Tätigkeitsbericht

Datenschutzbeauftragter des Fürstentums Liechtenstein

2008

Inhaltsverzeichnis

1. Vorwort

Der 7. Tätigkeitsbericht liegt hiermit vor. Unser Tätigkeitsbericht soll die Öffentlichkeit über die Tätigkeiten des vergangenen Jahres informieren und damit auch dazu beitragen, dass das Bewusstsein zum Datenschutz gestärkt wird.

Bereits im Vorwort des letzten Tätigkeitsberichts wurden gravierende Verletzungen des Datenschutzrechts in Europa, aber auch in Liechtenstein aufgezeigt. Vergangenes Jahr war das Ausmass der Steueraffäre noch nicht erkennbar. Gewiss sind die Auswirkungen auch im Zusammenhang mit der globalen Finanzkrise zu sehen. Allgemein sind im Finanzbereich grosse Änderungen im Gange, was den Schutz der Privatsphäre betrifft. In Liechtenstein ist oft vom Schutz der Privatsphäre die Rede, wenn es eigentlich um deren finanziellen Aspekt geht. Es ist jedoch wichtig, den Datenschutz und damit die Privatsphäre in seiner ganzen Bandbreite darzustellen. Der vorliegende Tätigkeitsbericht stellt ein Element zur Sensibilisierung zum Schutz der Privatsphäre dar.

Das vergangene Jahr war hauptsächlich geprägt durch Vorbereitungen zu einem künftigen Beitritt Liechtensteins zu den Abkommen von Schengen und Dublin. In diesem Zusammenhang wurde auch das Datenschutzgesetz geändert. Die Stabsstelle für Datenschutz wurde von der Landesverwaltung ausgegliedert und dem Landtag unterstellt. Damit war weiters eine Namensänderung auf Datenschutzstelle verbunden. Dankenswerter Weise beschloss der Landtag auch die erforderlichen zusätzlichen Stellen. Darüber hinaus wurden für die anstehende Datenschutzevaluation verschiedene Vorbereitungsarbeiten getroffen.

Ein anderer Kernpunkt betrifft die Entwicklung im Bereich der Videoüberwachung. Nach der Entscheidung der Datenschutzkommission zur Videoüberwachung in der Fussgängerzone in Vaduz hat sich der Landtag in einer anderen Revision des Datenschutzgesetzes des letzten Jahres dazu entschieden, eine klare Regelung zu treffen. Damit kann in diesem Zusammenhang ein Wildwuchs, wie er andernorts zu beobachten ist, vermieden werden. Die Entscheidung der Datenschutzkommission hat nicht nur die Meinung des Datenschutzbeauftragten bestätigt. Vielmehr hat sie einige Grundaussagen zum Schutz der Privatsphäre bei staatlichen Massnahmen getroffen und kann somit als ein Meilenstein gesehen werden.

Im Gesundheitsbereich fanden zwei Vorhaben aus dem Vorjahr ihren erfolgreichen Abschluss. Einerseits beim so genannten «Integrierten Case Management» und andererseits beim Teilprojekt «Kopie der Arztrechnung». Diese beiden Vorhaben sind im Zusammenhang mit den Kostensteigerungen im Gesundheitswesen zu sehen. Dabei spielt der Datenschutz eine wichtige Rolle.

Wir erhielten vergangenes Jahr auch wieder zahlreiche Anfragen. An dieser Stelle seien nur einige genannt, welche im Bericht, zusammen mit weiteren Aktivitäten, vertieft dargestellt werden: Neben einem «Evergreen», Fragen zum Schutz am Arbeitsplatz, ging es beispielsweise um die Einrichtung einer Videoattrappe durch eine Behörde zu präventiven Zwecken, um Abklärungen einer Behörde zu persönlichen Befähigungen zur Berufsausübung mit Hilfe des Internets, um die sichere Kommunikation bei einer Onlinebestellung, um den Schutz der Persönlichkeit nach dem Tod, oder um den Einsatz von Detektiven.

Erfreulicherweise war auch ein starker Anstieg bei den Zugriffen auf unsere Internetseite festzustellen. Auf dieser Plattform informieren wir über alle wichtigen Themen rund um den Datenschutz, wie z.B. über einen Bericht zum Datenschutz bei sozialen Netzwerkdiensten.

Aus dem internationalen Bereich sind zwei wichtige Dokumente nennenswert: Einerseits geht es um den Schutz der Privatsphäre von Kindern vor allem im Schulbereich und andererseits um die international geführte Diskussion der Anforderungen des Datenschutzes an Suchmaschinen im Internet.

Schliesslich ist auch die Idee der Schaffung eines «Datenstandorts Liechtenstein» interessant, welche aufgegriffen werden könnte.

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

Durch die im letzten Jahr beschlossene Neuorganisation und den im Zusammenhang mit dem Schengenbeitritt beschlossenen Ausbau des Personalstands der Datenschutzstelle hat sich sehr viel geändert. Eine dieser Änderungen betrifft auch den Aufbau dieses Tätigkeitsberichts, der neu gegliedert wurde. Ich wünsche Ihnen eine anregende Lektüre.

Vaduz, im Juli 2009

Dr. Philipp Mittelberger
Datenschutzbeauftragter

2. Datenschutz allgemein

2.1. ALLGEMEINE DATENSCHUTZRECHTLICHE FRAGEN

Datenschutz ist ein Ausfluss der von der Verfassung geschützten Privatsphäre. In einer etwas anderen Form ist er auch beim Persönlichkeitsschutz zu berücksichtigen. Wenn manchmal behauptet wird, dass sich mit Inkrafttreten des DSG einiges geändert hat, muss hierzu relativierend gesagt werden, dass es nicht nur um Datenschutz im Sinne des Datenschutzgesetzes (DSG) geht, sondern vielmehr auch um Persönlichkeitsschutz, der im Personen- und Gesellschaftsrecht geregelt ist.

Ein gutes Beispiel in diesem Zusammenhang ist die Frage, ob der **Schutz personenbezogener Informationen** auch noch **nach dem Tod** gültig ist. Um diesen Schutz geht es z.B. im Zusammenhang mit der Publikation des Namenbuchs des Historischen Vereins, bei einer Bekanntgabe von Daten durch das Landesarchiv zu Forschungszwecken oder etwa im Fall einer im Landesspital verstorbenen Person. Grundsätzlich werden nur lebende Personen vom DSG geschützt. Das liechtensteinische Datenschutzrecht kennt keinen so genannten *postmortalen Persönlichkeitsschutz*. Eine verstorbene Person besitzt folglich keine Rechtsfähigkeit mehr.[1]

Dieser Grundsatz wird jedoch in einigen wenigen *Ausnahmen* durchbrochen: Zum Beispiel wirkt die *berufliche Schweigepflicht über den Tod der betroffenen Person hinaus.*[2] Ist eine Person im Spital verstorben, darf das Spital keine Daten der verstorbenen Person bekannt geben. Konfrontiert mit der Frage, ob das Landesspital Daten beispielsweise an die Tochter einer verstorbenen Person bekannt geben darf, muss unterschieden werden: Geht es darum, dass sich eine rechtliche Auseinandersetzung anbahnt, ist das persönliche Interesse der anfragenden Person wohl zu bejahen. Ist zu befürchten, dass die anfragende Person selbst einen gesundheitlichen Schaden nehmen kann (z.B. genetische Krankheit), sollte ein Arzt diese Auskunft geben.[3] In diesen speziellen Fällen geht es darum, dass es sich um die Geltendmachung von *eigenen Datenschutzrechten der Nachkommen* handelt, die vom Recht des Verstorbenen auf informationelle Selbstbestimmung zu unterscheiden ist. In gewissen Zusammenhängen kann auch von Nachwirkungen der Persönlichkeit des Verstorbenen gesprochen werden.

Der **Geschichtsschreibung** kommt beispielsweise ein erhebliches öffentliches Interesse zu. Der Anspruch der Allgemeinheit, das in der Vergangenheit Geschehene für die Zukunft wahrheitsgetreu zu dokumentieren, dürfte in der Regel die Persönlichkeitsrechte der jeweils Betroffenen überwiegen. Nichtsdestotrotz müssen zur Erreichung dieses Ziels nicht immer alle Namen von Personen konkret erwähnt werden. Die Nennung aller Beteiligter ist nicht durchwegs von grossem öffentlichen Interesse. Zusammen mit dem Landesarchiv wurden daher diesbezüglich Kriterien aufgestellt, wann auf eine Namensbekanntgabe verzichtet werden kann. Dies soll vor allem dann der Fall sein, wenn es sich um Personen handelt, deren Handlungen nicht bedeutend waren und die mithin als «Statisten» eingestuft werden können.

Im Rahmen eines Gerichtsverfahrens zur Durchsetzung des Auskunftsrechts wurden wir um ein **Gutachten** *zur Auslegung der Begriffe der Datensammlung* und der *Ausnahme der Geltung des Gesetzes bei Personendaten,* welche auf Grund des *Sorgfaltspflichtgesetzes* anzulegen sind, ersucht. Weiters um Beantwortung der Frage, *in welcher Form eine Auskunft* zu erfolgen hat. Nach der gesetzlichen Definition ist eine Datensammlung «jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind».[4] Der liechtensteinische Gesetzgeber hat sich hierbei an der Vorgabe der Datenschutzrichtlinie orientiert, diese jedoch in Anlehnung an das Schweizer Datenschutzgesetz zu Gunsten der betroffenen Personen erweitert. Nach der Richtlinie kommt es für das Vorliegen einer Datensammlung auf die Zweckbestimmung bzw. Strukturierung der Elemente an. Auf diese Voraussetzungen stellt das Schweizer Datenschutzgesetz jedoch nicht entscheidend ab. Der Schutzbereich sollte daher bewusst weiter ausgedehnt werden, um zu verhindern, dass die Bestimmungen des DSG allein durch blosse ungeordnete oder verstreute Ablagen von Papierunterlagen unterlaufen werden kann.[5]

[1] Vgl. Art. 50 PGR.
[2] Vgl. Maurer-Lambrou/Vogt (Herausgeber), Basler Kommentar, Datenschutzgesetz, 2. Auflage, 2006, Urs Belser, Art. 3 Randnummer 9.
[3] Vgl. Art. 11 Abs. 3 DSG.
[4] Art. 3a Abs. 1 Buchstabe i DSG.
[5] So die Eidgenössische Datenschutzkommission in ihrer Entscheidung vom 21. November 1997, Nr. 04/97, E.5, Seite 5 ff., abzurufen unter *http://www.fir.unisg.ch/Datenschutz/pdf/9704_Urteil_vpb.pdf.*

Wie im Gutachten festgehalten, ist die *Auslegung des liechtensteinischen DSG* und damit auch die Auslegung des Begriffs der Datensammlung grundsätzlich an der *Schweizer Rezeptionsvorlage auszurichten.* Für das Vorliegen einer Datensammlung ist daher datenschutzrechtlich allein ausschlaggebend, dass die zu einer bestimmten Person gehörenden Daten auffindbar sind. Die Sammlung kann hingegen ganz unterschiedlich organisiert und aufgebaut sein.[6] Dies führt dazu, dass bloss ungeordnete oder verstreute Ablagen von Papierunterlagen nicht als Datensammlung angesehen werden können. So können beispielsweise auch interne Aufzeichnungen bzw. Aktenvermerke eine Datensammlung bilden oder ein Teil davon sein. Dies jedoch nur unter der Voraussetzung, dass sie sich nach Personen erschliessen lassen, was in jedem Einzelfall konkret zu entscheiden ist.

Zur Frage, ob das *DSG im Rahmen des Sorgfaltspflichtgesetzes (SPG)* anwendbar ist, kommt das Gutachten zum Schluss, dass der Vorbehalt von Art. 2 Abs. 3 Buchstabe g DSG[7] nur im ganz engen zeitlichen Rahmen des «Anlegens», im Sinne von «Beschaffen» zur Anwendung kommen kann. Umgekehrt bedeutet dies: Sobald Personendaten einmal angelegt sind und in Folge bearbeitet werden, fallen sie unter das DSG, selbst wenn sie im Zusammenhang mit dem SPG stehen.

Zu guter Letzt hatte sich das Gutachten damit auseinander zu setzen, *in welcher Form eine Auskunft* nach Art. 11 DSG zu erfolgen hat. Zur Form einer Auskunft schreibt das Gesetz vor, dass diese *«in der Regel schriftlich»* zu erfolgen hat.[8] Die Formulierung «in der Regel» ist als strenger Grundsatz auszulegen, von dem nur ausnahmsweise abgewichen werden darf. Eine schriftliche Auskunft darf nur dann durch eine Einsicht an Ort und Stelle oder mündliche Auskunft ersetzt werden, wenn die *betroffene Person dem ausdrücklich zustimmt.*[9] Dem Inhaber einer Datensammlung steht insofern kein Spielraum zu: Willigt die Auskunft begehrende Person nicht uneingeschränkt ein, hat die Auskunft schriftlich zu erfolgen. Für die Ausnahme von der Schriftlichkeit muss also eine wirksame Einwilligung durch die Auskunft begehrende Person vorliegen.

2.2. DATENBEKANNTGABE IM INLAND

Wie die Anfragenstatistik des Berichtsjahrs zeigt, waren wir mit dem Bereich Datenbekanntgabe im Inland häufig befasst.[10] Von zahlreichen Anfragen seien auszugsweise die Folgenden erwähnt:

Bei der Frage einer **regelmässigen Meldung der Adressenänderungen** der Gemeinden an die Post im jeweiligen Gemeindegebiet kommt es darauf an, ob sie der Erfüllung ihrer gesetzlichen *Aufgaben sach- und zweckdienlich* ist. Eine der gesetzlichen Hauptaufgaben der Post AG besteht in der korrekten Zustellung von Briefen.[11] Zur Wahrnehmung dieser Aufgabe ist es daher wichtig, dass die Post über die richtigen Adressen verfügt. Vor diesem Hintergrund kann daher davon ausgegangen werden, dass die *Einwilligung* der betroffenen Personen in die Bekanntgabe ihrer Adressenänderungen nach den Umständen *vorausgesetzt* werden darf.[12] Wichtig ist, dass die bekannt gegebenen Adressen nicht zweckentfremdet verwendet, wie z.B. verkauft, werden.

Eine Anfrage betraf die **Bekanntgabe von Schulnoten** innerhalb eines **Intranets**. Hierbei war die Einführung eines Systems angedacht, über welches nicht nur die jeweiligen Prüfungsteilnehmer Zugriff auf ihre eigenen Noten haben sollten, sondern alle Personen, die im System registriert sind. Bei der Einführung eines solchen Systems sind insbesondere der Grundsatz der *Verhältnismässigkeit* und die Frage nach dem *Zweck* zu berücksichtigen. Die Bekanntgabe von Schulnoten hat grundsätzlich und ausschliesslich an den betroffenen Schüler bzw. Prüfungsteilnehmer *persönlich* zu erfolgen. Als Ausnahme von diesem Grundsatz kann die Notenbekanntgabe an Erziehungsberechtigte von minderjährigen Schülern genannt werden.[13]

Im neu ausgestalteten Erhebungsbogen zur **Energiestatistik 2007** wurde auch nach den entsprechenden Namen der Lieferanten gefragt. Bei der datenschutzrechtlichen Beurteilung dieser Frage kam es entscheidend darauf an, ob die *Nennung* des Namens der Lieferanten für die Erstellung der Energiesta-

[6] Vgl. Botschaft des Bundesrates zum Schweizer Bundesgesetz über den Datenschutz vom 23. März 1988, Seite 447 ff.
[7] Art. 2 Abs. 3 Buchstabe g DSG besagt: «Dieses Gesetz findet keine Anwendung auf: Personendaten, welche aufgrund des Sorgfaltspflichtgesetzes anzulegen sind».
[8] Art. 11 Abs. 5 Satz 1 DSG in Verbindung mit Art. 1 Abs. 2 DSV.
[9] Vgl. BGE 123 II 534, E.3.c, Seite 541.
[10] Vgl. Anhang, 13.1.
[11] Vgl. Art. 6 der Postverordnung.
[12] Vgl. Art. 23 Abs. 1 Buchstabe b DSG.
[13] In diesem Zusammenhang sei auch auf die Stellungnahme der Art. 29 Datenschutzgruppe hingewiesen, die sich eingehend mit dem Umgang von Personendaten von Minderjährigen befasst, unter anderem auch mit der Bekanntgabe von Schulnoten. Vgl. 10.2.1.

tistik *erforderlich* ist. Liegt ein *berechtigtes Interesse* vor, ist zu prüfen, ob dieses höher zu bewerten ist als das Interesse des Auskunftspflichtigen. Zu berücksichtigen ist hierbei insbesondere, dass die Daten bei der Erstellung von Statistiken *absolut vertraulich* zu behandeln sind.[14] Ausserdem dürfen die Daten nur in *anonymisierter Form* veröffentlicht werden.

