;
- Steuergesetz;
- Strassenverkehrsgesetz;
- Verordnung über die Ausübung von Tätigkeiten nach Art. 180a des Personen- und Gesellschaftsrechts;
- Verordnung über die Informationssysteme bei der Landespolizei;
- Verordnung über den nationalen Teil des Schengener Informationssystems und das SIRENE-Büro;
- ViCLAS-Konkordat.

4. Internationale Zusammenarbeit

4.1 Art. 29 Datenschutzgruppe

Die Art. 29 Datenschutzgruppe erweist sich weiterhin als ein Gremium, in dem wichtige Themen behandelt werden, die auch für Liechtenstein von grosser Bedeutung sind.

Anfang des Jahres wurde ein Arbeitsprogramm 2010-2011 angenommen. Dabei wurde festgestellt, dass sie nicht nur eine Anwendung der derzeitigen Rechtsvorschriften sicherstellen, sondern auch die Herausforderungen der Zukunft in Angriff nehmen will. Die Arbeitsgruppe muss sich etwa den neuen technologischen Entwicklungen und der Globalisierung stellen, aber auch die institutionellen Änderungen, die sich durch den Vertrag von Lissabon ergeben, angehen. Als Kern der Tätigkeiten kristallisierten sich die Vorarbeiten zu einer **Revision der Datenschutzrichtlinie** heraus. Die Arbeitsgruppe erstellte verschiedene Papiere und Stellungnahmen zum Thema, da diese Revision sich unmittelbar auf die Arbeit der Datenschutzbehörden auswirken wird. Die Europäische Kommission verabschiedete zur Zukunft des Datenschutzes ein *„Gesamtkonzept für den Datenschutz in der Europäischen Union"*, das als Basis für die Revision gilt. Die Öffentlichkeit wurde zur Stellungnahme eingeladen. Als betroffene Behörde waren auch wir mit der Vorbereitung einer Stellungnahme befasst.

Die Arbeitsgruppe beschäftigte sich ausserdem mit dem auch in Liechtenstein aktuell gewordenen Thema **Google Street View** und nicht nur mit dem Kernthema selbst, sondern auch mit dem im Verlauf der Aufnahmen aufgetauchten Aspekt der Sammlung von WLAN-Daten. Da die Fahrten in Liechtenstein noch nicht stattgefunden haben, ist dieser Aspekt für uns nicht so wichtig. Etwas schwierig gestaltet sich dieses Thema in der Arbeitsgruppe, da Street View in einigen Ländern bereits verwirklicht ist und in anderen erst noch ansteht. Insgesamt erwiesen sich die Informationen der Arbeitsgruppe wie auch anderer Datenschutzbehörden bei den bisherigen Verhandlungen mit Google als sehr hilfreich.[96]

Die Arbeitsgruppe verabschiedete auch den **Bericht** 01/2010 über die zweite gemeinsame Durchsetzungsmassnahme. Diese Massnahme beschäftigte sich mit der **Umsetzung der Richtlinie zur Vorratsdatenspeicherung** von Verkehrsdaten im Telekommunikationsbereich. Obwohl die Richtlinie in Liechtenstein noch nicht umgesetzt werden musste, war sie inhaltlich bereits teils bestehendes Recht. Vor diesem Hintergrund hatten wir uns dazu entschlossen, an der Untersuchung teilzunehmen. Die

95 Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 25, abrufbar unter: http://www.llv.li/pdf-llv-li-stellungnahme_4_2007_zum_begriff_personenbezogene_daten-2.pdf.

96 S. dazu ausführlich unter 1.2.

Schlussfolgerungen der einzelnen teilnehmenden EWR-Datenschutzbehörden flossen in den erwähnten Bericht ein, der verschiedene Empfehlungen enthält. Da wir auch mit einer Vorbereitung einer Kontrolle im Telekommunikationssektor begonnen haben, werden die Empfehlungen dort zu berücksichtigen sein.

Die Arbeitsgruppe nahm zudem eine **Stellungnahme zum anwendbaren Recht** an, die angesichts einer zusammenwachsenden Welt und der zahlreichen innereuropäischen Datenflüsse in der Praxis sehr wichtig sein wird.

