DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Tätigkeitsbericht 2011

Datenschutzstelle des Fürstentums Liechtenstein

INHALTSVERZEICHNIS

VORWORT

Dies ist unser 10. Tätigkeitsbericht.

Wir konnten wieder zahlreiche Anfragen von Behörden, Unternehmen und Bürgern beantworten – nach dem vergangenen Jahr wieder ein neuer Rekord an eingegangenen Fragen. Einige davon werden im Bericht ausführlich dargestellt, da sie aus unserer Sicht für die breite Öffentlichkeit von Interesse sind. Darüber hinaus war unsere Arbeit von folgenden Schwerpunkten gekennzeichnet:

Erneut war für uns die **Öffentlichkeitsarbeit** zentral: Der *Europäische Datenschutztag* stand unter dem Motto „Schau mal, wer da spricht"– Was Handys, Notebooks & Co alles erzählen. Dabei wurde der Datenschutz und die Mobilität bei der Nutzung von Handys, Notebooks und Tablet-PCs thematisiert.

Daneben nahmen wir aktiv an öffentlichen Veranstaltungen zu folgenden Themen teil: *„Der Zugriff des Staates auf private Daten am Beispiel der Vorratsdatenspeicherung"*, *„Gesundheitsrecht am Puls der Zeit – Der gläserne Patient"* und *„Content in the Cloud – wie Cloud Computing das betriebliche Informationsmanagement revolutioniert"*.

Seit gut zwei Jahren haben Behörden und Unternehmen die Möglichkeit, einen **Datenschutzverantwortlichen** zu benennen. Dies ist ein Instrument der Selbstregulierung und als solches zu begrüssen. Nachdem bis Anfang des letzten Jahres kaum ein Verantwortlicher bei uns gemeldet war, behandelten wir das Thema prioritär. In diesem Zusammenhang organisierten wir ein Treffen für die Datenschutzverantwortlichen und Personen, die am Thema interessiert waren. Wir möchten solche Veranstaltungen regelmässig durchführen.

Ausserdem schufen wir eine *Empfehlung zu den technischen und organisatorischen Massnahmen des Datenschutzes*, veröffentlichten einen Aufsatz zu *Cloud Computing* und aktualisierten verschiedene weitere Richtlinien.

Im Rahmen unserer **beratenden Funktion** setzten wir uns mit technischen Neuerungen wie *Google Analytics* und mit Entwicklungen im Rahmen von *Facebook* auseinander. Zudem gelangten wir an die Medienkommission und regten die Schaffung einer *Ombudsstelle für Medien* an. Grund dafür ist, dass in der Berichterstattung der Medien in Liechtenstein immer wieder leicht herauszufinden ist, um welche Person es sich handelt. Stattdessen sollte unserer Ansicht nach primär die Sache im Vordergrund stehen. Ausserdem äusserten wir uns zu umfassenden Fragen des *Datenschutzes am Arbeitsplatz*.

Im Zusammenhang mit der *Vorratsdatenspeicherung* waren wir weiterhin aktiv. So wiesen wir neben dem genannten Vortrag die Regierung darauf hin, dass gemäss der Rechtsprechung des deutschen Bundesverfassungsgerichts, aber auch gemäss der entsprechenden Richtlinie, ein Anpassungsbedarf der Strafprozessordnung besteht.

Im Rahmen unserer **internationalen Aufgaben** fand die *Schengen-Evaluation* statt. Liechtenstein ist seit Ende des letzten Jahres Schengen-Mitglied. Dies bedeutet für uns, dass wir insbesondere regelmässige Kontrollen durchführen müssen. Dies wurde bei der Evaluation gefordert.

Wir nahmen zu 24 **Gesetzesvorhaben** Stellung. Darunter befand sich im Rahmen einer neuerlichen *Revision des Datenschutzgesetzes (DSG)*, aber auch etwa die *Revision der Strafprozessordnung*, die durch die Umsetzung des Rahmenbeschlusses zum Datenschutz in der Dritten Säule notwendig wurde, oder die *Gesamtrevision des Versicherungsaufsichtsgesetzes*.