Auf eine *Anonymisierung* kommt es auch bei einer **Datenbank gerichtlicher Entscheidungen** an, welche teils veröffentlichte, teils unveröffentlichte Entscheidungen enthält. Zunächst wurden die Entscheidungen zwar in bereinigter Form wiedergegeben, eine vollständige Anonymisierung fand jedoch nicht statt. So sind in den Entscheidungen nicht nur Namen der Parteien und Rechtsvertreter enthalten, sondern im Rahmen der Entscheidungsgründe lassen sich teilweise auch Angaben zum Gesundheitszustand einer Partei oder gar Persönlichkeitsprofile finden. Damit enthält die Datenbank *besonders schützenswerte Daten gemäss DSG.*[15] Dies bedeutet, dass die Datenbank eine *ausdrückliche gesetzliche Grundlage benötigt,*[16] sofern keine *Anonymisierung* erfolgt.

Ob Gemeinden die **Namen und Adressen der über 65-jährigen Gemeindeeinwohner** bekannt geben dürfen, um so gezielt an diese Interessengemeinschaft eine Zeitschrift kostenlos versenden zu können, hängt von den *Zielen* des Herausgebers ab. Erfolgt eine Bekanntgabe von Personendaten zu überwiegend *ideellen* Zwecken, steht ihr aus datenschutzrechtlicher Sicht nichts entgegen. Anders verhält es sich hingegen, wenn der Herausgeber überwiegend kommerzielle Ziele damit verfolgt.

Weiterhin hatten wir uns mit der geplanten **Veröffentlichung des Namenbuchs** zu befassen. Die noch aus dem Jahr 2007 stammenden Beschwerden[17] hierzu konnten erfolgreich abgeschlossen werden.

2.3. DATENBEKANNTGABE MIT AUSLANDSBEZUG

Viele Anfragen, insbesondere von privaten Unternehmen, betrafen die Frage der **Meldepflicht von Datentransfers ins Ausland.**[18] Deshalb soll an dieser Stelle etwas vertieft darauf eingegangen werden: Geht es um eine Datenbekanntgabe in ein Land, in dem ein *gleichwertiger Datenschutz gewährleistet* wird, sind *keine besonderen Vorkehrungen* zu treffen. Einen gleichwertigen Datenschutz gewährleisten alle EU-/EWR-Staaten sowie die im Anhang zur Datenschutzverordnung (DSV) aufgelisteten Länder, wie beispielsweise die Schweiz.

Bei einem Datentransfer in *Drittländer ohne gleichwertigen Datenschutz* sieht das Gesetz in *bestimmten Fällen eine Meldepflicht* an uns vor. Eine Meldepflicht besteht dann nicht, wenn die betroffene Person im Vorfeld über den Datentransfer ins Ausland *hinreichend informiert* wurde. Eine Meldepflicht entfällt weiters, wenn ein Gesetz die entsprechende Datenbekanntgabe explizit vorsieht. Das Zusammenspiel von DSG und DSV[19] ist in diesem Zusammenhang sehr komplex. Häufige Fragen betrafen eine allfällige Meldepflicht bei Kenntnis der betroffenen Personen von der Datenbekanntgabe im Allgemeinen und bei Kenntnis der betroffenen Personen von der Bekanntgabe besonders schützenswerter Daten im Besonderen. Solche Fallkonstellationen sind beispielsweise bei Lebensversicherungen oder Krankenkassen denkbar. Festzuhalten bleibt im Ergebnis hierzu, dass die Kenntnis der betroffenen Person einer Meldepflicht grundsätzlich vorgeht.

Bei international tätigen Konzernen ist ein Datentransfer ins Ausland an der Tagesordnung. Personendaten werden oft innerhalb des Konzerns zwischen den einzelnen nationalen Unternehmenszweigen ausgetauscht, wie beispielsweise die Mitarbeiterdaten einer Konzernzentrale in Liechtenstein mit einer Tochtergesellschaft in China. Sollen hierbei Personendaten (auch) in Drittländer bekannt gegeben werden, stellen die so genannten **verbindlichen unternehmensinternen Datenschutzregelungen** (Binding Corporate Rules, BCR) eine geeignete Lösung dar.[20] Diese sollen grenzüberschreitend einen gleichwertigen Datenschutz innerhalb des Konzerns gewährleisten. Geht es hingegen um einen Datentransfer zwischen zwei getrennten Unternehmen, von denen sich eines in einem so genannten Drittstaat befindet, können die *Standardvertragsklauseln (Contractual Clauses)* der Europäischen Kom-

[14] Vgl. Art. 16 Statistikgesetz.
[15] Vgl. Art. 3 Abs. 1 Buchstabe e und f DSG.
[16] Vgl. Art. 21 Abs. 1 DSG in Verbindung mit Art. 23 Abs. 1 DSG.
[17] Vgl. Tätigkeitsbericht 2007, 5.2.
[18] Vgl. Art. 8 DSG a. F.
[19] Art. 6 und 8 DSV a. F.
[20] Das Regelwerk zu den BCR wurde im Berichtsjahr von der Art. 29 Datenschutzgruppe ständig ausgebaut und aktualisiert. Vgl. dazu ausführlich 10.2.1.

mission herangezogen werden. Im Berichtsjahr wurde eine steigende Zahl von Anfragen von Unternehmen aus der Privatwirtschaft zu diesem Fragenkomplex festgestellt.

Eine ausländische Firma bot sich an, ausstehende **Geldbussen** nach der *Strassenverkehrsordnung* im Ausland einzutreiben. Dies würde jedoch voraussetzen, dass die entsprechenden Halterdaten dieser ausländischen Firma zuvor bekannt gegeben werden müssten. Bei dieser Konstellation würde es sich also um einen klassischen Fall des Outsourcings ins Ausland handeln. Voraussetzung für einen rechtmässigen Datentransfer wäre demnach ein Vertrag, der die besonderen datenschutzrechtlichen Rahmenbedingungen in Bezug auf einen Transfer ins Ausland zu berücksichtigen hätte.

Nicht nur im Gesundheitsbereich ist es inzwischen durchaus üblich, dass z.B. der behandelnde Arzt die Abrechnungen nicht mehr selbst in seiner Praxis vornimmt, sondern dafür ein (IT-)Unternehmen beauftragt. In Liechtenstein werden hierfür häufig Unternehmen in der Schweiz beauftragt, so dass zusätzlich die Voraussetzungen für einen Datentransfer ins Ausland zu berücksichtigen sind. In diesem Fall handelt es sich um eine **Datenverarbeitung im Auftrag**, für die die besonderen Anforderungen nach Art. 19 DSG zu beachten sind. Danach bleibt die Auftrag erteilende Stelle datenschutzrechtlich weiterhin verantwortlich für die Datenbearbeitung. Der Auftragnehmer befindet sich dagegen in einer Doppelfunktion. Einerseits wird er im Rahmen des Auftragverhältnisses selbst zu einer Daten bearbeitenden Stelle, andererseits kann er bezüglich der Bearbeitung der ihm übermittelten Daten keine eigenständigen Entscheidungsbefugnisse ableiten. Insoweit bleibt er an die vom Auftraggeber erteilten Weisungen gebunden. Bei der Bearbeitung hat er dieselben Sorgfaltspflichten einzuhalten wie der Auftraggeber.

Zur Frage, ob ein **Arzt** seine Daten zur Abrechnung an ein **Unternehmen im Ausland** weiter leiten darf, kann Folgendes angemerkt werden: Zur *Abrechnung von Arztleistungen* werden in der Regel auch die zu Grunde liegenden Gesundheitsdaten weitergeleitet. Die Datenbearbeitung durch Dritte ist daher nur zulässig, wenn dies *gesetzlich vorgesehen* ist, oder der Patient *vorher darauf hingewiesen* wurde und er seine entsprechende *Einwilligung ausdrücklich erklärt* hat. Mit einer Einverständniserklärung kann auch die Kenntnis des Betroffenen vorausgesetzt werden, die eine Meldepflicht des Datentransfers an uns ersetzt. Ausserdem muss der Auftrag erteilende Arzt dafür sorgen, dass die Daten nur so bearbeitet werden, wie er es selbst tun dürfte. Er hat also dafür Sorge zu tragen, dass das *Arztgeheimnis entsprechend respektiert* wird.[21] Gesetzliche oder einzelvertragliche Geheimhaltungspflichten können im einzelnen Fall ein solches Outsourcing verbieten.

Eine Frage betraf die Zulässigkeit der *Speicherung von Daten im Ausland,* welche von einer liechtensteinischen Gesellschaft verwaltet wurden, allein für den Zweck, bei einer **Katastrophe** das Geschäft möglichst reibungslos weiter betreiben zu können.[22] Auch hier richtet sich die Zulässigkeit insbesondere danach, ob im betreffenden Ausland ein *gleichwertiger Datenschutz gewährleistet* wird und ob auf Seiten der betroffenen Person Kenntnis darüber gegeben ist.

In einer anderen Anfrage aus dem Ausland ging es darum, wie lange ins Ausland weitergeleitete Daten aufbewahrt werden dürfen. Die zulässigen **Aufbewahrungsfristen** sind zum Teil in Spezialgesetzen geregelt. Medizinische Unterlagen beispielsweise müssen zehn Jahre lang aufbewahrt werden.[23] Im *DSG* selbst wird *keine Speicherdauer* beziffert. Hier gilt der allgemeine Grundsatz, dass Personendaten zu löschen oder zu vernichten sind, wenn der Zweck, zu dem sie bearbeitet wurden, erfüllt ist.

2.4. GELTENDMACHUNG GESETZLICHER RECHTE

Im Rahmen eines *Rechtsfürsorgeverfahrens* vor dem Landgericht wurden wir erstmals hinsichtlich einer **Auskunftsklage** für die Erstellung eines **Rechtsgutachtens** angefragt.[24] Bei diesem Verfahren ging es unter anderem darum, ob das Auskunftsrecht auch *interne Aktennotizen* umfassen kann. Dies ist unserer Ansicht nach unter bestimmten Voraussetzungen zu bejahen. Nämlich dann, wenn es um Angaben geht, welche sich auf eine identifizierte oder identifizierbare Person bezie-

[21] Vgl. Leitfaden für die Bearbeitung von Personendaten im medizinischen Bereich des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), S. 25 ff. *http://www.edoeb.admin.ch/dokumentation/00445/00472/00920/index.html?lang=de.*
[22] So genanntes Business Continuity Management (BCM).
[23] Vgl. Art. 14 Ärztegesetz.
[24] Vgl. 2.1.

hen und es sich nicht um rein persönliche Bemerkungen handelt.[25]

Erstmals seit Einführung eines **indirekten Auskunftsrechts** nach Art. 34 h Polizeigesetz (PolG) im vergangenen Jahr[26] hatten wir ein entsprechendes Gesuch zu bearbeiten. Konkret war zu überprüfen, ob Personendaten der Antragsteller im Zusammenhang mit dem Staatsschutz oder mit Ermittlungen zur vorbeugenden Bekämpfung von Straftaten von der Landespolizei bearbeitet werden und ob die Bearbeitung rechtmässig erfolgt.[27] Im Zuge der Überprüfung war es möglich, die bis dahin noch offenen (Verfahrens-)Fragen zu klären.

Wie schon 2007 betrafen einige Beschwerden auch den Erhalt von **unerwünschter Werbung**. Auffällig war in diesem Kontext, dass der Absender der Werbung oftmals aus dem Ausland kam. Um diesen Beschwerden erfolgreich nachgehen zu können, ist es wichtig zu wissen, woher die jeweiligen Werbefirmen die Namen und Adressen der in Liechtenstein wohnenden Personen erhalten haben. Die Herkunft der Daten kann allerdings nur mittels eines Auskunftsbegehrens herausgefunden werden, welches die Adressaten der Werbesendung persönlich stellen müssen.[28] Wir haben insofern kein eigenes Auskunftsrecht und sind auf die Mitwirkung der Betroffenen angewiesen. Erst wenn die Auskunft nicht vollständig oder nur unvollständig erteilt wird, können wir von uns aus eingreifen, sofern der Absender in Liechtenstein angesiedelt ist. Unter Berücksichtigung dieser Rechtslage können wir also in vielen Fällen nicht weiter tätig werden, wenn die betroffenen Personen ihr Auskunftsrecht selbst nicht wahrnehmen wollen.

Zur Form der Auskunft im Rahmen eines Auskunftsbegehrens verweisen wir auf unser Rechtsgutachten.[29]

[25] Vgl. Entscheidung zwischen Datenschutzkommission (EDSK) vom 21. November 1997, Nr. 04/97, E.5, Seite 5 ff. und vom 18. November 2005, 06/04 E.5.
[26] Vgl. hierzu die Ausführungen zur Abänderung des PolG im Tätigkeitsbericht 2007, 4.4.
[27] Art. 34h Abs. 1 PolG besagt: «Jede Person kann bei der Datenschutzstelle verlangen, dass diese prüfe, ob bei der Landespolizei rechtmässig Daten im Rahmen des Staatsschutzes (Art. 2 Abs. 2) oder zur vorbeugenden Bekämpfung von Straftaten (Art. 2 Abs. 1 Bst. d) über sie bearbeitet werden. Die Datenschutzstelle teilt der Gesuch stellenden Person in einer stets gleich lautenden Antwort mit, dass in Bezug auf sie entweder keine Daten unrechtmässig bearbeitet werden oder dass sie bei Vorhandensein allfälliger Fehler in der Datenbearbeitung eine Empfehlung zu deren Behebung verfügt habe».
[28] Vgl. Art. 11 DSG. Musterschreiben zum Auskunftsbegehren sind abzurufen unter: *http://www.llv.li/form-llv-sds-musterschreiben.htm.*
[29] Vgl. 2.1.

3. Technologischer Datenschutz

3.1. PROJEKTE

Wie im letzten Tätigkeitsbericht erwähnt,[30] gab die Regierung ein Rechtsgutachten zur Beschaffenheit der **zentralen Personenverwaltung** (ZPV) in Auftrag. Dieses Gutachten bestätigt die Anliegen des Datenschutzes. Neben der dringenden Empfehlung zur Schaffung einer gesetzlichen Grundlage[31] werden sechs zentrale Punkte angesprochen:

1. Der *Zugriff auf Vergangenheitsdaten ist einzuschränken:* In der ZPV findet bis zum jetzigen Zeitpunkt keine Datenbereinigung und somit eine Speicherung der Daten ohne zeitliche Beschränkung statt. Das Gutachten empfiehlt, eine entsprechende Einschränkung umzusetzen, welche den Zugriff auf historische und somit nicht mehr notwendige Daten unterbindet.
2. Die *Verhältnismässigkeit* der Datenbearbeitung ist herzustellen: Das System lässt in der derzeitigen Implementierung keine Trennung zwischen globalen und amtsinternen Datenbeständen zu. Das Gutachten empfiehlt die Einrichtung eines Mechanismus, der einem Sachbearbeiter lediglich die für dessen Tätigkeit erforderlichen Tatenbestände und Informationen bereitstellt.
3. Das *gesetzlich vorgesehene Sperrecht:* Die ZPV lässt derzeit keine Möglichkeit zu, einen Datensatz einer Person mit einem im DSG vorgesehenen Sperrhinweis zu markieren.
4. *Löschung von Datensätzen:* Wie bereits bei den Vergangenheitsdaten erwähnt, sieht der derzeitige Aufbau der ZPV keine Löschung vor. Das Gutachten empfiehlt, eine entsprechende Funktionalität zu implementieren.
5. *Installation einer Leseprotokollierung:* Zur Vorbeugung von Missbrauch und zwecks Nachvollziehbarkeit der Lesezugriffe sind Abfragen in der ZPV zu protokollieren. Eine solche Protokollierung wurde bis zu diesem Zeitpunkt nur eingeschränkt umgesetzt. Es wird im Gutachten empfohlen, die bestehende Protokollierung jedenfalls zu erweitern.
6. *Testdaten* sind zu *anonymisieren:* Datenbestände zu Test- und Schulungszwecken sind jedenfalls vor deren Nutzung zu anonymisieren.