4.2 Gemeinsame Kontrollinstanz Schengen

Wir nahmen weiterhin als Beobachterin an Sitzungen der Gemeinsamen Kontrollinstanz Schengen teil. Die Gemeinsame Kontrollinstanz Schengen überwacht, ob die Verwendung der Daten im Schengener Informationssystem (SIS) mit dem Schengener Durchführungsübereinkommen übereinstimmt.

Im Berichtsjahr konnte die **koordinierte Prüfung** von Ausschreibungen zur **Einreiseverweigerung** in das Schengengebiet abgeschlossen werden. Dabei handelte es sich um eine Nachuntersuchung zu Art. 96 des Schengener Durchführungsübereinkommens. Die Bestimmungen dieses Artikels zielen u. a. darauf ab, Personen, die schon einmal abgeschoben oder ausgewiesen worden sind (z.B. nach einem abgelehnten Asylantrag), vorläufig nicht erneut ins Schengengebiet einreisen zu lassen, um gegebenenfalls neuerlich Asyl zu beantragen.

Des Weiteren wurde im Rahmen des SIS ein **Leitfaden** zur Wahrnehmung des Auskunftsrechts fertig gestellt. Darin werden die Einzelheiten der Ausübung des **Auskunftsrechts** betreffend das SIS beschrieben. Er soll einerseits den Betroffenen die Ausübung ihres Auskunftsrechts erleichtern. Andererseits ist der Leitfaden auch als praktisches Hilfsmittel für Personen bestimmt, die beruflich mit dem Auskunftsrecht zu tun haben (Datenschutzbehörden, Polizeikräfte, Ausländerbehörden, Rechtsanwälte usw.). Der Leitfaden umfasst drei Teile: einen Abriss der Grundprinzipien und der wichtigsten Definitionen im Zusammenhang mit dem SIS, eine Beschreibung des Verfahrens zur Ausübung des Auskunftsrechts in jedem betroffenen Staat und schliesslich eine Schilderung mehrerer besonderer Situationen, in denen ein spezielles Verfahren erforderlich ist.

4.3 Eurodac Supervision Coordination Group

Ein wesentliches Thema betraf eine zukünftige **koordinierte Kontrolle** betreffend die **vorzeitige Löschung** von Daten: Das Eurodac System sieht strikte zeitliche Fristen für die Speicherung von Daten vor. Diese Fristen differieren zwar je nach Kategorie von Daten, der Grundsatz sieht jedoch eine automatische Löschung der Daten aus der Zentraleinheit spätestens 10 Jahre nach Abnahme der Fingerabdrücke vor. Zusätzlich zu diesem System der automatischen Löschung sieht die Eurodac Verordnung eine vorzeitige Löschung in bestimmten Fällen vor, etwa wenn sich der Status eines Asylsuchenden geändert hat. Die vorzeitige Löschung wird in einzelnen Mitgliedsstaaten nicht immer in adäquater Weise sichergestellt, wie sich aus den Beiträgen der nationalen Datenschutzbehörden bei einer ersten koordinierten Kontrolle herauskristallisiert hat. Der Hauptzweck dieser Inspektion ist es, zu prüfen, ob und wie die vorzeitige Löschung von den nationalen Eurodac Behörden durchgeführt wird, und ob eventuell Bedarf für neue technische Lösungen besteht.

4.4 Europarat

Der Beratende Konventionsausschuss des Europarats beendete die Arbeiten an einer Empfehlung zum Thema **„Profiling"**. Der Beschluss des letzten Jahres, wonach die Empfehlung nur für den privaten Sektor anwendbar sein soll, wurde wieder rückgängig gemacht. Wie bereits erwähnt, ist dieser Text für Liechtenstein besonders interessant, da Liechtenstein neben der Schweiz das einzige Land in Europa zu sein scheint, welches den Begriff des *„Persönlichkeitsprofils"* gesetzlich vorsieht. Gemäss einer vom Europarat in Auftrag gegebenen Expertenstudie geht es z.B. um die Datenbearbeitung durch Suchmaschinen, das digitale Kabelfernsehen, die Bildung von Kundenprofilen, insbesondere bei Banken und Versicherungen, usw.[97]

97 Vgl. Tätigkeitsbericht 2008, 10.2.2.

4.5 Europäische Datenschutzkonferenz

Wir nahmen auch im Berichtsjahr als Beobachterin an Sitzungen der **Working Party on Police and Justice** teil. Ein Thema betraf den *Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten*, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Dieser Rahmenbeschluss stellt eine Weiterentwicklung des Schengen-Besitzstandes dar und ist somit für den Schengen-Beitritt relevant.