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

Vaduz, im April 2012

Dr. Philipp Mittelberger
Datenschutzbeauftragter

BERICHTERSTATTUNG 2011

Die Zahl der Anfragen, die an uns gerichtet werden, nimmt weiterhin zu. Im vergangenen Jahr wurden so viele Anfragen wie noch nie an uns gestellt. Im Jahr 2011 gingen insgesamt 559 Anfragen ein, was gegenüber dem Jahr 2010 eine leichte Zunahme bedeutet.[1] Die Zugriffszahlen auf unserer Internetseite stiegen ebenfalls von 54'682 auf 73'356, was einer Zunahme von über einen Drittel gleichkommt. Dies kann gewiss auf ein steigendes Bewusstsein für den Schutz der Privatsphäre zurückgeführt werden.

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

1. Fälle aus unserer Beratungspraxis

1.1. Wahrnehmung gesetzlicher Rechte/Beschwerden

Die hier aufgeführten Beispiele beschreiben einige wenige Fälle, welche auch in anderen Abschnitten behandelt werden könnten. Da es sich durchwegs um Fälle handelt, in denen sich besorgte oder betroffene Personen an uns wandten, sollen sie hier näher ausgeführt werden.

Das DSG sieht die Möglichkeit eines **Rechtsmittels** bei Verfügungen von Behörden in Datenschutzfragen vor. Uns ist nach wie vor[2] kein Fall bekannt, in dem auf diese Rechtsmittelmöglichkeit hingewiesen wird. Dies gilt auch für einen Fall, in dem sich eine Person gegen die zwangsweise Offenlegung ihres Lebenslaufes in einem Kurs des Arbeitsmarktservices wehrte. Obwohl es hier explizit um ein Datenschutzanliegen ging, enthielt die in diesem Zusammenhang ergangene Verfügung keinen entsprechenden Rechtsmittelhinweis. Ausserdem wurde in der Verfügung nicht begründet, weshalb die Offenlegung eines Lebenslaufes in einem Kurs Pflicht sein soll. Es bleibt abzuwarten, wie das Verfahren weitergeht, da gegen die Verfügung bei der Regierung Beschwerde eingereicht wurde.

In der Landesverwaltung besteht eine zentrale Datenbank, die zahlreiche Personendaten, insbesondere über die gesamte Bevölkerung, enthält. Sie wurde Ende der Neunzigerjahre geschaffen und dient für andere Datenbanken als Basis. Seit 2003 forderten wir die Schaffung einer rechtlichen Grundlage für dieses wichtige Arbeitsinstrument.[3] Dem wurde nun mit der Schaffung eines Gesetzes über das **Zentrale Personenregister** endlich nachgekommen. Möglicherweise wurden in diesem Zusammenhang einzelne **Auskunftsbegehren** an die Landesverwaltung gestellt, mit denen sich Betroffene darüber erkundigen wollten, welche Amtsstellen welche Daten über sie bearbeiten. Wir wurden vereinzelt von Amtsstellen kontaktiert, die sich nach einer korrekten und gesetzmässigen Antwort erkundigten.

Bei einem Unternehmen waren **versehentlich Kunden** per **E-Mail** so angeschrieben worden, dass letztere für die **anderen Adressaten** ersichtlich waren. Daraufhin kontaktierte uns dieses Unternehmen, um uns diesen Fehler mitzuteilen. Wir konnten dahingehend beraten, wie solche Vorfälle in der Zukunft vermieden werden könnten.[4] Offenbar war diese E-Mail auch an das Liechtensteiner Volksblatt gegangen. Bei uns ging eine Meldung ein, wonach Empfänger der Mailliste danach auch vom Volksblatt zu Werbezwecken kontaktiert wurden. Aus diesem Anlass richteten wir einige Fragen an das Volksblatt. Die Antwort war nicht sehr aufschlussreich, sondern warf weitere Fragen auf, die in der Folge – und trotz unseres Hinweises auf die gesetzlichen Bestimmungen – unbeantwortet blieben. Einerseits konnte auf Grund der Kontaktaufnahme des von der Datenpanne betroffenen Unternehmens mit uns die Sache einfach und kooperativ geregelt werden. Andererseits ist es bedauernswert, wenn trotz Hinweis auf die Einhaltung gesetzlicher Bestimmungen nicht in einem befriedigenden Mass reagiert wird. Schliesslich