Eine verwaltungsinterne Arbeitsgruppe wurde damit beauftragt, für die im gegenständlichen Gutachten angesprochenen Empfehlungen Entwürfe und Umsetzungsvorschläge auszuarbeiten und der Regierung vorzulegen.

Die so genannte **Personenidentifikationsnummer** (PEID) stellt ein wichtiges Element der ZPV dar und wird mittlerweile auch als neue AHV-Nummer verwendet.[32] Grundsätzlich ist aus Datenschutzsicht nichts gegen eine Verwendung einer nationalen Kennnummer einzuwenden. Im Gegenteil: Die Datenschutzrichtlinie überlässt die Bestimmung der Bedingungen, nach denen eine nationale Kennziffer oder andere Kennzeichen allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen, den Mitgliedstaaten.[33]

Da in Liechtenstein Personen mit demselben Namen häufig doppelt, oder gar mehrfach, vorkommen, kann eine solche Nummer sogar von grossem Vorteil sein. Nichtsdestotrotz sind auch die Risiken zu sehen, da Daten unter Umständen nicht zweckbestimmt bearbeitet werden. Zudem stellt sich die Frage der *Verhältnismässigkeit*. Dazu kommt, dass diese Nummer in Liechtenstein eben nicht nur durch die Landesverwaltung, sondern auch durch die AHV (Alters- und Hinterlassenenversicherung) verwendet wird, während in anderen Ländern differenzierte Lösungen bestehen. So kennt *Österreich* das Modell der so genannten *bereichsspezifischen Personenkennzeichen.*[34] Das erwähnte *Rechtsgutachten* zur ZPV schlägt vor, sich am *österreichischen Ansatz* zu orientieren.

Auch in der Schweiz ist die Verwendung der Nummer gesetzlich geregelt.[35] In Frankreich wiederum wurde die Verwendung der Sozialversicherungsnummer für Bereiche ausserhalb des

[30] Vgl. Tätigkeitsbericht 2007, 5.1.1.1.
[31] Vgl. Tätigkeitsbericht 2003, 4.1.2.
[32] Vgl. Tätigkeitsbericht 2007, 5.1.2.
[33] Vgl. Art 8 Abs. 7 RL 95/46/EG.
[34] Bei diesem Modell werden Zahlen zur Identifikation durch Ableitung aus einer eindeutigen Stammzahl der betroffenen Person gebildet. Für die Berechnung dieser eindeutigen Stammzahl von natürlichen und juristischen Personen dient bei meldepflichtigen Personen die Zahl der Eintragung im Zentralen Melderegister, während für alle anderen Personen die Zahl der Eintragung im Ergänzungsregister herangezogen wird. Von der abgeleiteten Zahl kann in weiterer Folge nicht mehr auf die Stammzahl zurückgerechnet werden. Durch diese Vorgehensweise wird verhindert, dass über verschiedene bereichsspezifische Personenkennzeichen eine Verbindung über Bereichsgrenzen hinweg zu ein und derselben natürlichen oder juristischen Person hergestellt werden kann. *http://reference.e-government.gv.at/uploads/media/Stammzahl-bPK-Algorithmen-1_1_1-20070131.pdf.*
[35] Vgl. Art. 50c ff. des Bundesgesetzes über die Alters- und Hinterlassenenversicherung und Art. 13 ff. des Registerharmonisierungsgesetzes.

Sozial- und Gesundheitsbereichs untersagt.[36] Einige Länder kennen gar keine nationale Kennnummer.

Die PEID ist in der Landesverwaltung ein wichtiges Arbeitsinstrument, das nicht grundsätzlich in Frage gestellt werden soll. Doch beim gegenwärtigen Zustand ist festzustellen, dass es für die PEID keine gesetzliche Grundlage gibt, die eine klare Verwendung regeln würde, wie dies z.B. in Frankreich, der Schweiz oder Österreich der Fall ist. Sie wird beispielsweise auch von den Gemeinden verwendet, ohne dass diese mit der ZPV arbeiten. Es stellt sich daher die Frage, ob diese Verwendung überhaupt nötig ist. Zusätzlich zu einer gesetzlichen Regelung sind Massnahmen technischer Natur denkbar, um die Verwendung der Nummer zu kontrollieren.[37]

Im Rahmen des Vorprojektes **«Enterprise Content Management»** (ECM) erfolgte keine nennenswerte Tätigkeit. Dieses Vorprojekt bezweckt die Einführung eines Dokumentenmanagementsystems in der Landesverwaltung.[38]

3.2. REGISTER DER DATENSAMMLUNGEN

Die Überlegungen zur Vereinfachung der Führung des Registers der Datensammlungen konnten konkretisiert und teilweise umgesetzt werden. Auf der Internetseite sind neue Formulare verfügbar.[39]

[36] *http://www.cnil.fr/la-cnil/actu-cnil/article/article//la-cnil-refuse-lutilisation-du-numero-de-securite-sociale-nir-par-des-organismes-de-recouvreme/.*
[37] Vgl. dazu den Tätigkeitsbericht 2008 der nationalen Kommission für den Datenschutz aus Luxemburg, S. 21 ff.: *http://www.cnpd.lu/objets/publications/rapports/rapport_activite_2008.pdf.*
[38] Vgl. Tätigkeitsbericht 2005, 4.5.
[39] *http://www.llv.li/form-llv-dss-dss_dsg_dsv.htm.*

4. Telekommunikation

Ein wichtiges Thema im Telekommunikationsbereich betraf die in Europa umstrittene **Vorratsdatenspeicherung** sämtlicher Verkehrsdaten aller Teilnehmer. Dabei geht es um die Speicherung sämtlicher Verkehrsdaten *(«wer, wann, mit wem»)* auf Vorrat. Neben hohen Kosten für die Datenspeicherung wäre damit auch ein Paradigmenwechsel im Strafrecht verbunden, der zu einem Generalverdacht – auch gegenüber Unschuldigen – führt.[40]

Die Vorratsdatenspeicherung wurde in Liechtenstein *bereits weitgehend eingeführt*.[41] Während nach der Richtlinie Daten nur zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zu bearbeiten sind, ist die Zweckbestimmung in der liechtensteinischen Regelung nicht so genau. Auf Grund der Anfrage eines betroffenen Unternehmens gaben wir zu diesem Zweck ein Rechtsgutachten mit folgender Frage in Auftrag: «Sind die staatlichen Massnahmen des Kommunikationsgesetzes und der Verordnung über elektronische Kommunikationsnetze und Dienste (VKND) zur Bearbeitung von Daten mit der liechtensteinischen Landesverfassung und dem DSG vereinbar?»

Das Rechtsgutachten lag zwar zum Ende des Berichtsjahres noch nicht in seiner offiziellen Fassung vor. Dennoch kristallisierten sich bereits im Vorfeld folgende Schlussfolgerungen heraus: Ein zentrales grundrechtliches Problem im Zusammenhang mit der Telekommunikationsüberwachung ist der *Schutz von Zeugnisverweigerungsrechten.*[42] Ausserdem wird die *voraussetzungslose* Vorratsdatenspeicherung als *verfassungsrechtlich* problematisch angesehen. Eine endgültige rechtliche Beurteilung wird jedoch von den noch ausstehenden Entscheidungen der einschlägigen ausländischen Grundrechtsprechung abhängig gemacht. Wir waren bezüglich der Problematik Vorratsdatenspeicherung auch in Kontakt mit der zuständigen Aufsichtsbehörde, dem Amt für Kommunikation (AK). Interessant in diesem Zusammenhang ist der Umstand, dass wir vereinzelt von deutschen Unternehmen angefragt wurden, die sich nach alternativen Datenstandorten erkundigten. Allgemein gesprochen könnte die Idee eines Unternehmens *«Liechtenstein als Datenstandort»* untersucht werden, da dies möglicherweise wirtschaftlich interessant und gewiss datenschutzfreundlich ist.

Auf Anfrage des AK erfolgte zudem eine **Überprüfung der Datenschutzbestimmungen** neuer Allgemeiner Geschäftsbedingungen (AGB) von liechtensteinischen Telekommunikationsanbietern. Eine solche Zusammenarbeit ist zu begrüssen, da dadurch unser Wissen direkt einfliessen kann.

Wir wurden von einer Behörde angefragt, wie mit **verloren gegangenen Mobiltelefonen** umgegangen werden soll, die eine gewisse Zeit lang in einem Fundbüro aufbewahrt wurden. Oft werden Datenträger wieder in Stand gesetzt und im Secondhand-Business verkauft. Die Frage der *Löschung von Daten* auf diesen *Datenträgern* wird *oft vernachlässigt.* In diesem konkreten Fall entschied man sich dazu, die Mobiltelefone, und damit die sich auf den Mobiltelefonen befindlichen Daten, durch ein qualifiziertes Unternehmen vernichten zu lassen.

Eine Anfrage betraf die Beurteilung von **Botnetzen** aus datenschutzrechtlicher Sicht. Allgemein wird unter einem Botnetz die Vernetzung durch *Schadsoftware «infizierter» Computersysteme* verstanden. Die erwähnte Software zur Kontrolle und Fernsteuerung des betroffenen Computersystems wird dabei im Vorfeld ohne Kenntnis des Anwenders auf dessen Rechner installiert. Durch die Möglichkeit der gezielten und gleichzeitigen Kontrolle einer grossen Anzahl von infizierten Computern werden diese häufig für so genannte DDoS Angriffe[43] und andere kriminelle Handlungen sowie für die Verteilung von Spam[44] eingesetzt.

Über *«Hintertüren»* kann ein Angreifer auf lokal gespeicherte Daten *zugreifen*, wichtige persönliche Angaben wie Passwörter sowie andere vertrauliche Zugangsdaten *ausspähen* und in weiterer Folge an einen entfernten Computer *weiterleiten*. Laut Studie des European Network and Information Society Agency (ENISA) stellen Botnetze ein wachsendes Problem dar, das öffentliche Stellen, die Privatwirtschaft und auch die einzelnen

[40] Vgl. Tätigkeitsbericht 2005, 7.
[41] Vgl. Art. 52 Abs. 2 Kommunikationsgesetz (KomG).
[42] Diese gesetzlich normierten Zeugnisverweigerungsrechte dienen in der Regel der Durchsetzung von Berufsgeheimnissen. Bezüglich einer Vorratsdatenspeicherung ist in der liechtensteinischen Strafprozessordnung (StPO) jedoch nur die Verwertung von Inhaltsdaten betreffend Gespräche mit dem Verteidiger für unzulässig erklärt worden. Damit werden weder Verkehrsdaten noch die anderen Berufsgeheimnisträger, wie zum Beispiel Rechtsanwälte, Psychologen, etc., erfasst. Im Rechtsgutachten wird dieser ungenügende Schutz von Zeugnisverweigerungsrechten ausdrücklich gerügt.
[43] DDoS *(engl. Distributed Denial of Service)* bezeichnet einen verteilten Angriff durch mehrere Computer auf ein im selben Netzwerk (z.B. Internet) befindliches System. Ziel dieses Angriffs ist es, einen oder mehrere der laufenden Dienste (z.B. Web-Service) ausser Betrieb zu setzen oder zu blockieren. Der Angriff wird meist automatisiert durchgeführt.
[44] Als Spam werden Nachrichten bezeichnet, die dem Empfänger unverlangt und zumeist unerwünscht elektronisch übermittelt werden.

Benutzer mit verheerenden Konsequenzen eines Identitätsdiebstahls bedroht.[45]

Eine weitere Anfrage betraf die Beurteilung der **Internetseite «rottenneighbor.com»**. Auf der Internetseite können Kommentare und Bewertungen über Personen in Verbindung mit deren Wohnort abgegeben werden.[46] Zu jeder Bewertung kann zusätzlich ein Freitext eingegeben werden. Eine Identifizierung der betroffenen Person ist oft aufgrund des Namens und der Adresse leicht möglich. Dieser anonym nutzbare Dienst wird offensichtlich vorwiegend für die Denunzierung und Beleidigung von Personen genutzt. Dieser Zweck wird durch den Namen des Portals noch unterstrichen, der sich mit *«verkommene Nachbarn»* übersetzen lässt. Die Betroffenen haben kaum Einfluss auf die über sie abgegebenen Kommentare. Es besteht zwar die Möglichkeit, einen bestehenden Eintrag für eine Löschung zu kennzeichnen *(«flag for removal»)*, doch garantiert diese Markierung nicht, dass dieser Eintrag auch tatsächlich entfernt wird.[47] Neben moralischen Aspekten sind aber vor allem auch rechtliche zu bedenken.

Im Unterschied zu Internetportalen zur Beurteilung von Personen aufgrund ihrer beruflichen Tätigkeiten oder öffentlichen Funktion, wird der *Nachbar als Privatmensch* und somit in seinem *grundrechtlich geschützten inneren Lebensbereich bewertet.* Diese Bewertung ist subjektiv und somit weder objektiv mess- noch feststellbar. Da im gegenständlichen Fall die Meinungsäusserungsfreiheit wegen der Prangerwirkung hinter dem Recht auf informationelle Selbstbestimmung zurückstehen muss, wäre der Betrieb eines solchen Dienstes in Liechtenstein unzulässig. Da der Sitz der Internetseite jedoch in den Vereinigten Staaten von Amerika liegt, ist eine Durchsetzung der Rechte schwierig.

Bedenken im Zusammenhang mit der **sicheren Übertragung von Kreditkarteninformationen** beim Einkauf im Internet war Gegenstand einer weiteren Anfrage. Bei der in Liechtenstein ansässigen Firma war für den Kunden beim Einkauf im Internet nicht klar erkennbar, ob die übermittelten Informationen, wie insbesondere Kreditkartendaten, verschlüsselt übertragen werden. Ein Absatz in den AGB's erwähnte jedoch eine *sichere SSL*[48] *verschlüsselte Verbindung.* Nach Rückfrage beim betroffenen Plattformbetreiber konnte in Erfahrung gebracht werden, dass aufgrund von technischen Umstellungen die SSL Verschlüsselung vorübergehend durch eine alternative Verschlüsselung ersetzt worden war. Die Daten waren somit bei der Übertragung zu jeder Zeit vor unberechtigtem Zugriff *geschützt*, doch war dieser Schutz für den Kunden beim Einkauf nicht erkennbar. Zwischenzeitlich hat der Betreiber eine SSL basierende Lösung in Verwendung, wodurch die aktive Verschlüsselung nun auch für Kunden leicht erkennbar und überprüfbar ist.

Wie Datenschutz und **Internetsuchmaschinen** zusammen passen, damit hat sich die Art. 29 Datenschutzgruppe ausführlich auseinandergesetzt und ein entsprechendes Arbeitspapier herausgegeben.[49]

[45] *http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_botnets.pdf.* Als Beispiel für die rasche Ausbreitung von Schadsoftware in diesem Zusammenhang kann der im Oktober 2008 entdeckte Computerwurm «Conficker» genannt werden. Weltweit waren am Ende des Berichtsjahres mehr als 1 Million Rechner mit diesem Wurm infiziert. Obwohl bis zum Ende des Berichtsjahres die Absicht der Entwickler der Schadsoftware «Conficker» nicht geklärt werden konnte, zeigt unter anderem die Infektion zahlreicher Systeme in der Landesregierung sowie in Krankenhäusern von Kärnten (Österreich) und die Ausbreitung auf Computern der französischen Luftwaffe sowie der deutschen Bundeswehr sehr deutlich, dass Botnetze datenschutzrechtlich durchaus ein Problem darstellen können.

[46] Auf einer Karte, basierend auf Google-Maps, werden jene Stellen mit einem Haus-Symbol gekennzeichnet, wo bereits die zuvor erwähnten Kommentare durch Besucher der Internetseite abgegeben worden sind. Die Farbe des Symbols soll dabei zum Ausdruck bringen, ob der dortige Bewohner für einen «guten» (grünes Symbol) oder «schlechten» (rotes Symbol) Nachbarn gehalten wird.