Wie bereits ausgeführt, arbeitet die Europäische Kommission an einem *neuen, einheitlichen Rechtsrahmen im Bereich Datenschutz*. Ein solcher ist aufgrund des Wegfalls der Säulenstruktur mit dem *Vertrag von Lissabon* notwendig. Die Working Party on Police and Justice beschäftigte sich vergangenes Jahr auch mit diesem Thema.

Im Rahmen der europäischen Konferenz werden zweimal pro Jahr sogenannte **Case Handling Workshops** abgehalten. Bei diesen Workshops werden aktuelle Themen und konkrete Fälle behandelt, welche für die Datenschutzbehörden in Europa wichtig sind. Im Berichtsjahr nahmen wir nur an einem Workshop teil. Bei dieser Veranstaltung ging es darum, wie in den verschiedenen Ländern Datenschutzkontrollen geführt werden. Zum ersten Mal war der Workshop so organisiert, dass es drei Gruppen gab, in denen die Themen besprochen wurden. Die Gruppen waren nach Grösse und Personalbestand der Datenschutzbehörde eingeteilt. Dieser Workshop war für uns besonders wertvoll, da wir uns in diesem Jahr das notwendige Know-how zur Durchführung von Datenschutzkontrollen angeeignet haben.

4.6 Internationale Datenschutzkonferenz

Im Rahmen der International Working Group on Data Protection in Telecommunications brachten wir eine Diskussionsgrundlage zum Thema *Datenschutz auf mobilen Endgeräten (Mobiltelefone, Notebooks, usw.)* ein.[98] Mobile Geräte besitzen naturgemäss eine kleine Bauform und ein geringes Gewicht, wodurch sich spezifische Risiken für die Datensicherheit, wie z.B. der Manipulation, dem Verlust und auch dem Diebstahl der Daten, ergeben. Während eine Manipulation oder Löschung von Daten in der Regel für den Dateninhaber rasch erkennbar ist, wird ein Datendiebstahl oftmals erst dann bemerkt, wenn die Daten selbst oder das Ergebnis einer Bearbeitung an einem anderen Ort wieder auftauchen.

Bei den Risiken unterscheidet das *Arbeitspapier zwischen Risiken in der Kommunikation* (z.B. Verwendung offener unverschlüsselter drahtloser Netzwerkzugänge, Auswertung von Standortdaten, usw.) sowie von spezifischen Risiken der Datenbearbeitung und Speicherung (z.B. Infektion durch Schadsoftware bzw. der Datenbeschädigung durch unsichere Applikationen, nicht beglaubigter (zertifizierter) Drittsoftware usw.). Basierend auf den zahlreichen Risiken der Nutzung von mobilen Geräten erarbeitete die Arbeitsgruppe unter unserer Federführung Empfehlungen sowohl für die Hersteller/Anbieter als auch die Nutzer, die anschliessend veröffentlicht wurden. Die *Bewusstseinsbildung der Anwender* wird dabei als wichtiger Punkt zur Vorbeugung von Missbrauch, Datenverlust und Diebstahl genannt. Konkret empfiehlt das Arbeitspapier den Anbietern sämtlichen Anwendern jene Möglichkeiten zur Verfügung zu stellen, die eine ordnungsgemässe Wahrnehmung der Eigenverantwortung ermöglicht, z.B. entsprechend einfache und verständliche Nutzerinformationen und Hinweise.

Weiters wird empfohlen, die Geräte mit *datenschutzfreundlichen Sicherheitseinstellungen* auszuliefern. Auch sollten Schnittstellen, die zur Erhebung und Übermittlung von Daten dienen (z.B. Kamera, GPS, Mikrofon, IrDA, Bluetooth, WLAN, usw.), werksseitig bei der ersten Inbetriebnahme deaktiviert sein. Weiters sollten Anbieter/Hersteller den Nutzern vor dem Herunterladen und vor der Installation von Applikationen die Möglichkeit geben, insbesondere den Namen und die elektronische Signatur des Anbieters, die Nutzungsbedingungen, die zur Ausführung erforderlichen Zugriffsrechte auf Gerätehardware sowie bereits installierter Software, Hinweise zur Deinstallation als auch weitere sicherheitsrelevante Informationen und Warnhinweise in einfacher Weise und in einer selbst gewählten Sprache einzusehen.