1 2010 waren es 523, vgl. dazu Details im Anhang.
2 Vgl. Tätigkeitsbericht 2010, II, 1.1. und Art. 34 DSG.
3 Vgl. schon Tätigkeitsbericht 2003, 4.1.2.
4 Gegenständlich wurde für die Versendung eines Newsletters ein E-Mail -Programm verwendet. Aus unserer Sicht hat diese Vorgehensweise zwei kritische Schwächen:
1.) Bei einer manuellen Übernahme (z.B. durch Kopieren/Einfügen) einer E-Mail-Empfängerliste von einer Applikation in eine andere, wobei die Zielfelder (z.B. die Outlook-Adressfelder „An", „Cc" oder „Bcc") durch den Benutzer frei bestimmt werden können, fehlt es an jeglichem Kontrollmechanismus. Erlassene Regelungen und Vorgaben können auf diese Weise vom Benutzer weder erzwungen noch kontrolliert werden;
2.) Bei unsachgemässer Handhabung von „Bcc" können vertrauliche Informationen oder Personendaten für nicht bestimmte Adressaten bekannt gegeben werden. Dies insbesondere, da in den technischen Ausführungen (RFC-5322) festgehalten ist, dass grundsätzlich, jedoch nicht zwingend, entsprechende Implementierungen dieses Feld für das Senden von Nachrichten an Empfänger auf eine solche Weise verwenden sollen, dass die Empfängerliste für die Adressaten nicht sichtbar ist.

wäre ein gesetzgemässer Umgang mit Kundendaten im Interesse aller. Es bleibt zu wünschen, dass es sich dabei um einen Einzelfall handelt.

Ein ehemaliger Kunde eines **Personalvermittlungsbüros** beschwerte sich bei uns, dass seinem Antrag auf **vollständige Löschung** seiner Daten nicht nachgekommen wurde. Er hatte ausdrücklich einer weiteren Bearbeitung seiner Personendaten durch das Personalvermittlungsbüro widersprochen.

Wir haben dem Verantwortlichen des Personalvermittlungsbüros als Datenbearbeiter mitgeteilt, dass auch eine einmal erteilte *Einwilligung jederzeit und vollumfänglich widerrufen* werden kann. Ein entsprechendes Verbot ist grundsätzlich zu beachten und hat nur ausnahmsweise bei Vorliegen eines anderweitigen Rechtfertigungsgrundes zurückzustehen.[5] Im gegenständlichen Fall hat das Personalvermittlungsbüro jegliche weitere Bearbeitung der den Widerspruchsführer betreffenden Daten zu unterlassen, dies vor allem in Bezug auf interne Akten und Bearbeitungsvermerke. Ausgenommen ist die blosse Dokumentation des Widerspruchsrechts.

1.2. Technologischer Datenschutz

Im **Interne**t sind zahlreiche freie Dienste für E-Mails, soziale Netzwerke, Blogs usw. verfügbar. Gemeinsam ist sämtlichen **Diensten**, dass sich der Benutzer im Vorfeld für den jeweiligen Dienst **registrieren** muss. Es kommt immer wieder vor, dass bestehende Benutzerkonten solcher Dienste **„verwaisen"**, da sie aus irgendwelchen Gründen nicht mehr benutzt werden. In diesem Zusammenhang wurde die Frage an uns gerichtet, was mit E-Mail-Konten geschieht, welche durch den Benutzer über eine bestimmte Zeit nicht mehr verwendet werden und was insbesondere mit den dort eingegebenen personenbezogenen Daten passiert. Die Speicherdauer und der Umgang von „verwaisten" Nutzerkonten hängen stark vom verwendeten Service-Provider und Dienst ab.

Als hilfreiche Quelle zur Klärung der gegenständlichen Fragen sind die jeweiligen *Nutzungsbedingungen* bzw. die *Datenschutzerklärungen* zu nennen. In den Nutzungsbedingungen zu *Google* Mail findet sich z.B. folgender Absatz: *„Bitte beachten Sie, dass verbleibende Kopien von gelöschten Nachrichten und Konten bis zu 60 Tage auf unseren aktiven Servern verbleiben können, bis sie gelöscht werden, und eventuell auf unseren Offline-Sicherungssystemen erhalten bleiben."*[6] Eine entsprechende Erklärung findet sich auch beim freien E-Mail-Serviceanbieter Yahoo!: *„Wenn Accounts vier Monate nicht genutzt wurden, gelten sie als inaktiv und werden deaktiviert und dann gelöscht."*[7] Auch bei anderen Anbietern finden sich vergleichbare Regelungen. Grundsätzlich empfehlen wir, nicht bis zur automatischen Deaktivierung durch den Plattformbetreiber zuzuwarten, sondern die Daten *aktiv und bewusst zu löschen* und nicht mehr benötigte Benutzerkonten zu *deaktivieren*.