[47] In den Nutzungsbedingungen der Betreiber findet sich dazu folgende Bemerkung: «[…] das Kennzeichnen von Inhalten (Anm. Kennzeichnung zur Löschung mittels «flag for removal») bedeutet nicht notwendigerweise, dass er von der Seite entfernt wird.» Gemäss den Nutzungsbedingungen sind Anmerkungen oder Kommentare, die andere Personen beleidigen, diese bedrohen oder dessen Rechte verletzen, nicht zulässig. Durch den Betreiber der Plattform erfolgt jedoch keine Kontrolle. Vielmehr wird durch die Nutzungsbedingungen der Eindruck erweckt, dass die Nutzer ausdrücklich zu anonymen Kommentaren eingeladen werden.

[48] SSL (Secure Sockets Layer) ist die Bezeichnung für ein hybrides Verschlüsselungsprotokoll zur Datenübertragung im Internet.

[49] Vgl. 10.2.1.

5. Gesundheit und Soziales

Die Projektbegleitung zum **Integrierten Case Management** (ICM) konnte am Anfang des Berichtsjahres *erfolgreich abgeschlossen* werden.[50] Beim ICM geht es um eine aktive Unterstützung eines längerfristig arbeitsunfähigen Arbeitnehmers durch einen bei den Krankenkassen angegliederten so genannten *Case Manager bei der Wiedereingliederung ins Arbeitsleben.* Nur mit dem *ausdrücklichen Einverständnis* des betroffenen Arbeitnehmers darf der Case Manager tätig werden. Er fungiert dabei als *Bindeglied* zwischen den Krankenkassen, dem Arbeitgeber, eventuell der Invalidenversicherung (IV), und dem Arbeitnehmer und dessen Familie. Im Rahmen der Fallbearbeitung müssen der Case Manager und die anderen Beteiligten naturgemäss Personendaten und umfassende Informationen über die Gesundheit des Arbeitnehmers bearbeiten. Zusammen mit uns wurden daher detaillierte Geheimhaltungs- und Datenschutzvereinbarungen erarbeitet. Sie zielen darauf ab, die Persönlichkeitsrechte des betroffenen Arbeitnehmers best möglichst zu achten und eine datenschutzrechtlich zulässige Bearbeitung der (besonders schützenswerten) Personendaten zu garantieren.

Im Zusammenhang mit der IV wurde bezüglich der **IV-internen Handhabung von Personendaten**, insbesondere von Gesundheitsdaten, genauer nachgefragt. Bekanntermassen sieht das Krankenversicherungsgesetz (KVG) vor, dass, auf Wunsch eines Patienten, seine Daten nur an den Vertrauensarzt einer Krankenkasse gelangen dürfen. Das Invalidenversicherungsgesetz (IVG) kennt demgegenüber keine solche Regelung, obwohl es im IV-Bereich ebenso um Gesundheitsdaten geht, die zudem auf Grund von Abklärungen zur *Invalidität besonders heikel* sind. In diesem Kontext wurde unter anderem der Frage nachgegangen, ob Ärzte, die für die IV tätig sind, mit dem *Vertrauensarzt nach dem Krankenversicherungsgesetz vergleichbar* sind.[51]

Im Gegensatz zum Vertrauensarzt nach KVG ist die Stelle eines Arztes des *Regionalen ärztlichen Dienstes* (RAD) *gesetzlich nicht definiert.* Die Hauptaufgabe eines RAD-Arztes liegt in der Beratung der IV in einzelnen Fällen, beispielsweise Empfehlungen in Abklärungsverfahren, Stellungnahmen zur Arbeitsfähigkeit oder Beratung der Mitarbeitenden. Trotz der Unterschiede zwischen IVG und KVG geht es in beiden Bereichen um sensible Gesundheitsdaten. Ja mehr noch: Angaben zur Invalidität einer Person können gewiss als heikler eingestuft werden als gewisse Behandlungen nach dem KVG. Somit stellt sich die Frage, wieso der Vertrauensarzt nur im KVG, nicht aber auch im IVG vorgesehen ist.

Wir waren auch intensiv mit der **Auslegung von Art. 19 Abs. 2 KVG**[52] beschäftigt. Bei der Frage, *wer an wen und in welchem Umfang* Daten in einer Zusammenfassung für jeden Leistungserbringer bekannt geben darf, ist zwischen der Publikation der Statistik und der Bekanntgabe von Personendaten zu unterscheiden. Eine Publikation der Statistik ist aus datenschutzrechtlicher Sicht unbedenklich. Eine Bekanntgabe von Personendaten, aus denen in der Regel Rückschlüsse auf den einzelnen Leistungserbringer möglich sind, ist hingegen nach KGV und DSG im jeweiligen Einzelfall zu beurteilen. Ausserdem sind an die Bearbeitung der Daten strenge Anforderungen zu stellen.

Das Teilprojekt **«Originalrechnung an den Patienten»** wurde, wie im letzten Tätigkeitsbericht beschrieben, von der Regierung gut geheissen.[53] Zur Umsetzung dieses Teilprojekts wurden Faltblätter erstellt, mit denen Patienten auf die Möglichkeit aufmerksam gemacht wurden, dass sie eine Kopie der Rechnung des Arztes an die Krankenkasse zu ihrer Information bestellen können. Anlass dieser Idee ist eine Schärfung des Kostenbewusstseins im Gesundheitswesen.

[50] Vgl. Tätigkeitsbericht 2007, 4.1. und 4.5.

[51] Vgl. hierzu Art. 20 und 20a Krankenversicherungsgesetz (KVG).

[52] Art. 19 Abs. 2 KVG bestimmt: «Die Kassen melden dem Kassenverband nach dessen Vorgaben für jedes Kalenderjahr die an die einzelnen Leistungserbringer erbrachten Kostenvergütungen in der Obligatorischen und der Freiwilligenversicherung für Krankenpflege. Der Kassenverband fasst diese Angaben zu einer Statistik der Behandlungskosten zusammen. Er achtet dabei auf eine möglichst hohe Vergleichbarkeit mit entsprechenden Statistiken im Ausland. Der Kassenverband fasst zusätzlich die Angaben der Kassen für jeden Leistungserbringer zusammen. Er überprüft gestützt darauf, ob die Leistungserbringer den Grundsatz von Abs. 1 beachtet haben oder ob die Voraussetzung für eine Rückforderung nach Abs. 2 erfüllt sind. Der Kassenverband stellt das Gesamtergebnis und die Zusammenfassung für jeden Leistungserbringer der Regierung zur Festlegung und Überprüfung der Kostenziele im Sinne von Art. 19b zur Verfügung.»

[53] Vgl. Tätigkeitsbericht 2007, 4.5.

6. Polizei und Sicherheit

Das 2007 vor der DSK angestrengte Verfahren zur **Videoüberwachung im Städtle Vaduz**[54] wurde mit einer Entscheidung rechtskräftig abgeschlossen. Das Verfahren war auf Grund einer voraus gegangenen Beschwerde angestrengt worden. Die DSK ist in ihrer Entscheidung *vollumfänglich* unserer vorangegangenen Empfehlung gefolgt. Demnach hat die Gemeinde Vaduz die Videoüberwachung im Städtle Vaduz auf ein *verhältnismässiges Mass zu reduzieren.*[55] Im Rahmen der Entscheidung der Datenschutzkommission (DSK) wurde neben der Verhältnismässigkeit auch das Fehlen einer hinreichend konkreten Gesetzesgrundlage für eine Videoüberwachung im öffentlichen Raum moniert. Dies wurde zum Anlass genommen, im Rahmen der zweiten Teilrevision des DSG eine Rechtsgrundlage für die Videoüberwachung zu schaffen. Diese Teilrevision tritt am 1. Juli 2009 in Kraft.[56]

In einer Anfrage ging es darum, unter welchen Bedingungen eine **Videoüberwachung** in einem **privaten Geschäft** möglich ist. Anlass der Überlegung zur Einführung einer Videoüberwachung war die Tatsache, dass es vermehrt zu Diebstählen gekommen ist. Ähnlich wie bei der Videoüberwachung bei Behörden wurde von uns darauf hingewiesen, dass der Schutz des Eigentums ein Rechtfertigungsgrund für eine solche Massnahme darstellen kann. Wie bei Behörden ist aber auch eine Videoüberwachung durch private Personen mit einem *gut sichtbaren Hinweisschild* über das Überwachungssystem zu informieren, sofern die Kamera nicht sichtbar ist. Die Datensicherheit ist jederzeit sicherzustellen. Die Kamera ist derart aufzustellen, dass nur die für den *verfolgten Zweck* notwendigen Bilder in ihrem Aufnahmefeld erscheinen. Zu beachten ist auch, dass die Daten nur dem verfolgten Zweck entsprechend bearbeitet werden und sobald als möglich zu löschen sind. *Webcams*[57] sind genau so wie Videokameras zu behandeln, soweit sie dieselben Funktionen ausüben können und demselben Zweck dienen sollen.

Eine Behörde erkundigte sich nach der Zulässigkeit der Installation einer **Kameraattrappe** zu präventiven Zwecken. Dadurch sollten Sachbeschädigungen vermieden werden. Allgemein muss sich eine Behörde an den Grundsatz von Treu und Glauben halten. Für eine betroffene Person macht es keinen Unterschied, ob sie tatsächlich gefilmt wird oder nicht. Sie geht jedenfalls davon aus, dass sie gefilmt wird. Kameraattrappen bewirken daher einen Eingriff in ihr Privatleben, massgebend ist der *Eindruck der Überwachung* auf die «gefilmte» Person.[58]

Im Rahmen der Zusammenarbeit mit der Landespolizei gaben wir zum **indirekten Auskunftsrecht**[59] eine Empfehlung zur Präzisierung von verschiedenen Datenbearbeitungen ab.

[54] Vgl. Tätigkeitsbericht 2007, 5.1.1.2.
[55] Vgl. dazu Anhang, 13.2. Die vollständige Entscheidung der DSK vom 07. April 2008, DSK 2007/1, ist abzurufen unter: *http://www.llv.li/entscheidung_der_datenschutzkommission_zur_videoueberwachung_in_der_fussgaengerzone_in__vaduz.pdf;* vgl. auch Dr. Philipp Mittelberger, Videoüberwachung im Lichte der Verfassung, in: digma September 2008, Heft 3, S. 140 ff., abzurufen unter: *http://www.llv.li/videoueberwachung_im_lichte_der_verfassung_von_dr._philipp_mittelberger.pdf.*
[56] Vgl. ausführlich hierzu 9.
[57] Bei einer Webcam überträgt eine Kamera deren Bilder direkt auf eine Internetseite.
[58] Vgl. ein Urteil des Obersten Gerichtshofs Österreichs: *http://www.dsk.gv.at/DocView.axd?CobId=31100.*
[59] Art. 34h Polizeigesetz (PolG). Vgl. 2.4.

7. Wirtschaft und Finanzen

Die neue Gewerbeverordnung sieht vor, dass der Geschäftsführer eines Unternehmens für das Gewerberegister nicht nur seinen Namen und Adresse angeben, sondern auch die tatsächliche Ausübung seiner Tätigkeit und deren Umfang nachweisen muss.[60] Als Nachweis der **tatsächlichen Ausübung der Geschäftsführertätigkeit** wurde die Vorlage des *Arbeitsvertrags* verlangt. Ein Arbeitsvertrag enthält jedoch auch Angaben, die für das Gewerberegister nicht unbedingt erforderlich sind, wie insbesondere Angaben zu Gehalt, Tätigkeit oder allfälliger Sondervereinbarungen. Wir konnten darauf *hinwirken,* dass auf die Vorlage eines Arbeitsvertrags als Nachweis der tatsächlichen Ausübung einer Geschäftsführertätigkeit *verzichtet* wird. Stattdessen genügt eine entsprechende *Bestätigung im Antragsformular.*

Eine Anfrage betraf den Einsatz **ausländischer Privatdetektive** in Liechtenstein. Versicherungsgesellschaften geben verdeckte Nachforschungen in Auftrag, um zu überprüfen, ob eine (Versicherungs-)Leistung zu Recht bezogen wird. Grundsätzlich dürfen im EWR und in der Schweiz zugelassene Privatdetektive unter bestimmten Voraussetzungen auch in Liechtenstein ihrer Tätigkeit nachgehen.[61] Das IVG ermöglicht zum Beispiel,[62] dass private Fachleute oder geeignete Dritte mit der Abklärung des Sachverhalts beauftragt werden dürfen. Es sieht zur Bekämpfung eines ungerechtfertigten Leistungsbezugs die Möglichkeit vor, Spezialisten, also auch Privatdetektive, beizuziehen. Inwieweit im Rahmen dieser Tätigkeit der Datenschutz und das Recht auf Privatsphäre der jeweils betroffenen Personen gewahrt bleiben, ist *fallbezogen* zu beurteilen. Jedoch ermöglicht das DSG bei Vorliegen ein entsprechendes Interesse eine Datenbearbeitung, und damit die Tätigkeit eines Detektivs.

Die Finanzmarktaufsicht (FMA) als zuständige Aufsichtsbehörde von Versicherungsunternehmen kann diese in bestimmten Fällen **vom Versicherungsgeheimnis entbinden**.[63] Davor ist jedoch Rücksprache mit der Stabsstelle für Datenschutz zu nehmen. Zur einheitlichen Handhabung solcher Fälle haben wir mit der FMA ein gemeinsames *Prozedere* ausgearbeitet. Eine Frage betraf beispielsweise die allfällige Befreiung eines Insolvenzverwalters als Stellvertreter des insolventen Versicherungsnehmers vom Versicherungsgeheimnis.

Die Regierung hat im Januar den Schlussbericht des Projekts **«Futuro»** zur Etablierung einer Vision für den Finanzplatz Liechtenstein angenommen. Berücksichtigt wurden dabei auch gesamtwirtschaftliche Bedürfnisse. In der Folge wurde die Arbeitsgruppe *«Privatsphäre and Asset Protection»* mit dem Auftrag eingesetzt, Massnahmen zur Sicherung der Privatsphäre auszuarbeiten. Wir konnten in dieser Arbeitsgruppe mitarbeiten.

«Datenschutzaspekte der europäischen Dienstleistungsrichtlinie» war das Thema einer durch die europäische Akademie für Informationsfreiheit und Datenschutz veranstalteten Konferenz. Die Konferenz verfolgte insgesamt das Anliegen, bei der Umsetzung der Dienstleistungsrichtlinie auf die Berücksichtigung des Datenschutzes hinzuwirken. Ein Schwerpunkt lag unter anderem auf der Ausgestaltung des so *genannten einheitlichen Ansprechpartners,* der in jedem Mitgliedstaat eingerichtet werden muss. Dieser muss nicht notwendigerweise eine physische Person sein. Bei der Erbringung einer Dienstleistung in einem anderen Vertragsstaat des EWR-Abkommens soll eine Ansprechperson die verwaltungsinterne Arbeit koordinieren. Der Dienstleister erspart sich dadurch den Gang zu verschiedenen Ämtern. Da im Rahmen der Koordination mitunter zentral sehr viele Personendaten bearbeitet werden, ist auch auf den Datenschutz zu achten.

[60] Art. 34 Abs. 2 Ziffer 8 Gewerbeverordnung (GewV).
[61] Art. 26 ff. Gewerbeverordnung (GewV).
[62] Art. 80 Invalidenversicherungsgesetz (IVG).
[63] Art. 44 Abs. 4 Versicherungsaufsichtsgesetz.

8. Arbeitsbereich

Die Anfrage einer Behörde betraf das Heranziehen von **Internetangaben** zur Beurteilung der persönlichen **Befähigung** für eine **Berufsqualifikation.** Bekanntlich konsultieren Unternehmen vor Bewerbungsgesprächen vermehrt das Internet, was nicht unproblematisch ist. Schliesslich werden die Inhalte des Internets von den Nutzern frei gestaltet. Im konkreten Fall stützte sich diese Behörde auf Angaben einer russischen Internetseite. Sofern eine Behörde (oder ein Unternehmen) solche Informationen überhaupt verwendet, sollte sie unbedingt darauf achten, dass es sich dabei um *nachweislich richtige Informationen* handelt. Nach dem *DSG haben Daten richtig* zu sein.[64]

Wiederholte Anfragen aus der Privatbranche zeigten den Bedarf an Information darüber, inwieweit ein **Arbeitgeber** den **E-Mail-Verkehr** sowie den **Internetzugang** seiner Mitarbeiter kontrollieren bzw. überwachen darf. Hierbei geht es insbesondere um die Frage, *ob und in welchem Umfang eine private Nutzung zulässig* ist. Diesbezüglich lassen sich verschiedene Geschäftspraktiken beobachten: Von einer unbeschränkten privaten Nutzung über das Verbot bestimmter Internetseiten oder einer zeitlichen Beschränkung bis hin zu einem absoluten Verbot jeglicher privater Nutzung ist alles denkbar.