Für die Nutzer empfiehlt die Arbeitsgruppe, *öffentliche Internetzugänge mit Vorsicht zu verwenden*.

98 Vgl. Tätigkeitsbericht 2009, 4.6.

Vertrauliche Informationen und Daten sollten nicht über unsichere Netzwerkverbindungen verarbeitet werden. Auch sollten für den unmittelbaren Betrieb nicht benötigte Schnittstellen über die Einstellungen des mobilen Geräts deaktiviert und der Zugriff der installierten Fremdapplikationen sollte auf die für den ordnungsgemässen Betrieb erforderlichen Daten eingeschränkt werden. So benötigt zum Beispiel nicht jede Anwendung den Zugriff auf das Adressbuch oder den Kalender des mobilen Geräts. [99]

Weiters wurde das **Arbeitspapier „Working Paper on the Use of Deep Packet Inspection (DPI)**[100] **for Marketing Purposes"** angenommen. Primär empfiehlt die Arbeitsgruppe darin den Internet-Providern, die Nutzung von DPI-Technologien zur gezielten Steuerung nutzungsbezogener Werbung (engl. Behavioural Advertising) zu unterlassen und spricht sich ganz klar dagegen aus.[101]

5. In eigener Sache

Im letzten Tätigkeitsbericht hatten wir einige **Grundgedanken** zum Schutz der Privatsphäre in Liechtenstein formuliert. Datenschutz kann als ein Wettbewerbsvorteil gesehen werden, der mit den in den Grundgedanken geäusserten Ideen etwa eines *„Datenstandortes Liechtenstein"*, eines Datenschutz Gütesiegels oder einer Art *Datenschutzpreis (privacy award)* verbessert werden kann.[102] Ohne Frage wären auch entsprechende Massnahmen des Gesetzgebers wichtig, wobei in den Worten der Regierung eine gute Mischung zwischen persönlichen Freiheiten und notwendiger Überwachung erreicht werden muss.[103] Dabei sollte die immaterielle Natur des Schutzes des Persönlichkeitsrechts entsprechend berücksichtigt werden.[104] Es ist auch zu hoffen, dass einige Fälle, die bei der Datenschutzkommission hängig sind, Klarheit in verschiedenen Angelegenheiten schaffen.

Mit dem Inkrafttreten des Vertrages von Lissabon wurde der Datenschutz in der EU deutlich aufgewertet.[105] In Liechtenstein wird der Datenschutz nicht in der Verfassung genannt, stellt aber immerhin einen Teilbereich der *Geheim- und Privatsphäre* gemäss Art 32 Abs 1 LV bzw. Art 8 EMRK dar; dies im Einklang mit der Schweiz, aber im Gegensatz zu Österreich und Deutschland, wo jeweils ein entsprechendes *spezifisches Grundrecht* besteht.[106] Da der Vertrag von Lissabon für Liechtenstein nicht anwendbar ist, hat eine entsprechende Aufwertung des Datenschutzes in Liechtenstein nicht stattgefunden.

Das DSG weist einzelne Unstimmigkeiten auf. Beispielsweise wurde uns zwar mit der letzten Revision des Gesetzes die Möglichkeit gegeben, Entscheidungen der Datenschutzkommission, die nicht in unserem Sinne erfolgen, weiterzuziehen. Dies gilt jedoch nicht im Fall von Bewilligungen zu Videoüberwachungsanlagen im öffentlichen Raum. Auf diese Unstimmigkeit haben wir beim Ressort Justiz hingewiesen, da die Datenschutzrichtlinie eine solche Ausnahme nicht vorsieht. Ebenso wenig ist dies vom Zusatzprotokoll zum Datenschutzabkommen des Europarates, welches von Liechtenstein 2009 ratifiziert wurde und für Liechtenstein im Berichtsjahr in Kraft getreten ist, vorgesehen.