Keine automatische *Löschung von inaktiven Nutzerkonten* existiert derzeit beim grössten sozialen Netzwerkanbieter, *Facebook*. Die Datenschutzbehörde in Irland führte eine Kontrolle bei Facebook durch, wobei die Datenlöschung inaktiver Konten ebenfalls thematisiert wurde. Die Nutzer von Facebook können wählen, ob sie deren Konto deaktiviert oder gelöscht haben wollen.[8] Falls das Konto auf der „Sicherheitseinstellungen"-Seite deaktiviert wird, ist das Profil und alle damit verbundenen Informationen auf der Internetseite von Facebook nicht mehr sichtbar. Einige Informationen, z.B. die verschickten Nachrichten, sind unter Umständen jedoch weiterhin für andere zugänglich. Bei einer Deaktivierung des Kontos ist das *Reaktivieren zu einem späteren Zeitpunkt* möglich, da Facebook Profilinformationen (Freunde, Fotos, Interessen usw.) nicht vollständig löscht, sondern auf unbestimmte Zeit vorrätig hält. Verlangt der Nutzer von Facebook die Löschung seines Kontos, ist eine spätere *Reaktivierung* nicht möglich. Im Bericht zur Datenschutzprüfung wird festgestellt, dass die Löschung insbesondere von geteilten

5 Ein solcher Rechtfertigungsgrund ist insbesondere gegeben, wenn sich der Bearbeiter zum Beispiel auf ein gesetzliches Recht berufen kann oder gar einer Bearbeitungspflicht untersteht. Nur in diesem Ausnahmefall darf der Datenbearbeiter entgegen des ausdrücklichen Widerspruchs der betroffenen Person die Daten im notwendigen Umfang weiter bearbeiten.

6 http://mail.google.com/support/bin/answer.py?hl=de&answer=8152 Weiters findet sich in den Google-Mail-Programmrichtlinien folgender Satz unter Kontoaktivität: „Google löscht Ihr Konto in Übereinstimmung mit den Nutzungsbedingungen, wenn Sie sich über einen Zeitraum von neun Monaten nicht in Ihrem Konto anmelden."

7 http://help.yahoo.com/l/de/yahoo/mail/yahoomail/account/account-04.html.

8 http://www.facebook.com/help/?faq=224562897555674.

Inhalten, wie z.B. von Gruppen oder Nachrichten, die mehreren Benutzern gemeinsam gehören, nicht in allen Fällen ordnungsgemäss funktioniert. Facebook wurde von der Datenschutzbehörde in Irland aufgefordert, robuste Mechanismen zur Kontolöschung auszuarbeiten und so rasch als möglich zu implementieren.[9]

Wir bekamen eine Anfrage einer Person (A), die nicht Mitglied von Facebook war, und eine E-Mail mit folgendem Inhalt von Facebook bekam: *„B möchte dein Freund bei Facebook sein. […] Facebook kann dir helfen mit ihnen [Anmerkung: Familie und Freunden] in Kontakt zu bleiben.“* B hatte A mehrere Monate zuvor via Facebook eine Einladung zu einer Veranstaltung gesendet. Die Kontaktdaten von A wurden offensichtlich über längere Zeit von Facebook aufbewahrt und für die Versendung der gegenständlichen Mitgliedschaftseinladung zu einem späteren Zeitpunkt zweckentfremdet. Eine Rückfrage bei der zuständigen Datenschutzbehörde in Irland ergab, dass Facebook auch Kontaktinformationen von Nichtmitgliedern sammelt und speichert. Dies indem z.B. die E-Mail-Adressen von über Facebook verschickten Einladungen zu Veranstaltungen vorrätig gehalten oder Kontaktinformationen in den Adressbüchern der Mobiltelefone und den E-Mail-Postfächern der Mitglieder ausgelesen werden. Nach der Übertragung der Kontaktdaten an Facebook werden diese unter anderem für die Versendung von Einladungen an Nichtmitglieder verwendet.[10] Bezeichnet wird diese Art der offensiven Mitgliederwerbung **„Freunde finden“** *(engl. friend finder)* sowie „**Personen, die du vielleicht kennst**“ *(engl. people you may know)*.