Wichtig ist in allen Fällen jedoch: Die Arbeitnehmer *sollten* über ein *Nutzungsreglement* informiert werden, über ein allfälliges *Überwachungsreglement müssen* sie hingegen informiert werden.[65] In diesem Zusammenhang steht auch die Frage, wie *E-Mail und Internetzugang während einer unerwarteten Abwesenheit* eines Mitarbeiters zu regeln sind. Hier gilt Folgendes: Zunächst sollte ein Abwesenheitsassistent mit dem Hinweis erstellt werden, dass der betroffene Arbeitnehmer abwesend ist und dass die E-Mail zur Bearbeitung an eine bestimmte Person in Vertretung weitergeleitet wird. Zuvor sollte diese Abwesenheitsmitteilung an den abwesenden Arbeitnehmer zur Information weitergereicht worden sein. Der vom Betrieb benannte Vertreter darf E-Mails, die explizit als privat gekennzeichnet sind, jedoch nicht öffnen. Alle anderen E-Mails, die einen geschäftlichen Zusammenhang ausweisen, darf der Vertreter öffnen.

Um *die* **Zulässigkeit der Bekanntgabe von Namen** ging es in der Frage, ob ein *Busfahrer* während der Arbeitszeit zum *Tragen eines Namensschilds verpflichtet* werden kann. Grundsätzlich steht es dem Arbeitgeber im Rahmen seines Weisungsrechts[66] zu, auch Anordnungen bzgl. des betrieblichen Verhaltens der Arbeitnehmer zu treffen. Hierbei ist jedoch das Persönlichkeitsrecht des Arbeitnehmers zu respektieren. Dieses findet seinen besonderen Schutz in der umfassenden Fürsorgepflicht des Arbeitsgebers. Die Fürsorgepflicht wird weiter dahingehend konkretisiert, dass der Arbeitgeber Daten über den Arbeitnehmer u. a. nur dann bearbeiten darf, soweit sie zur Durchführung des Arbeitsvertrags erforderlich sind.[67] Das Persönlichkeitsrecht einschränkende Weisungen des Arbeitgebers sind danach nur gerechtfertigt, wenn sie zur Durchführung des Arbeitsvertrags und zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich sind.[68] Im konkreten Fall waren daher die verfassungsrechtlich geschützten Persönlichkeitsrechte der Arbeitnehmer gegen das Weisungsrecht des Arbeitgebers abzuwägen. Zu berücksichtigen war, dass Busfahrer, im Unterschied zu Personal von Restaurants oder anderer Dienstleistungsunternehmen, in der Regel keinen persönlichen Kontakt mit Kunden haben oder diese beraten.

Aus konkretem Anlass beschäftigten wir uns im Berichtsjahr mit grundsätzlichen Überlegungen zu einem **Meldesystem von Korruption** oder anderen Missständen im Arbeitsbereich. Ein solches Meldesystem kann in Verbindung mit einem effektiven System zum Informantenschutz als wirksame Massnahme zur Stärkung des Vertrauens führen. Im betroffenen Betrieb kann es durch Einführung eines *internen Rapportsystems* bzw. von *Hotlines* oder durch Einführung der *Stelle eines Ombudsmannes* geschaffen werden. In der Schweiz wird derzeit beispielsweise die Einführung eines gesetzlichen Schutzes bei internen Meldungen von Missständen am Arbeitsplatz diskutiert.[69] Zu diesem Thema hat sich auch die Art. 29 Datenschutzgruppe geäussert.[70]

[64] Vgl. Art. 7 DSG.
[65] Vgl. unsere Richtlinien über Internet- und Emailüberwachung am Arbeitsplatz für öffentliche Verwaltungen und Privatwirtschaft: *http://www.llv.li/r1ichtlinien_ueber_internet-_und_e-mail-ueberwachung_am_arbeitsplatz_fuer_oeffentliche_verwaltungen_und_privatwirtschaft.pdf.*
[66] Vgl. Art. 7 des Einzelarbeitsvertragsrechts nach § 1173a Allg. Bürgerliches Gesetzbuch (ABGB).
[67] Vgl. Art. 28a des Einzelarbeitsvertragsrechts nach § 1173a ABGB.
[68] Vgl. hierzu auch Gauch / Schmid, Kommentar zum Obligationenrecht, 3. Auflage, 2006, Art. 328, Randnummer 6 ff.
[69] Vgl. Teilrevision des Schweizer Obligationenrechts (Schutz bei Meldung von Missständen am Arbeitsplatz), Erläutender Bericht zum Vorentwurf des Bundesrats, abzurufen unter: *http://www.bj.admin.ch/etc/medialib/data/pressemitteilung/2008/pm_2008-12-05.Par.0001.File.tmp/vn-ber-d.pdf.*
[70] *http://www.llv.li/amtsstellen/llv-dss-spezialthemen/llv-dss-spezialthemen-finanzielles/llv-dss-spezialthemen-whistleblowing.htm.*

9. Gesetzesvorhaben

Insgesamt gaben wir zu **20 Vernehmlassungsverfahren** in verschiedenen Stadien des Gesetzgebungsverfahrens konkret eine Stellungnahme ab. Aufgrund besonderer datenschutzrechtlicher Relevanz sind hierbei die **zwei Teilrevisionen des DSG** und eine *Sammelvorlage* hervorzuheben, auf die im Folgenden näher eingegangen werden soll:

Die **erste Teilrevision** des DSG war in Zusammenhang eines zukünftigen Beitritts zu **Schengen** und **Dublin** zu sehen[71] und betraf die *Struktur und Organisation der Stabsstelle für Datenschutz* (SDS). Notwendig war sie aufgrund des Beitritts Liechtensteins zu den Abkommen von Schengen und Dublin geworden, in dessen Rahmen auch ein Fokus auf dem Datenschutz liegt. Bisher war die SDS in die Landesverwaltung eingebettet und administrativ dem Ressort Justiz zugeteilt. Demzufolge wurde sie eher als eine klassische Amtsstelle denn als eine unabhängige Institution wahrgenommen, obwohl die Unabhängigkeit gesetzlich vorgesehen war.[72] Die Einbettung in die Landesverwaltung birgt sicherlich viele Vorteile in sich, insbesondere im Hinblick auf die Infrastruktur. Unter Berücksichtigung der Datenschutzrichtlinie aber erfüllte die SDS damit nicht die Voraussetzungen an eine *«völlig unabhängige Kontrollstelle»*.[73] Diese völlige Unabhängigkeit bedeutet, dass die Institution des DSB *institutionell, personell und finanziell vollständig selbstständig* sein muss. Gleichzeitig war mit der Ausgliederung eine Namensänderung in *Datenschutzstelle* (DSS) verbunden.

Der *DSB* wird neu nicht mehr von der Regierung bestellt, sondern vom *Landtag gewählt.* Die DSS erhält auch ein eigenes *Beschwerderecht,* wenn die Datenschutzkommission nicht dem Antrag der DSS folgt. Diese bedeutenden Gesetzesänderungen treten mit 01. Januar 2009 in Kraft. Sie spielen auch für die *Evaluation* durch Datenschutzexperten aus Schengen-Ländern im Vorfeld des Schengenbeitritts eine bedeutende Rolle.[74]

In einer **zweiten Teilrevision** ging es im Wesentlichen um eine bessere Umsetzung der **Datenschutzrichtlinie**, der Bestimmungen des **Zusatzprotokolls zum Datenschutzabkommen** des Europarats sowie um **Forderungen der EFTA Surveillance Authority** (ESA). Ausserdem sollte eine Anpassung an das per 01. Januar 2008 revidierte Schweizer Bundesgesetz für den Datenschutz, das dem liechtensteinischen als Rezeptionsvorlage diente, erfolgen. Weiters sollte eine rechtliche Grundlage für Videoüberwachungen im öffentlichen Raum, wie sie die DSK in der Entscheidung zur Videoüberwachungen in der Fussgängerzone von Vaduz gefordert hatte,[75] geschaffen werden.

Die Forderungen der ESA betrafen vor allem eine Anpassung der Bestimmungen zur *Datenbekanntgabe ins Ausland* und zur *Registrierungspflicht von Datensammlungen.* Bisher mussten private Personen Datensammlungen nur ausnahmsweise registrieren lassen, was nicht der Richtlinie entsprach.

Von der letzten Revision des Schweizer Bundesgesetzes für den Datenschutz wurde insbesondere die Einführung von *Zertifizierungsverfahren* übernommen. Mittels eines Zertifizierungsverfahrens kann für betriebliche Abläufe und Organisationsstrukturen, aber auch für informationstechnische Produkte die Auszeichnung durch ein noch zu gründendes *Datenschutzqualitätszeichen* verliehen werden. Abgesehen von der Schaffung eines Wettbewerbsvorteils führen Zertifizierungsverfahren zu einer Stärkung der Selbstverantwortung der Inhaber der Datensammlungen und tragen sicherlich dazu bei, den Datenschutz zu fördern.

Zusätzlich ist vorgesehen, im Rahmen der DSV die Funktion eines *betrieblichen Datenschutzbeauftragten* zu schaffen.[76] Diese Funktion ist mittlerweile in einigen europäischen Ländern, zu denen auch die Schweiz zählt, gesetzlich verankert. Die Bestimmung einer firmeninternen Stelle, die für die Einhaltung des Datenschutzes verantwortlich ist, erleichtert die Umsetzung und Koordinierung der datenschutzrechtlichen Vorgaben. Die zweite Teilrevision tritt zum 01. Juli 2009 in Kraft.

Das DSG sah eine Übergangsfrist vor, wonach für die Bearbeitung von besonders schützenswerten Daten und/oder Persönlichkeitsprofilen eine ausdrückliche gesetzliche Grundlage ge-

[71] Vgl. hierzu ausführlich 10.1.
[72] Vgl. Art. 28 Abs. 2 DSG: «[Er, der Datenschutzbeauftragte] er führt seine Aufgabe unabhängig. Er kann einem Ressort der Regierung administrativ zugeordnet werden.»
[73] Vgl. Art. 28 der Richtlinie 95/46/EG («complete independence»).
[74] Diese Experten analysieren die bestehende Gesetzgebung und deren Umsetzung in die Praxis im Hinblick darauf, ob der Datenschutz den Ansprüchen eines Beitritts zu den Abkommen zu Schengen und Dublin entspricht.
[75] Vgl. 2.1.
[76] Hierzu soll die DSV angepasst werden.

schaffen werden musste. Dem wurde nunmehr in einer *Sammelvorlage bezüglich der Bearbeitung von Personendaten* nachgekommen.[77]

Weiters haben wir zu folgenden Gesetzesprojekten eine Stellungnahme abgegeben:

- Ausserstreitgesetz;
- Einführung eines Betreuungs- und Pflegegeldes bei Hauspflege;
- Gesetz über Ausländerinnen und Ausländer ohne EWR- oder Schweizer Staatsangehörigkeit;
- Gesetz über Elektrizitätsmarkt;
- Gesetz über Erdgasmarkt;
- Gesetz über die Krankenversicherung;
- Gesetz über die Vermittlung von und den Handel mit Kriegsmaterial;
- Gesetz über die Vermittlung und den Handel mit nuklearen Gütern, radioaktiven Abfällen, doppelt verwendbaren Gütern und besonderen militärischen Gütern;
- Gesetz über Zahlungsdienste;
- Offenlegungsgesetz;
- Personalverordnungen;
- Rechtshilfegesetz;
- Religionsgesetz;
- Schaffung gesetzlicher Grundlagen zur Führung und Transparenz von öffentlichen Unternehmen;
- Strafregistergesetz;
- Umsetzung der Geldwäscherichtlinie 2005/60/EG;
- Waffengesetz.

[77] Angepasst wurden beispielsweise folgende Gesetze: Arbeitslosen- und Arbeitsvermittlungsgesetz, Gesetz über Mietbeiträge für Familien, Gemeindegesetz, Invaliditätsversicherungsgesetz, Sozialhilfegesetz, Berufsbildungsgesetz, Jugendgesetz, Bewährungshilfegesetz, Schulgesetz, Strafregistergesetz, Flüchtlingsgesetz.

10. Europa und Internationales

10.1. SCHENGEN / DUBLIN

Ende Februar unterzeichnete die Regierung die **Beitrittserklärung** zu den **Abkommen** von **Schengen** und **Dublin**. In beiden Abkommen spielt der Datenschutz eine bedeutende Rolle. Mit dem Beitritt werden die Personenkontrollen an den Grenzen zwischen den Schengen-Mitgliedstaaten aufgehoben und der freie Personenverkehr ist durch das gesamte Vertragsgebiet ohne weitere Grenzkontrollen möglich. Die Teilnahme an Schengen bedeutet für Liechtenstein auch, dass zukünftig der *Zugriff auf das Schengener Informationssystem* (SIS) *zur Fahndungs- und Personenabfrage* möglich ist.

Das SIS, welches im Schengener Durchführungsübereinkommen (SDÜ) definiert ist, beinhaltet Millionen von Datensätzen zu gefahndeten Personen, Fahrzeugen und Gegenständen. Die SDÜ schreibt detailliert vor, *welche Daten zu welchen Zwecken bearbeiten* werden dürfen. Gleichzeitig sieht das SDÜ einen *Kontrollmechanismus* vor. In diesem Sinne werden diejenigen Stellen zu prüfen sein, welche Zugriff auf die im SIS gespeicherten Informationen haben, diese abrufen oder bearbeiten können. Das Ziel ist es, die Datenqualität so hoch wie möglich zu halten und Missbrauch vorzubeugen. Es ist offensichtlich, dass es bei der irrtümlichen Ausschreibung einer Person bzw. eines Fahrzeugs für die betroffene Person im Ausland zu unangenehmen Konsequenzen kommen kann.

Ähnlich wie das SIS sieht auch das Abkommen von *Dublin* eine Vernetzung der nationalen Ausländerbehörden vor. Deshalb wurde ein gemeinschaftsweites System zur *Abnahme der Fingerabdrücke von Asylwerbern,* der *Eurodac,* beschlossen. Eurodac ermöglicht die Identifizierung dieser Personen. Das Abkommen von Dublin soll insbesondere auch das so genannte *Asylshopping* vermeiden.

Die Eurodac Verordnung sieht – ebenso wie das SDÜ – detaillierte Datenbearbeitung und Datenschutzbestimmungen vor. Wir sind in beiden Fällen jeweils die *zuständige Aufsichtsstelle.*[78]

Im Rahmen der entsprechenden Kontrollgremien auf europäischer Ebene, die *Gemeinsame Kontrollinstanz von Schengen* oder die *Eurodac Supervision Coordination Group* werden Untersuchungen über die Anwendung der rechtlichen Bestimmungen durchgeführt. So gab es im Berichtsjahr beispielsweise Untersuchungen der Gemeinsamen Kontrollinstanz von Schengen zur Anwendung von Art. 97 und Art. 98 SDÜ in den Mitgliedstaaten. Eine Untersuchung der Eurodac Supervision Coordination Group betraf die Informationen an die Betroffenen sowie die Feststellung des Alters von minderjährigen Asylsuchenden.

Mit einem Beitritt zu den Abkommen von Schengen und Dublin sind neue Aufgaben für den Datenschutz auf nationaler Ebene verbunden: So müssen *Kontrollen bei den entsprechenden Amtsstellen* durchgeführt werden, die SIS wie auch Eurodac benutzen. Entsprechend den Empfehlungen der *«Best Practices» – Kataloge* sollen die Kontrollen regelmässig und nicht bloss im Beschwerdefall durchgeführt werden. Durch eine Teilnahme als Beobachter in diesen Gremien konnten wir bereits erste wichtige Erfahrungen sammeln.