So wurden mit der letzten Revision des Gesetzes die Bestimmungen zur **Anmeldung von Datensammlungen** geändert. Diese Änderung führte nach unserer Ansicht zu gewissen Problemen in der Praxis. Wir haben das Ressort Justiz, welches für das DSG zuständig ist, auch darauf hingewiesen. Ebenso haben wir angeregt, dass eine Bestimmung geschaffen wird, mit der kleinere Unternehmen von einer Meldepflicht zum Register ausgenommen werden. Eine solche Regelung könnte sich daran orientieren, dass nur Unternehmen ab einer gewissen Grösse oder

99 http://www.datenschutz-berlin.de/attachments/724/WP_Mobile_Verarbeitung_und_Datensicherheit_final_clean_675_41_19.pdf?1292412668.

100 Vereinfacht dargestellt steht Deep Packet Inspection (DPI) für ein Verfahren zur Überwachung und Filterung von Netzwerkverkehr, wobei neben den Verwaltungsdaten (engl. Header) auch die Inhalte der übertragenen Datenpakete auf bestimmte Merkmale und Eigenschaften untersucht werden.

101 http://www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf?1292413821.

102 Vgl. Tätigkeitsbericht 2009, II.1.

103 Agenda 2020 für das Fürstentum Liechtenstein, S. 27: http://regierung.li/fileadmin/dateien/Downloads/RA-2010-1845-Agenda-2020-05-10-2010.pdf.

104 Urteil des deutschen Bundesverfassungsgerichts zur Vorratsdatenspeicherung vom 02.03.2010, Randnummer 252.

105 Mitteilung der Europäischen Kommission vom 22.04.2010: „Ein Raum der Freiheit, der Sicherheit und des Rechts für die Bürger Europas – Aktionsplan zur Umsetzung des Stockholmer Programms".

106 Vgl. Hilmar Hoch: Die Regelung des staatlichen Zugriffs auf Fernmeldedaten im Kommunikationsgesetz aus grundrechtlicher Sicht, in: LJZ 4 / 2009, S. 101.

Unternehmen, die „problematische" Daten bearbeiten, einer Meldepflicht unterstehen.

Wie schon mehrfach erwähnt, haben wir die Aufgabe, ein **Register der Datensammlungen** zu führen.[107] Dieses Register dient zum einen der Transparenz gegenüber der Öffentlichkeit und soll die Ausübung des Auskunftsrechts erleichtern. Ausserdem ermöglicht die Erfassung der Datensammlungen die Aufsicht.[108] Der Gesetzgeber hat die Wichtigkeit dieser Bestimmung dadurch unterstrichen, dass eine private Person, die *vorsätzlich Datensammlungen nicht meldet oder bei der Meldung falsche Angaben macht, strafbar ist*.[109] Diese Wichtigkeit kann damit umschrieben werden, dass die Registermeldung das zentrale Element eines mehrstufigen Kontrollsystems darstellt.[110] Mittels einer Zusammenstellung häufig gestellter Fragen und den dazugehörigen Antworten *(engl. FAQ)* haben wir die seit 01. Juli 2009 geltenden Gesetzesbestimmungen näher erläutert und die bis dato eingegangenen Anfragen dargestellt. Wir haben das Register auch modernisiert und den Anmeldeprozess, die Voraussetzungen für die gesetzlich vorgeschriebenen jährlichen Meldungen sowie die Recherche im Register auf der Internetseite benutzerfreundlicher gestaltet und wesentlich vereinfacht. Anträge können nun elektronisch eingereicht werden, wo sie ohne Medienbruch direkt in das Register zur Prüfung übernommen werden können. Durch diese Umstellung wird insbesondere die Datenqualität der im Register geführten Datensammlungen erhöht. Zu Jahresende waren 542 Datensammlungen im Register registriert.

107 Vgl. u. a. Tätigkeitsbericht 2007, 6., Tätigkeitsbericht 2008, 3.2. und Tätigkeitsbericht 2009, 1.1.2.; weitere Informationen unter: http://www.llv.li/amtsstellen/llv-dss-register_datensammlungen.htm.

108 Heinz-Josef Stotter, StVG, PolG, DSG, Triesen 2009, S. 540. S. auch Dietmar Jahnel, Handbuch Datenschutzrecht, Wien 2010, S. 319 ff.