Die Datenschutzbehörde in Irland informierte sich auf Grund unserer Anfrage bei Facebook und klärte die Zusammenhänge zwischen Veranstaltungseinladungen an Nichtmitglieder und der Funktion „Freunde finden“ ab. Wir bekamen daraufhin die Rückmeldung, dass zukünftig bei Einladungen zu Veranstaltungen für den Empfänger und Nichtmitglied von Facebook die Möglichkeit besteht, Facebook die anderweitige Nutzung seiner E-Mail-Adresse zu untersagen.

Welche Daten hat Facebook über ein Mitglied gesammelt? Mit der Funktion **„Lade deine Informationen herunter“**[11] kann durch ein Mitglied ein Auskunftsbegehren bei Facebook angestossen werden. Facebook stellt daraufhin die gespeicherten Informationen[12] in einem Archiv zusammen und informiert den Nutzer in weiterer Folge per E-Mail über die Möglichkeit des Downloads. Die irische Datenschutzbehörde fordert den Ausbau dieser Funktionalität sowie die Ausweitung auf andere von Facebook gespeicherten Datenkategorien.[13] Der Bericht der irischen Datenschutzbehörde ist ein erster Schritt zur Prüfung von Facebook. Wir werden die Weiterentwicklung verfolgen.

Mehrere Anfragen betrafen die Vergabe von Passwörtern. Wie sieht ein **sicheres Passwort** aus? Abhängig vom Einsatzzweck sowie begleitenden Umständen wird die Antwort variieren. **Merkmale** eines guten Passworts sind zumindest: Es besteht aus mindestens acht Zeichen; aus Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen. Für unterschiedliche Dienste sollten verschiedene Passwörter verwendet werden. Gute Passwörter schützen nicht nur vor unberechtigtem Zugriff auf Daten und Systeme, sondern verhindern zudem, dass Dritte IT-Systeme unter dem Namen und der Identität einer anderen Person nutzen können (Identitätsdiebstahl).[14] Passwörter sind jedenfalls geheim zu halten, sollten nicht niedergeschrieben werden, gehören regelmässig geändert und nicht mit Dritten geteilt, Initial-Passwörter sollten beim ersten Anmeldevorgang sowie bestehende Passwörter bei Anzeichen einer missbräuchlichen Verwendung sofort geändert werden. Mit einem *Passwort-Check*[15] kann die Qualität eines Passworts überprüft werden.

9 Report of Audit, 21. Dezember 2011, http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf, S. 113 ff.

10 http://www.llv.li/amtsstellen/llv-dss-spezialthemen/llv-dss-spezialthemen-soziale-netzwerke.htm.

11 „Lade eine Kopie deiner Facebook-Daten herunter.“, https://www.facebook.com/settings.

12 Daten zur Erstellung sowie Re- und Deaktivierung des Kontos, Anmelde- und Abmeldeinformationen, vorherige Namen, Fotos, Beiträge, Nachrichten, Freundeslisten, erhaltene und gesendete Freundschaftsanfragen, Chat-Konversationen, Informationen zu Veranstaltungen, Familienangaben, Infos zum Anstupsen (engl. pokes), Infos zum Beziehungsstatus, Mobiltelefonnummern usw.