Die Regierung setzte eine *Arbeitsgruppe* zur Umsetzung der Anforderungen von Schengen und Dublin ein, in der wir mitarbeiten. Im März 2008 fand die Datenschutzevaluation der Schweiz statt. Wir konnten Erfahrungen dieser Evaluation wie auch weitere Informationen in die Arbeitsgruppe einbringen. Einmal mehr wurde dabei auf die Wichtigkeit einer unabhängigen Datenschutzstelle als Kontrollstelle hingewiesen.[79]

Der Schengenbeitritt erfordert auch eine *Informationskampagne,* insbesondere, damit die betroffenen Personen auf ihre Rechte aufmerksam gemacht werden. Weiters sollen Schulungen durchgeführt werden.

10.2. INTERNATIONALE VEREINIGUNGEN

10.2.1. ART. 29 DATENSCHUTZGRUPPE

Das Gremium unabhängiger nationaler Datenschutzbehörden des EWR, die so genannte **Art. 29 Datenschutzgruppe**, diskutiert *aktuelle Themen,* die sowohl auf europäischer, als auch nationaler Ebene für den Datenschutz von Bedeutung sind. Insbesondere werden in regelmässigen Abständen Dokumente[80] zu Themen von internationaler Relevanz verabschiedet, die auch für Liechtenstein von Bedeutung sind. Davon sind vor allem folgende Dokumente nennenswert:

[78] Vgl. Art. 19 SDÜ und Art. 20 Eurodac-Verordnung.
[79] Vgl. 9.
[80] Die so genannten Working Papers (WP) sind chronologisch abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_de.htm.*

In einem Arbeitspapier beschäftigte sie sich ausschliesslich mit dem **Schutz der personenbezogenen Daten von Kindern**.[81] Kinder sind im Vergleich zu Erwachsenen leichter verletzlich und sind somit auch aus datenschutzrechtlicher Sicht besonders schutzbedürftig. Erwähnenswert ist, dass es keine gemeinschaftsrechtlichen Rechtsvorschriften gibt, die ausschliesslich Kinder betreffen. Die massgeblichen Datenschutzregeln gelten für alle natürlichen Personen gleichermassen. Bei einem Kind sind jedoch die unterschiedlichen Reifegrade zu berücksichtigen. Beispielsweise, ab wann es sich mit seinen eigenen Daten befassen kann oder inwieweit der Vertreter das Recht auf Vertretung von Minderjährigen in Fällen besitzt, in denen die Offenlegung personenbezogener Daten dem Wohl des Kindes schaden würde.

Weiters wurde in diesem Papier untersucht, unter welchen Umständen z.B. *Fotos auf Internetseiten* veröffentlicht, *Gesundheitsdaten bearbeitet* werden dürfen oder eine *Videoüberwachung* zulässig ist. Neben dem allgemein wichtigen Grundsatz des Kindeswohls kommen der Beurteilung der Anpassung an den Reifegrad des Kindes und dem Recht auf Anhörung eine entscheidende Bedeutung zu. Auch Daten über den Gesundheitszustand von Kindern dürfen nur mit der *Einwilligung der Vertreter* des Kindes oder im *Notfall* verarbeitet werden. Die Verarbeitung sollte nur durch *Ärzte oder Lehrer* und solches Personal durchgeführt werden, die einer *Schweigepflicht* unterliegen.

Immer häufiger *erstellen Schulen eigene Internetseiten*. Die Art. 29 Datenschutzgruppe empfiehlt zum Schutz personenbezogener Daten von und durch Kinder(n) die Einführung von Mechanismen für den *eingeschränkten Zugriff* (z.B. Anmeldung mittels Benutzerkennung und Passwort). Besonders in Bezug auf die Veröffentlichung von *Schülerfotos* sollten ihre Vertreter aufmerksam gemacht und deren bzw. die *Einwilligung* des Kindes eingeholt werden, sofern es die nötige Reife besitzt. Dieses Dokument wurde dem Schulamt zugestellt und der Öffentlichkeit zugänglich gemacht.

In einem anderen Arbeitspapier[82] analysiert die Art. 29 Datenschutzgruppe die Möglichkeiten der **Suchmaschinen**, legt die Rechtslage dar und zieht daraus ihre Schlussfolgerungen. Diese lauten, zusammengefasst, wie folgt: Als Suchmaschine ist ein in der Regel *kostenloser Dienst* zu verstehen, der seinem Benutzer beim *Auffinden von Information im Internet* behilflich ist. Diese Funktion ist in der heutigen Informationsgesellschaft von grosser Bedeutung. Allerdings hinterlässt der einzelne Internetbenutzer bei jeder Suchabfrage unvermeidbare Spuren.

Bei der Benutzung des Suchdienstes werden vom Suchmaschinenbetreiber mehrere Arten von Daten *protokolliert.* Dies sind insbesondere Inhalt, Datum und Uhrzeit der Anfrage, IP–Adresse[83], Browser–Cookies[84], Flash–Cookies[85], benutzerspezifische Einstellungen sowie Daten, die sich auf den Computer des Benutzers, auf die angebotenen Inhalte und auch auf die anschliessende Benutzernavigation beziehen. Jeder Computer besitzt eine IP–Adresse, die ihm vom Internet Provider oder einem lokalen Netzwerkdienst (statisch oder dynamisch) zugeordnet wird. Ein Suchmaschinenbetreiber kann so verschiedene Anfragen und Suchsitzungen miteinander verknüpfen. Über die IP-Adresse ist also ohne Weiteres eine konkrete Person bestimmbar. Nach Ansicht der Art. 29 Datenschutzgruppe handelt es sich bei IP-Adressen um «personenbezogene Daten», die dem Datenschutzrecht unterliegen.[86]

Die Art. 29 Datenschutzgruppe stellt daher in ihrer Stellungnahme Forderungen an die Betreiber von Internetsuchmaschinen, um zu einem ausgewogenen Ausgleich zwischen den Interessen der Suchmaschinenanbieter und der Persönlichkeitsrechte der Suchmaschinenbenutzer zu gelangen. Eine der ent-

[81] Arbeitspapier 1/2008 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen), angenommen am 18. Februar 2008 (WP 147), abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_de.pdf.*

[82] Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, angenommen am 04.04.08 (WP 148); *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_de.pdf.*

[83] IP steht für «Internet Protocol», das grundlegende Protokoll im Internet und vielen lokalen Netzen. Hieraus leitet sich umgangssprachlich der Begriff der IP-Adresse ab. Damit ist die im Rahmen dieses Protokolls an einen Rechner vergebene Nummer gemeint, unter der der Rechner im Netz erreichbar ist. Ein Suchmaschinenbetreiber kann auch verschiedene Anfragen und Suchsitzungen, die von einer einzigen IP-Adresse ausgehen, miteinander verknüpfen (vgl. WP 148, aaO, S. 7).

[84] Browser-Cookies (auch HTTP- oder Web-Cookies genannt) bezeichnen Informationen, die ein Webserver zu einem Browser (= spezielle Computerprogramme zum Betrachten von Webseiten im World Wide Web) sendet. Browser-Cookies werden also von der Suchmaschine übermittelt und auf dem Computer des Benutzers gespeichert. Sie ermöglichen so eine genauere Identifizierung des Benutzers der IP-Adresse.

[85] Flash-Cookies (auch Local Shared Objects, LCO, genannt) stellen eine neue Art der Speicherung von Benutzerdaten auf dem surfenden Computer durch Nutzung des Adobe Flash Players dar. Im Gegensatz zu Browser-Cookies (s. vorhergehende Fussnote) ermöglicht diese Technik den Webseiten, Inhalte browserunabhängig und ohne Verfallsdatum auf dem Rechner des Webseitenbetrachters zu speichern. Gegenwärtig können Flash-Cookies nicht ohne Weiteres, etwa mit Hilfe der Standardlöschfunktionen der Internet Browser, gelöscht werden.

[86] *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf*; vgl. auch Tätigkeitsbericht 2007, 7.1.

scheidenden Schlussfolgerungen ist, dass die Datenschutzrichtlinie auf die Datenbearbeitung im Rahmen der Internetsuchmaschinen anzuwenden ist, selbst wenn der Sitz des Anbieters ausserhalb des EU-/EWR-Raums liegt.

Die Suchmaschinenbetreiber müssen *personenbezogene Daten löschen* oder *irreversibel anonymisieren,* sobald sie der angegebenen rechtmässigen Zweckbestimmung nicht mehr dienen. Ausserdem muss die *Speicherdauer* der Daten *angemessen* sein. Die Art. 29 Datenschutzgruppe fordert eine Speicherdauer von *höchstens sechs Monaten.* Bei allen geplanten *Querverbindungen* von Benutzerdaten und bei der Anreicherung von Benutzerprofilen muss die *Einwilligung* des Benutzers eingeholt werden.

Die Suchmaschinen müssen die Benutzer im Vorhinein über alle beabsichtigten Bearbeitungs- und Verwendungszwecke ihrer Daten informieren und ihre Rechte auf Auskunft, Einsichtnahme oder Berichtigung ihrer personenbezogenen Daten respektieren. Insofern wird gefordert, dass die Suchmaschinenbetreiber auf den jeweiligen Internetseiten Datenschutzbestimmungen einbauen sollten. Es bleibt abzuwarten, ob sich Datenschutz und die *Sicherheit der Daten* als ein den Kauf mitbestimmendes Kriterium herauskristallisieren und somit als Wettbewerbsvorteil von den Anbietern erkannt und eingesetzt wird.

Ein Schwerpunkt der Art. 29 Datenschutzgruppe lag im Berichtsjahr auf einer Verbesserung der **verbindlichen unternehmensinternen Datenschutzregelungen** (Binding Corporate Rules – BCR)[87]. Hierzu wurden drei Arbeitspapiere angenommen.[88]

Verbindliche unternehmensinterne Datenschutzregelungen stellen nach Meinung der Art. 29 Datenschutzgruppe eine geeignete Lösung für internationale Konzerne und ähnliche Unternehmensgruppen dar, um bei der *Übermittlung personenbezogener Daten* in Länder *ausserhalb des europäischen Wirtschaftsraums (EWR) ein angemessenes Datenschutzniveau* zu gewährleisten und ihren rechtlichen Verpflichtungen nachzukommen. Bereits 2003 und 2005 hatte die Art. 29 Datenschutzgruppe zu BCR zwei grundlegende Stellungnahmen erarbeitet.[89]

Diese Arbeitspapiere sollen nun, mit Unterstützung der nationalen Datenschutzbehörden, auf Grund ihrer gewonnenen Erfahrungen verbessert und noch stärker an der gängigen Praxis ausgerichtet werden.

So entstanden drei weitere Arbeitspapiere:

- Die *erste Stellungnahme*[90] enthält eine sehr praxisgerechte *Übersicht,* die den betroffenen Unternehmen die Anwendung der BCR erleichtern soll. Es wird insbesondere genau angegeben, *welche Bestimmungen in die BCR aufzunehmen* sind und welche Angaben das Antragsformular für die Genehmigung der BCR enthalten muss.[91]
- Das *nachfolgende Arbeitsdokument* gibt einen Rahmen für die *Struktur von BCR* vor.[92] Dabei handelt es sich, nach Aussage der Art. 29 Datenschutzgruppe, nicht um ein Muster, sondern um einen Vorschlag, wie eine verbindliche unternehmensinterne Datenschutzregelung strukturiert werden und wie sie inhaltlich aussehen könnte. Die verbindlichen unternehmensinternen Datenschutzregelungen sollten in jedem Einzelfall auf die Struktur, Datenverarbeitung, Datenschutzpolitik und Verfahren der jeweiligen Unternehmensgruppe konkret zugeschnitten sein.
- Das *dritte Arbeitspapier*[93] befasst sich mit *häufig gestellten Fragen* (Frequently Asked Questions, FAQ), wie z.B. mit der Frage, ob die verbindlichen unternehmensinternen Daten-

[87] Zu BCR vgl. auch 2.3.

[88] Vgl. *http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_de.htm.*

[89] Arbeitsdokument der Art. 29 Datenschutzgruppe zur Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer, angenommen am 3. Juni 2003 (WP 74), abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_de.pdf* und Arbeitsdokument «Muster-Checkliste für Anträge auf Genehmigungen verbindlicher unternehmensinterner Datenschutzregelungen», angenommen am 14. April 2005 (WP 108), abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_de.pdf.*

[90] Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR), angenommen am 24. Juni 2008 (WP 153), abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp153_de.pdf.*

[91] Vgl. zu den Antragsbedingungen die Empfehlung 1/2007 der Art. 29 Datenschutzgruppe über das Antragsformular für Genehmigungen von verbindlichen unternehmensinternen Datenschutzregelungen zur Übermittlung personenbezogener Daten, angenommen am 10. Januar 2007 (WP 133), abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp133_en.doc.*

[92] Arbeitsdokument «Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR)», angenommen am 24. Juni 2008 (WP 154), abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp154_de.pdf.*

[93] Arbeitsdokument zu «Häufig gestellten Fragen» über verbindliche unternehmensinterne Datenschutzregelungen (BCR), angenommen am 24. Juni 2008, überarbeitet und angenommen am 1. Oktober 2008 (WP 155), abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp155_de.pdf.*

schutzregelungen auf alle im Unternehmen verarbeiteten personenbezogenen Daten angewandt werden müssen. Die Art. 29 Datenschutzgruppe ist dabei, die FAQ fortlaufend zu ergänzen.

Alle drei Dokumente haben zum Ziel, international tätige Konzerne bei der Ausarbeitung von unternehmensübergreifenden Datenschutzregelungen zu unterstützen und deren reibungslose Genehmigung durch die zuständigen Stellen zu ermöglichen.

In diesem Zusammenhang ist von Interesse, dass sich im Rahmen der Art. 29 Datenschutzgruppe einige Länder zu einer *gegenseitigen Anerkennung* der BCR zusammengefunden haben. Nach diesem Prinzip erkennen die beteiligten Länder die verbindlichen unternehmensinternen Datenschutzregelungen ohne einer neuerlichen detaillierten inhaltlichen Prüfung an. Diese Datenschutzregelungen waren zuvor von einer der anderen beteiligten nationalen Datenschutzbehörde[94] eingehend geprüft und für rechtmässig befunden worden. Die gegenseitige Anerkennung basiert daher auf gegenseitigem Vertrauen und auf dem Grundsatz, dass die Datenschutzgesetzgebungen der beteiligten Länder alle den von der europäischen Datenschutzrichtlinie vorgegebenen Mindeststandard garantieren.[95]

10.2.2. EUROPARAT

Im Datenschutzausschuss des Europarats wurde eine **Expertenstudie zum Thema «profiling»** (also dem Erstellen von Profilen) diskutiert. Genannt werden in diesem Zusammenhang z.B. die Datenbearbeitung durch Suchmaschinen, das digitale Kabelfernsehen,[96] die Bildung von Kundenprofilen, insbesondere bei Banken und Versicherungen, usw. Auch in Bezug auf automatisierte Einzelentscheidungen oder zur Datenbearbeitung zu statistischen Zwecken sind interessante Passagen enthalten. Es wurde beschlossen, die Studie öffentlich zugänglich zu machen[97] und im Anschluss die Arbeiten fortzusetzen. Diese Studie ist aus Sicht Liechtensteins besonders interessant, da Liechtenstein neben der Schweiz das einzige Land in Europa zu sein scheint, welches den Begriff des «Persönlichkeitsprofils» gesetzlich vorsieht.[98]

Das Sekretariat stellte ausserdem den ersten Entwurf einer Liste von Elementen zur Erfüllung der Kriterien der **Unabhängigkeit** und **Befugnisse** einer **nationalen Datenschutzbehörde** vor. Anhand dieser Kriterien sollen gewisse Lücken, welche im erläuternden Bericht zum Zusatzprotokoll der Datenschutzkonvention aufscheinen, gefüllt werden. Diese Tätigkeit ist aus liechtensteinischer Sicht zu begrüssen, da die Ratifikation des Zusatzprotokolls geplant ist. Zudem ist die Unabhängigkeit, wie bereits ausgeführt, ein wesentliches Erfordernis für den Schengenbeitritt.

Das Zusatzprotokoll wurde von Liechtenstein bislang noch nicht unterzeichnet, obwohl die Voraussetzungen dazu mit den beiden letzten Revisionen des DSG geschaffen wurden.[99]

10.2.3. EUROPÄISCHE DATENSCHUTZKONFERENZ

An der Europäischen Datenschutzkonferenz konnte im Berichtsjahr nicht teilgenommen werden.