109 Art. 40 Abs. 2 Buchstabe a DSG.

110 Ulrich Dammann/Spiros Simitis: EG Datenschutzrichtlinie-Kommentar, Baden-Baden 1997, S. 239.

III. AUSBLICK

Wie erwähnt lässt der Beitritt zu **„Schengen" und „Dublin"** weiter auf sich warten. Wir werden voraussichtlich im Frühjahr 2011 die Datenschutzevaluation durchlaufen, die einem Beitritt zu „Schengen" vorangestellt ist. Dabei werden wir internationalen Experten unsere Arbeit darlegen. Diese werden danach einen Bericht zu unserer Schengentauglichkeit erstellen. Mit einem Beitritt zu „Schengen" und „Dublin" wachsen auch die Anforderungen, die an uns gestellt werden. Wie bereits ausgeführt, gibt es in beiden Bereichen harmonisierte Datenschutzkontrollen, die durchgeführt werden müssen. Das Knowhow zur Durchführung von Kontrollen haben wir inzwischen aufgebaut.

Ausserdem bleibt zu hoffen, dass verschiedene derzeit vor der **Datenschutzkommission** hängige Verfahren zur Klärung und Festigung von datenschutzrechtlichen Aspekten beitragen werden.

Wie ebenfalls erwähnt, darf man auf den Fortgang in Sachen **Google Street View** sehr gespannt sein. Dies gilt auch in Bezug auf das Gerichtsverfahren, das in der Schweiz derzeit läuft. Gespannt sein darf man nicht nur, weil dieses Verfahren zeigen wird, inwiefern die heutigen Rechtsgrundlagen genügen, um den Fall befriedigend zu lösen (und weil wir nicht so oft mit einem Weltkonzern zu tun haben).

Auf alle Fälle wird die begonnene Revision der **allgemeinen Datenschutzrichtlinie** zu gegebener Zeit auch bei uns zu Änderungen führen. Mit dem Vertrag von Lissabon wurde der Datenschutz in der EU gestärkt. Wir hoffen, dass die Revision der Richtlinie auch in Liechtenstein zu einer Stärkung des Datenschutzes führen wird. Ob das Gleiche für die Revision der Richtlinie zur Vorratsdatenspeicherung gilt, ist offen.