Im Rahmen der Europäischen Konferenz werden zwei mal pro Jahr so genannte **Case Handling Workshops** abgehalten. An diesen Workshops werden *aktuelle Themen und konkrete Fälle* behandelt, welche für die Datenschutzbehörden in Europa wichtig sind. Im Berichtsjahr nahmen wir an beiden Workshops teil, an denen sehr nützliche Informationen in Erfahrung gebracht werden konnten: Neben dem Schutz von Arbeitnehmern, der Biometrie oder dem betrieblichen Datenschutzbeauftragten, der auch in Liechtenstein eingeführt werden soll,[100] ging es um Aufgaben von Datenschutzbehörden im Zusammenhang mit Schengen/Dublin, Beschwerden im Zusammenhang mit dem Internet oder der Videoüberwachung.

[94] Diese Behörde wird in der Regel die so genannte «lead authority» sein: Im Rahmen des Antragsverfahrens müssen alle nationalen Datenschutzbehörden, in deren Zuständigkeitsbereich die BCR fallen, beteiligt werden und ihre Zustimmung geben. Eine der beteiligten Datenschutzbehörden wird zu Beginn als lead authority bestimmt, die den gesamten Prozess und die Abstimmung aller beteiligten Stellen koordiniert. Hierzu bietet sich regelmässig die Datenschutzbehörde jenes Landes an, in dem das Antrag stellende Unternehmen seinen Hauptsitz hat.

[95] Vgl. Pressemitteilung der Art. 29 Datenschutzgruppe vom 02. Oktober 2008, abzurufen unter: *http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_02_10_08_en.pdf*.

[96] Vgl. auch Arbeitspapier «Datenschutz bei der Verbreitung digitaler Medieninhalte und beim digitalen Fernsehen» der internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation: *http://www.datenschutz-berlin.de/attachments/350/digit_de.pdf?1201702162*.

[97] *http://www.coe.int/t/e/legal_affairs/legal_coperation/data_protection/documents/reports%20and%20studies%20by%20experts/1CRID_Profiling_2008_en.pdf*.

[98] Art. 3 Abs. 1 Buchstabe f DSG.

[99] Vgl. 9.

[100] Vgl. 9.

Die **Working Party on Police and Justice** WPPJ hat sich als wichtigste Untergruppe der Konferenz der Europäischen Datenschutzkonferenz etabliert. Als Pendant und Bindeglied zur Artikel 29 Datenschutzgruppe behandelt sie hauptsächlich die *wichtigsten datenschutzrechtlichen Fragen in der dritten Säule der EU, der polizeilichen und justiziellen Zusammenarbeit.* Dazu gehören auch Aspekte, die für Schengen relevant sein können. Im Berichtsjahr beschäftigte sich die WPPJ unter anderem mit der Umsetzung der Cybercrime Convention des Europarats, der Erstellung eines Datenschutzkatalogs für Kooperation und Aufsicht auf dem Gebiet der Rechtsdurchsetzung in der EU und der so genannten Schwedischen Initiative.

10.2.4 INTERNATIONALE DATENSCHUTZ-KONFERENZ

Die **Internationale Konferenz der Datenschutzbeauftragten** fand im Oktober in Strassburg statt.[101] Unter dem Thema *«Der Schutz der Privatsphäre in einer Welt ohne Grenzen»* nahmen vorwiegend Vertreter von Datenschutzbehörden und der Wirtschaft teil. Behandelt wurden die aktuellen Herausforderungen, die sich für den Datenschutz stellen. Die Konferenz verabschiedete unter anderem Entschliessungen zum Schutz der Privatsphäre von Kindern im Internet und zum Schutz der Privatsphäre in sozialen Netzwerken.

Die **Internationale Arbeitsgruppe Datenschutz im Telekommunikationsbereich** (International Working Group on Data Protection in Telecommunications – IWGDPT[102]) wurde im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten im Jahr 1983 auf Initiative des Berliner Datenschutzbeauftragten gegründet. Sie hat seither eine Vielzahl von Empfehlungen zur Verbesserung des Datenschutzes in der Telekommunikation erarbeitet. Teilnehmer sind Datenschutzbehörden, Regierungsvertreter und Vertreter internationaler Organisationen. Im Berichtsjahr wurde zur Problematik der *sozialen Netzwerke* ein Dokument, dem *«Rom Memorandum»* verabschiedet. In den letzten Jahren sind Webdienste, wie *facebook,* auch in Liechtenstein immer beliebter geworden. Das besagte Dokument soll in diesem Zusammenhang Risiken in Bezug auf die Privatsphäre aufzeigen. Es enthält auch Empfehlungen, die sich an die unterschiedlichen Akteure richten, d.h. Gesetzgeber, Anbieter von sozialen Netzwerkdiensten und Nutzer.[103]

10.2.5 PRIVATIM – VEREINIGUNG DER SCHWEIZER DATENSCHUTZBEAUFTRAGTEN

An der Frühjahrssitzung der Vereinigung der Datenschutzbeauftragten aller Kantone ging es vor allem um den *Beitritt zu Schengen und Dublin* und die Konsequenzen der stattgefundenen Evaluation. Für Liechtenstein sind die Erfahrungen aus der Schweiz im Hinblick auf die noch anstehende Evaluation sehr hilfreich. Insbesondere beim Datenschutzrecht können viele Parallelen gezogen werden.

10.2.6. PROJEKTPARTNERSCHAFT BEIM VIRTUELLEN DATENSCHUTZBÜRO

Wir sind einer von insgesamt 26 Projektpartnern[104] beim Virtuellen Datenschutzbüro, einer *Internetplattform*. Auf dieser werden wichtige Informationen, Neuigkeiten oder Entwicklungen rund um den Datenschutz zusammengefasst dargestellt.[105] Ausserdem werden Beratungsmöglichkeiten aufgezeigt sowie Hinweise auf aktuelle Pressemitteilungen und (Fortbildungs-)Veranstaltungen im Zusammenhang mit Datenschutz angeboten. Auch rechtliche Themen werden in einem ausführlichen Schlagwortregister anwenderfreundlich aufbereitet, wie beispielsweise zu *Kreditscoring*[106] *oder zum Bankgeheimnis*. Die Zusammenarbeit ist für uns wichtig und bereichernd.

[101] *www.privacyconference2008.org.*
[102] Die IWGDPT wird auch als «Berlin Gruppe» bezeichnet.
[103] *http://www.llv.li/pdf-llv-sds-675.36.13.*
[104] Zahl der Projektpartner Ende 2008. Als Projektpartner werden nur institutionalisierte Datenschutzkontrollinstanzen akzeptiert. Neben vielen deutschen Datenschutzbehörden sind mittlerweile auch vier Schweizer Datenschutzstellen Projektpartner. Das Virtuelle Datenschutzbüro wird federführend vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein in Deutschland verwaltet.
[105] Vgl. *http://www.datenschutz.de.*
[106] Mit einem Kreditscoring kann eine Bank die Kreditwürdigkeit eines Kunden ermitteln.

11. Aus der Stabsstelle für Datenschutz

11.1. VERANSTALTUNGEN / ÖFFENTLICHKEITS-ARBEIT

Unsere **Internetseite**[107] ist jene Plattform, auf der wir über alle wichtigen Themen rund um den Datenschutz informieren. Wie die Statistik zeigt, *stieg die Zahl der Zugriffe kontinuierlich:* Im Berichtsjahr betrug sie 234'646 bei 8'355 unterschiedlichen Besuchern. Damit hat sich die Anzahl der Zugriffe im Vergleich zum Vorjahr mehr als vervierfacht. 2007 haben 7'158 Personen 54'679 mal die Internetseite besucht.

2008 wurde insbesondere über folgende *Themenbereiche* informiert:

- Soziale Netzwerke im Internet;[108]
- Datenschutz und Kinder;[109]
- Internet und Kinder: In diesem Zusammenhang ist an die Verantwortung der Internetanbieter, aber vor allem auch an die Erziehungsverantwortlichen und Lehrkräfte zu appellieren, Kinder nicht ohne entsprechende Anleitung im Internet surfen zu lassen.
- Entscheidung der DSK zur Videoüberwachung in Vaduz;[110]
- *Urteil des Deutschen Bundesverfassungsgerichts zu geheimen Online-Durchsuchungen:* Im Februar 2008 traf das deutsche Bundesverfassungsgericht eine Entscheidung im Zusammenhang mit geheimen Onlineuntersuchungen, die europaweit bei den Datenschützern für Zustimmung sorgt. In dem Urteil hat das deutsche Bundesverfassungsgericht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Teil des allgemeinen Persönlichkeitsrecht formuliert, das Daten in Computern, Netzen und anderen IT-Systemen umfassend schützt.[111]

Anlässlich des **zweiten Europäischen Datenschutztags** am 28. Januar wurde eine Pressemitteilung versandt.

Dass der Datenschutz auch in der Privatwirtschaft immer wichtiger wird, zeigen die zunehmenden Anfragen aus dem privaten Bereich.[112] Uns war es daher ein grosses Anliegen, **Richtlinien für die Bearbeitung von Personendaten im privaten Bereich** herauszugeben.[113] Die Richtlinien geben mit vielen Beispielen aus der Praxis eine Anleitung für einen datenschutzkonformen Umgang mit Personendaten, wie z.B. bei Banken, Versicherungen und international tätigen Unternehmen. Schwerpunkte lagen hierbei neben der Darstellung eines *Datentransfers ins Ausland*[114] auf der *vorherigen Information der betroffenen Personen sowie den Anforderungen an eine rechtswirksame Einwilligung* in eine Datenbearbeitung.

Eine datenschutzrechtlich wirksame Einwilligung muss *ohne Zwang, freiwillig und in Kenntnis der Sachlage im konkreten Fall* erteilt werden. Diesen hohen Ansprüchen wird eine in den Allgemeinen Geschäftsbedingungen vorgesehene Einverständnisklausel oftmals nicht gerecht.

Ein weiteres Kapitel wird der *Datenbearbeitung unter Beteiligung Dritter* gewidmet, da in den letzten Jahren auf Grund der fortschreitenden Spezialisierungen vermehrt eine Unterauftragsvergabe in Betracht gezogen wurde.

Ausserdem wurden **Richtlinien über den Umgang mit unerwünschter Werbung**, *insbesondere Spam,* ausgegeben. Dabei wird über die *Einordnung und Handhabung* unerwünschter Werbung auf dem Postwege und übers Internet detailliert informiert. Neben einer grundlegenden Einführung, wann es sich überhaupt um unerwünschte Werbung handelt, zeigen die Richtlinien den Betroffenen ihre Rechte auf und bieten zahlreiche praktische Hinweise, wie man sich vor unerwünschter Werbung zukünftig schützen kann. Auch diese Richtlinien können bei uns bezogen oder über unsere Internetseite abgerufen werden.[115]

[107] *http://www.dss.llv.li.*
[108] Vgl. ausführlich zu sozialen Netzwerken, 10.2.1.
[109] Vgl. ausführlich zu Datenschutz und Kindern, 10.2.1.
[110] Vgl. ausführlich zur Entscheidung der DSK im Anhang, 12.2.
[111] Vgl. *http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-022.html.*
[112] Vgl. Statistik im Anhang, 13.1.
[113] *http://www.llv.li/amtsstellen/llv-dss-privatpersonen.htm.*
Die Bezeichnung «private Bereiche» ist im Gegensatz zum «öffentlichen Bereich» gemeint. Sie bezieht sich auf das privatwirtschaftliche Handeln in Abgrenzung zum staatlichen Handeln.
[114] Vgl. ausführlich zum Datentransfer ins Ausland, 2.3. und 10.2.1.
[115] Vgl. *http://www.llv.li/richtlinie_ueber_den_umgang_mit_unerwuenschter_direktwerbung_insbesondere_mit_spam-4.pdf.*

Schliesslich wurden die **Richtlinien über die Rechte betroffener Personen** komplett *neu bearbeitet und aktualisiert*.[116] So wurden viele Beispiele aus der Praxis eingebaut, wobei der Schwerpunkt auf den *Arbeitsbereich* bzw. auf das Thema der *unerwünschten Werbung* gelegt wurde. Ausführlich ist auch das *Auskunftsrecht* dargestellt, das jeder Einzelne jederzeit wahrnehmen kann, um herauszufinden, welche seiner Daten von wem bearbeitet werden und insbesondere, von wo die Daten verarbeitende Stelle diese erhalten hat.

11.2. SCHULUNGEN

Neben der jährlich stattfindenden *verwaltungsinternen Schulung* von Mitarbeitern fand erstmalig auch eine verwaltungsinterne *Schulung der Lehrlinge* statt. Auch schon während der Lehre sind Berührungspunkte mit dem Datenschutz an der Tagesordnung. So gilt das Datengeheimnis bereits in der Ausbildung.[117] Es ist daher wichtig, dass die Lehrlinge wissen, worum es bei Datenschutz geht, welche Ziele er verfolgt und was Datenschutz in der täglichen Arbeit bedeutet. Der Schwerpunkt der *allgemeinen Schulungsveranstaltung* für interessierte Mitarbeiter lag neben der Vermittlung von Grundlagen darauf, wie eine alltäglich stattfindende Bekanntgabe von Personendaten durch Behörden datenschutzkonform zu handhaben ist. Dabei wurde insbesondere ein Fokus auf das Spannungsfeld zwischen Datenbekanntgabe und Amtsgeheimnis gelegt.

11.3. ORGANISATORISCHES UND PERSONELLES

Der **Beitritt** Liechtensteins zu den Abkommen von **Schengen** und **Dublin** bedingt, wie ausgeführt,[118] eine *Stärkung der Unabhängigkeit*. Vor der ersten Teilrevision des DSG bestand ein *Konfliktpotenzial* zwischen der *organisatorischen und budgetären Gewalt* der Regierung über den Datenschutzbeauftragten (bzw. die Stabsstelle) einerseits und dessen (bzw. deren) Aufsichtsfunktion über die Behörden andererseits. Hinsichtlich der *technischen und administrativen Unterstützung* der Datenschutzstelle durch die Landesverwaltung befürwortete die Regierung den Abschluss einer *Leistungsvereinbarung* mit der Landesverwaltung, insbesondere für die Beschaffung und den Unterhalt der Informatik. Dadurch sollen mögliche Unklarheiten in diesem Bereich von vornherein ausgeschlossen werden. Diese Leistungsvereinbarung soll selbstverständlich die neue Organisation der Stabsstelle berücksichtigen.[119]

Die zahlreichen neuen Aufgaben wären mit dem vorhandenen Personalbestand nicht zu bewältigen gewesen. Wir haben daher *zusätzliche Stellen* beantragt, die noch im Berichtsjahr *genehmigt* wurden. Mit Beginn 2009 werden wir daher über folgende Stellenprozente verfügen, die teilweise jedoch noch befristet sind: 2.2 Juristen, 1.0 Sekretariat, 1.0 Informatik. Dies bedeutet einen Stellenzuwachs von insgesamt 1.5 Stellen, was bei so einer kleinen Stelle bedeutsam ist und für die Bewältigung der zukünftigen Aufgaben erforderlich sein wird.

Parallel dazu wurde entsprechend der neuen Vorgaben des DSG mit den Vorbereitungen für unsere *Loslösung aus der Landesverwaltung* begonnen. Diese Arbeiten waren zum Ende des Berichtsjahres noch nicht abgeschlossen.

[116] Vgl. *http://www.dss.llv.li/*.
[117] Vgl. Art. 41 DSG.
[118] Vgl. 9.
[119] Bericht und Antrag Nr. 70 / 2008.

12. Ausblick

Das Berichtsjahr war durch wesentliche *Neuerungen* gekennzeichnet. Von zentraler Bedeutung waren die Arbeiten zu den beiden Teilrevisionen des DSG, welche 2009 fortgeführt und weitestgehend abgeschlossen werden sollen. Das Inkrafttreten *neuer Datenschutzbestimmungen*, wie beispielsweise die *Genehmigungspflicht für Videoüberwachungsanlagen*, wird uns mit Gewissheit auch in Anspruch nehmen.

Auf dem Weg zum Schengenbeitritt stellt die *Vorbereitung der Datenschutzevaluation* ein weiterer Meilenstein dar. In diesem Zusammenhang sind auch einige organisatorische Fragen zu beantworten. Es gilt, die vorhandenen Ressourcen wirksam einzusetzen.

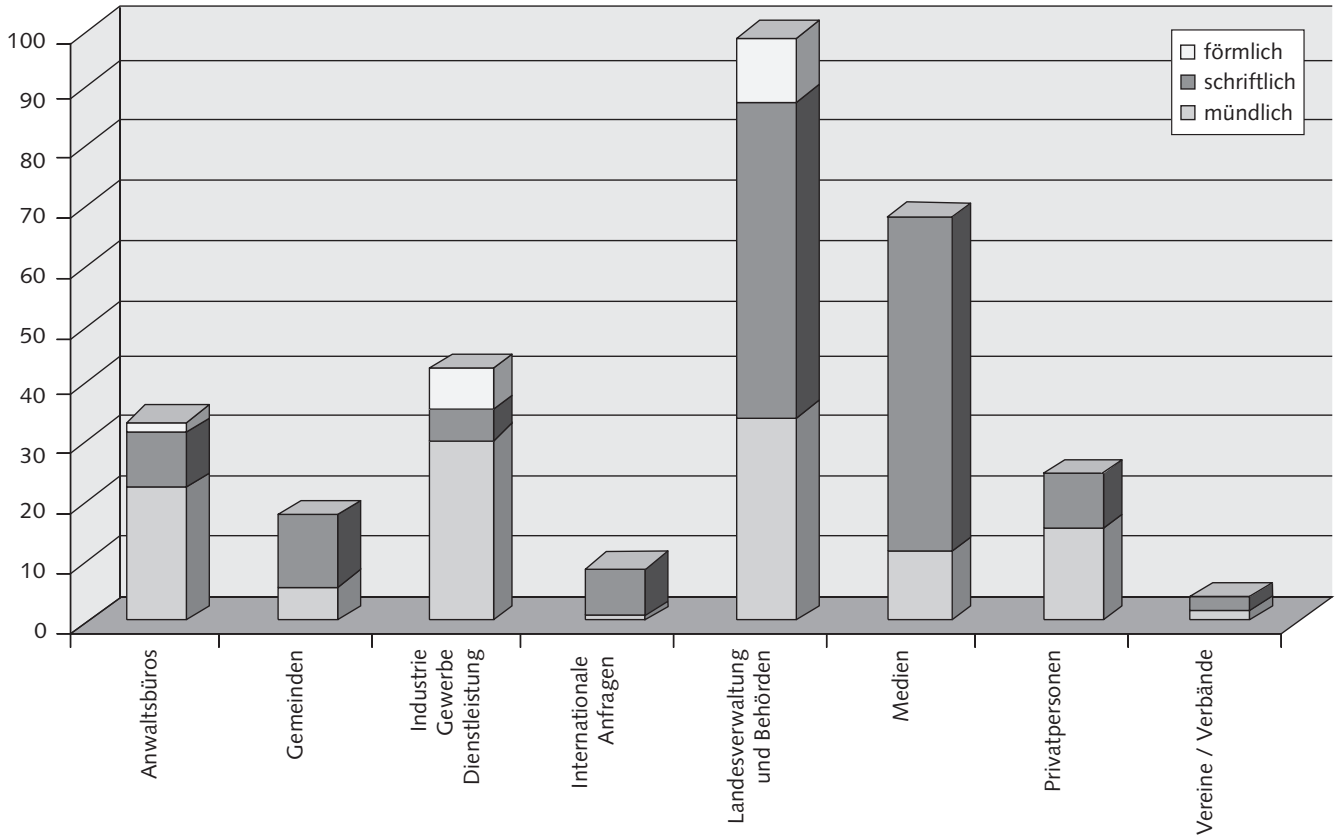
Nicht zuletzt aufgrund des Schengenbeitritts spielt die *Information der Öffentlichkeit* zu Themen rund um den Datenschutz weiterhin eine bedeutende Rolle. Der Auftakt hierfür soll die Durchführung einer *ersten grösseren Veranstaltung* anlässlich des Datenschutztages sein.

13. Anhang

13.1 STATISTIK

Im Berichtsjahr wurden insgesamt 316 registrierte Anfragen beantwortet. Von den 316 registrierten Anfragen wurden 126 mündlich, 156 schriftlich und 34 förmlich eingereicht. Die schriftlichen Anfragen reichten von kurzen Anfragen per E-Mail bis hin zu förmlichen Anfragen der Regierung, z.B. im Rahmen von Vernehmlassungsverfahren.

ANFRAGEN 2008



GESETZESTHEMEN

	Anwalts-büros	Gemein-den	Industrie, Gewerbe, Dienst-leistung	Inter-nationales	Landes-verwaltung und Behörden	Medien	Privat-personen	Vereine / Verbände	Gesamt-ergebnis
Allg. datenschutzrechtliche Fragen	3	1	7	4	13	36	2		66
Arbeitsbereich	4		5		2	6	1		18
Aussereuropäisches Recht					3				3
Datenbekanntgabe im Inland	2	11	3	1	30	1	8	2	58
Datenbekanntgabe m. Auslandsbezug	21	1	14	2	4				42
Geltendmachung gesetzlicher Rechte	2	1	1		7		6		17
Gesetzesvorhaben		1			34	1		1	37
Gesundheit und Soziales			1		1	1			3
Polizei und Sicherheit		3	6		3	6	1		19
Register der Datensammlungen			2						2
Technologischer Datenschutz	1		3		5	1	6	1	17
Telekommunikation	1		1		5	9	1		17
Umsetzung/Anwendung europ. Rechts				2	7	8			17
GESAMTERGEBNIS	**34**	**18**	**43**	**9**	**114**	**69**	**25**	**4**	**316**

13.2. DATENSCHUTZKOMMISSION

Die *Entscheidung der Datenschutzkommission des Fürstentums Liechtenstein (DSK)* vom 07. April 2008 zur **Videoüberwachung in der Fussgängerzone in Vaduz** stellt einen Grundsatzentscheid dar, der verfassungsrechtliche Anforderungen an den Staat zum Eingriff in die Privatsphäre wiedergibt.[120]

Zum Sachverhalt:
Auf Beschluss des Gemeinderats vom 29. August 2006 installierte die Gemeinde Vaduz Videokameras zur Überwachung der Fussgängerzone. Es fand rund um die Uhr eine flächendeckende Videoüberwachung durch 16 Kameras statt. In Bezug auf die gesetzliche Grundlage stützte sich die Gemeinde Vaduz hierbei auf Art. 52 Abs. 4 Gemeindegesetz.[121]

Auf Grund einer bei uns eingegangenen Beschwerde[122] hatte der DSB 2007 an die Gemeinde die Empfehlung abgegeben, die Videoüberwachung in der Fussgängerzone zu reduzieren, da nicht von einem verhältnismässigen Eingriff in die Privatsphäre ausgegangen werden könne. Ausserdem sei zu bezweifeln, dass Art. 52 Abs. 4 Gemeindegesetz eine hinreichend bestimmte Gesetzesgrundlage darstelle. Da die Gemeinde der Empfehlung nicht Folge leistete, legte der Datenschutzbeauftragte (DSB) die Angelegenheit der DSK zur Entscheidung vor.

Zu den Entscheidungsgründen:
Die flächendeckende Videoüberwachung der Fussgängerzone bewirkt einen erheblichen Eingriff in die grundrechtlich

[120] Die vollständige Entscheidung kann abgerufen werden unter: *http://www.llv.li/entscheidung_der_datenschutzkommission_zur_videoueberwachung_in_der_fussgaengerzone_in__vaduz.pdf.*
[121] Art. 52 Abs. 4 Gemeindegesetz besagt: «Er [der Gemeindevorsteher] steht der örtlichen Polizei vor und sorgt für Ruhe, Sicherheit und Ordnung. Er trifft die dazu nötigen Anordnungen und verhängt aufgrund gesetzlicher und ortspolizeilicher Vorschriften Bussen.»
[122] Vgl. Jahresbericht 2007.

geschützten Rechte auf Privatsphäre[123] und persönliche Freiheit[124] des einzelnen Passanten. Die flächendeckende Videoüberwachung eines öffentlichen Raums stellt schon deshalb einen erheblichen Eingriff in die Grundrechte der Privatsphäre und der persönlichen Freiheit dar, weil sie als Eingriff mit grosser Streubreite anzusehen ist, der verdachtsunabhängig alle Personen betrifft, die den überwachten Bereich betreten, ohne dass diese in einer Beziehung zu einem konkreten Fehlverhalten stehen bzw. den Eingriff durch ihr Verhalten veranlasst haben.[125]

Die Einschränkung eines Grundrechts ist nach Auffassung der DSK nur möglich, wenn sie auf einer gesetzlich Grundlage beruht, im öffentlichen Interesse liegt, verhältnismässig ist und den Kerngehalt des geschützten Rechtsguts nicht völlig aushöhlt. Diese Grundsätze gelten allein schon auf Grund der Europäischen Menschenrechtskonvention.

Die Generalklausel des Art. 52 Abs. 4 Gemeindegesetz als gesetzliche Grundlage wird von der DSK dementsprechend als nicht ausreichend empfunden, da eine flächendeckende Videoüberwachung eines öffentlichen Raums einen Eingriff von erheblichem Gewicht in die Privatsphäre und in das Grundrecht der persönlichen Freiheit darstellt und daher einer speziellen gesetzlichen Ermächtigung bedarf. Je grösser also die Intensität des Eingriffs ist, desto klarer müssen die Voraussetzungen dafür geregelt sein. Die DSK empfiehlt deshalb in ihrer Entscheidung die Schaffung einer spezialgesetzlichen Ermächtigung zur Videoüberwachung, da eine solche im Fürstentum Liechtenstein bisher nicht besteht und die Videoüberwachung eine immer grössere Rolle spielt.[126]

Das von der Gemeinde verfolgte öffentliche Interesse, für *Ruhe, Sicherheit und Ordnung* zu sorgen und konkrete Straftaten, wie beispielsweise Vandalismus und Sachbeschädigungen zu verhindern, sei zwar unbestritten. Dem *Verhältnismässigkeitsprinzip*[127] aber liegt der Gedanke zugrunde, dass ein *Eingriff* in ein Freiheitsrecht *nicht weitergehen darf, als das öffentliche Interesse es erfordert.* Die staatliche Massnahme *muss geeignet* sein, um den im öffentlichen Interesse *verfolgten Zweck* herbeizuführen. Die Massnahme muss im Hinblick auf den angestrebten Zweck zudem *erforderlich* sein, d.h. sie hat zu *unterbleiben,* wenn eine *gleich geeignete, aber mildere Massnahme* für den *angestrebten Erfolg ausreichen würde.* Der Eingriff darf in sachlicher, räumlicher und zeitlicher Beziehung *nicht über das Notwendige hinausgehen.*

Neben den Grundsätzen der Geeignetheit und der Erforderlichkeit muss eine Massnahme *zumutbar* sein, d.h. sie muss ein vernünftiges Verhältnis zwischen angestrebtem Ziel oder Zweck und Freiheitseingriff wahren.
Um die Verhältnismässigkeit überprüfen zu können, hatte der DSB schon im Vorfeld diverse Fragen an die Gemeinde Vaduz gerichtet. So ersuchte er um Auskunft, ob weniger weit gehende Massnahmen überprüft worden seien, ob der angestrebt Zweck nicht durch den gezielten, punktuellen Einsatz von Kameras auf bestimmte *«Hot Spots»* erreicht werden könne, zu wie vielen Schadensfällen es vor und nach Installierung der Videoüberwachung in der Fussgängerzone gekommen sei und in wie vielen Fällen die Videoaufzeichnung zur Aufklärung eines Sachverhalts gedient und zur Identifizierung des Täters beigetragen habe, etc. Diese Fragen konnten jedoch auch im Verfahren vor der DSK von der Gemeinde nur unzureichend beantwortet werden.

Die Datenschutzkommission bestätigt in ihrer Entscheidung daher die Empfehlung des Datenschutzbeauftragten, wonach die *flächendeckende und durchgehende* Überwachung entsprechend räumlich und/oder zeitlich auf das *notwendige Mass zu reduzieren* ist. Danach fragt sich insbesondere, ob eine 24 Stunden Überwachung an 7 Tagen in der Woche wirklich notwendig ist oder ob die Überwachung nicht auf bestimmte Tage sowie bestimmte Zeiten reduziert werden kann. Ausserdem ist zu überprüfen, ob nicht die gezielte *punktuelle Überwachung* bestimmter, im öffentlichen Interesse stehender Objekte ausreicht.

Anmerkung: Die Datenschutzkommission (DSK) ist neben uns eine weitere Instanz, die in strittigen Fällen zum Datenschutzrecht Entscheidungsbefugnis hat. Sie entscheidet gem. Art. 34 DSG als unabhängige Beschwerdeinstanz über

[123] Art. 32 Abs. 1 der liechtensteinischen Landesverfassung.
[124] Art. 8 Europäische Menschenrechtskonvention (EMRK).
[125] Vgl. Entscheidung des deutschen Bundesverfassungsgerichts vom 23.02.2007, Az. 1 BvR 2368/06.
[126] Vgl. 9, Gesetzesvorhaben zur zweiten Teilrevision des DSG.
[127] Vgl. Art. 4 DSG.

- Empfehlungen, die ihr von uns vorgelegt werden; und
- Beschwerden gegen Verfügungen von Behörden in Datenschutzfragen. Entscheidungen von Regierungen sind hiervon jedoch ausgenommen.

Die DSK besteht aus drei Mitgliedern und zwei Ersatzmitgliedern, die vom Landtag auf vier Jahre gewählt werden. Die letzte Wahl fand am 21. Juni 2006 statt (Mandatsperiode 2006–2010). Die Mitglieder der Kommission sind unabhängig und unterliegen den Bestimmungen des Gesetzes über die allgemeine Landesverwaltungspflege (LVG).

ABKÜRZUNGSVERZEICHNIS

aaO	am angegebenen Ort
ABGB	Allgemeines Bürgerliches Gesetzbuch
a. F.	alte Fassung
AGB	Allgemeine Geschäftsbedingungen
AHV-Nr.	Alters- und Hinterlassenenversicherungs-Nummer
AK	Amt für Kommunikation
BCR	Binding Corporate Rules (Verbindliche unternehmensinterne Datenschutzregelungen)
BCM	Business Continuity Management
DDoS	Distributed Denial of Service
DSB	Datenschutzbeauftragter
DSG	Datenschutzgesetz
DSK	Datenschutzkommission
DSV	Datenschutzverordnung
ECM	Enterprise Content Management
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDSK	Eidgenössische Datenschutzkommission
EG	Europäische Gemeinschaft
EMRK	Europäische Menschenrechtskonvention
ENISA	European Network and Information Society Agency
ESA	EFTA Surveillance Authority
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
FAQ's	Frequently Asked Questions (oft gestellte Fragen)
FMA	Finanzmarktaufsicht
GewV	Gewerbeverordnung
GPK	Geschäftsprüfungskommission
ICM	Integriertes Case Management
IP	Internet Protocol
IV	Invalidenversicherung
IVG	Invalidenversicherungsgesetz
IWGDPT	International Working Group on Data Protection in Telecommunications
KomG	Kommunikationsgesetz
KVG	Krankenversicherungsgesetz
LCO	Local Shared Objects
LLV	Liechtensteinische Landesverwaltung
LVG	Landesverwaltungspflegegesetz
PEID	Personenidentifikationsnummer
PGR	Personen- und Gesellschaftsrecht
PolG	Polizeigesetz
RAD	Regionaler ärztlicher Dienst
SDS	Stabsstelle für Datenschutz
SDÜ	Schengener Durchführungsübereinkommen
SIS	Schengener Informationssystem
SPG	Sicherheitspolizeigesetz
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
VKND	Verordnung über elektronische Kommunikationsnetze und Dienste
WP	Working Papers
WPPJ	Working Party on Police and Justice
ZPV	Zentrale Personenverwaltung

Datenschutzstelle
Kirchstrasse 8
FL-9490 Vaduz
Tel. +423 236 60 90
Fax +423 236 60 99
E-Mail: info@dss.llv.li
http://www.dss.llv.li