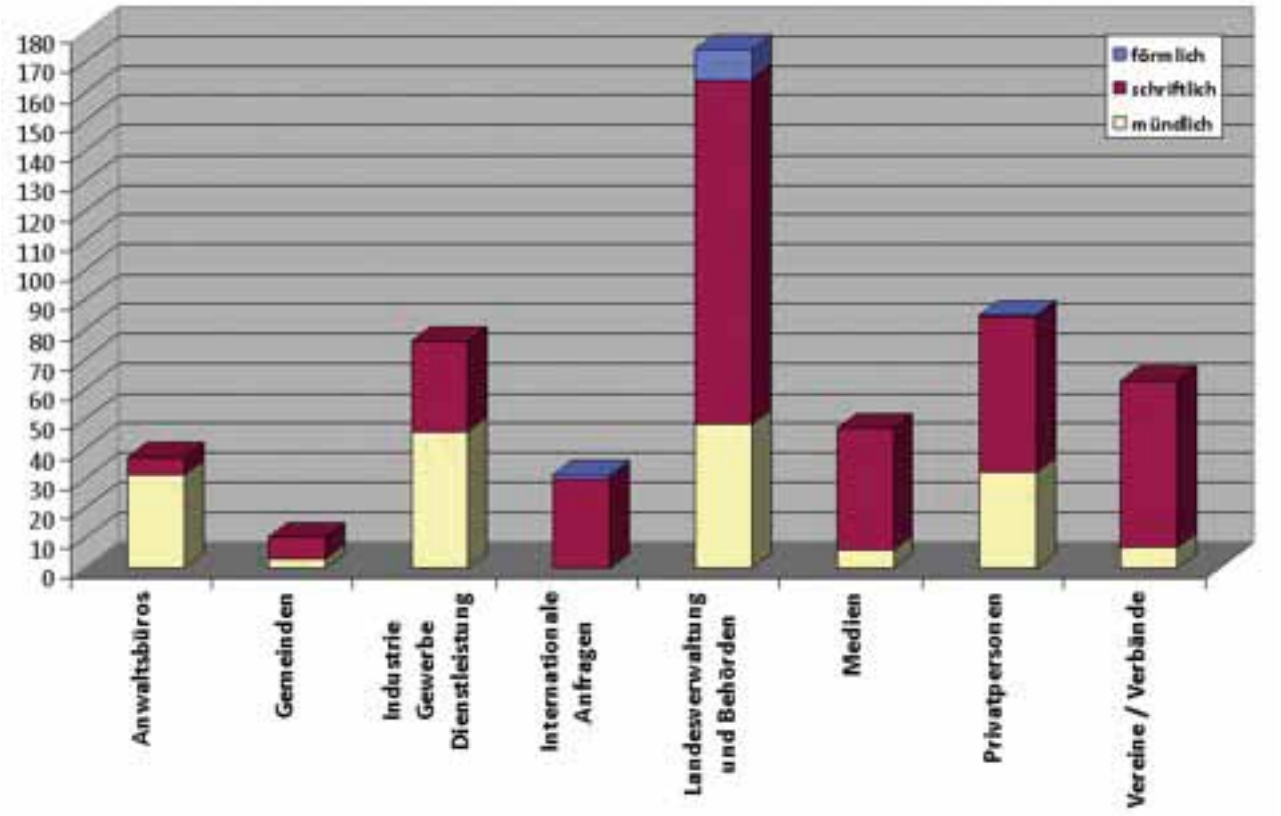
In unserer **Gesellschaft** ist einen **Wandel** zu beobachten, wonach die Wahrnehmung der Privatsphäre, zumindest im Internet, sich stark verändert. Zahlreiche Beispiele im Rahmen von sozialen Netzwerken wie Facebook scheinen dies zu belegen (Es ist aber auch möglich, dass dies nur ein vorübergehender „Hype" ist). Nichtsdestotrotz gibt es zahlreiche Lebensbereiche, in denen eine solche Freizügigkeit im Umgang mit den eigenen Daten nicht festzustellen ist. Die Privatsphäre ist ein Recht, das durch die Verfassung, und somit unsere Grundordnung geschützt wird. An einem Finanzplatz wie Liechtenstein erstaunt es nicht, dass vielfach vermögenswerte Informationen als sehr sensibel eingestuft werden. Wir arbeiten daran, diese Sichtweise auch auf die anderen Lebensbereiche auszudehnen.

Es gibt weiterhin viel zu tun!

IV. ANHANG

Statistik: Beratung privater Personen und Behörden

Die Beratung privater Personen und Behörden ist eine Kernaufgabe. Im Berichtsjahr gingen insgesamt 523 Anfragen ein, so viele Anfragen wie nie zuvor. Gegenüber dem Vorjahr bedeutet das eine Zunahme um 92 Anfragen. Wie die nachfolgende Übersicht zeigt, stammen die meisten Anfragen nach wie vor von der Landesverwaltung.



Gesetzesthemen

Bei den Sachgebieten standen allgemeine Datenschutzthemen gefolgt von Gesetzesvorhaben sowie der Geltendmachung gesetzlicher Rechte im Vordergrund. Vertikal sind die Themen und Sachgebiete aufgeführt, auf horizontaler Ebene, wer angefragt hat.

	Anwaltsbüros	Gemeinden	Industrie, Gewerbe, Dienstleistungen	Internationales	Landesverwaltung und Behörden	Medien	Private Personen	Vereine / Verbände
Datenschutz allgemein	14	3	16	14	55	14	22	34
Arbeitsbereich			9		1	6	1	1
Datenbekanntgabe Inland	1	6	1		22		11	3
Datenbekanntgabe Auslandsbezug	6		10	2	11	5	1	9
Geltendmachung gesetzlicher Rechte	2		4		7		32	5
Gesetzesvorhaben				3	51	1		
Gesundheit / Soziales			1		4		1	1
Polizei / Sicherheit			1		6	14	6	1
Register der Datensammlungen	2	1	13	12	2			
Technologischer Datenschutz	1		9		11	5	9	4
Telekommunikation	3		6		2	2	1	1
Wirtschaft / Finanzen	8		6		2		1	4
Gesamtergebnis	**37**	**10**	**76**	**31**	**174**	**47**	**85**	**63**

DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Kirchstrasse 8
FL-9490 Vaduz

Tel. +423 236 60 90
Fax +423 236 60 99

E-Mail info@dss.llv.li
Website www.dss.llv.li

10