13 Report of Audit, 21. Dezember 2011, http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf, S. 63ff.

14 Vgl. Dirk Fox, Frank Schaefer in DuD: Datenschutz und Datensicherheit, Ausgabe 7/2009, S. 425 ff.

15 Auf unserer Internetseite kann unter „Selbstdatenschutz“ ein Passwortcheck durchgeführt werden.

Google Analytics[16] ist ein kostenloser Dienst von Google Inc., mit dem Daten zum Nutzungsverhalten von Besuchern auf Internetseiten gesammelt und ausgewertet werden können. So wird unter anderem gespeichert, woher die Besucher kommen, welche Inhalte auf einer Internetseite aufgerufen und wie oft bzw. wie lange welche Unterseiten und Kategorien betrachtet werden. Google erzeugt aus den gesammelten Daten fortlaufend detaillierte Besucherstatistiken, die in weiterer Folge den Betreibern der Internetseiten anhand von „Reports" zur Verfügung gestellt werden. Die Auswertung und Aufbereitung der „Reports" findet hauptsächlich in den USA statt. Die Nutzungsbedingungen verpflichten die Betreiber der jeweiligen Internetseite zu einer entsprechenden Informationspflicht gegenüber den Internetseitenbesuchern, indem unter anderem darauf hingewiesen wird, dass *„sie […] ferner verpflichtet [sind], an prominenten Stellen ihrer Websites eine sachgerechte Datenschutzpolicy zu dokumentieren (und sich an diese zu halten). Auch werden sie alle zumutbaren Anstrengungen unternehmen, die Aufmerksamkeit der Nutzer ihrer Website auf [diese] Erklärung zu lenken […]"*.[17] Diese „Datenschutzpolicy" sowie ein Hinweis auf die Nutzung von Google Analytics fehlt häufig, wodurch es für Seitenbesucher nicht offensichtlich erkennbar ist, dass deren Surfverhalten an Google zur Auswertung übertragen wird. Neben der Informationspflicht sind für Seitenbetreiber weitere Punkte für den datenschutzfreundlichen Einsatz zu beachten.[18]
Zudem stellt das Produkt *„Piwik"* eine datenschutzfreundliche Alternative zu *„Google Analytics"* dar.[19]

1.3. Telekommunikation

Im Bereich der Telekommunikationsgesetzgebung haben uns weiterhin hauptsächlich die **Vorratsdatenspeicherung** sowie **Anfragen zu Teilnehmerdaten** beschäftigt.[20] Auf Grund der Wichtigkeit und europaweiten Aktualität dieser Thematik haben wir Datenschutz-Kontrollen im Sinne des Kommunikationsgesetzes (KomG) in die Wege geleitet.[21]

1.4. Gesundheit und Soziales

In der Vergangenheit hatten wir eine **Analyse über die Datenströme im Bereich der Sozialleistungen** angeregt, die im Landtag befürwortet wurde.[22] In diesem Zusammenhang ist auch die letztjährige *Revision des Sozialhilfegesetzes* zu sehen, die durch uns initiiert worden war. Mit dieser Revision wurden verschiedene Datenschutzbestimmungen geschaffen, die auch die Datenbekanntgabe – und damit zum Teil den Datenfluss – ausdrücklich regelt.[23] Bereits 2005 wurde eine *Analyse zum Sozialstaat Liechtenstein veröffentlicht.* Diese beschränkt sich nicht auf die Leistungen im sozialen Bereich im engeren Sinn, sondern ist übergreifend. Dargestellt werden 25 staatliche Leistungen, die von verschiedenen Seiten ausgeschüttet werden. Eine Analyse der Datenflüsse würde sich als sehr komplex erweisen. Diese Komplexität des Systems wurde auch durch die *Interpellationsbeantwortung der Regierung betreffend den Sozialmissbrauch* aufgezeigt.[24] Die Interpellation stellt unter anderem folgende Frage: „Gibt es betreffend Datenschutz Hürden, welche die Zusammenarbeit zwischen staatlichen Stellen, welche Sozialleistungen erbringen, erschweren oder verunmöglichen?"

Die Beantwortung fällt dahingehend aus, dass es im Bereich Gesundheit keine Hürden gibt, während sie im Bereich Soziales grossteils als gerechtfertigt erachtet werden. Dennoch gehen verschiedene Möglichkeiten der Verbesserung der Situation aus der Beantwortung hervor. So wäre es aus Sicht der AHV-IV-FAK Anstalten allenfalls sinnvoll, durch eine eigens dafür eingesetzte *Fachgruppe* (zuständige Ressorts/Praktiker/Datenschutzstelle) Lösungsmöglichkeiten erarbeiten zu lassen. Aus unserer Sicht sollte auch die Schaffung eines mit dem Schweizerischen Bundesgesetz über den *Allgemeinen Teil des Sozialversicherungsrechts* (ATSG) vergleichbaren Gesetzes geprüft werden. Wir hatten in einer Beant-

16 http://www.google.com/analytics/.
17 http://www.google.com/analytics/tos.html; vgl. 8.1.
18 Vgl. http://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_Webseitenbetreiber_in_Hamburg.pdf.
19 http://de.piwik.org/blog/2011/03/unabhangiges-landeszentrum-datenschutz-uld-piwik-datenschutzkonform-einsetzbar/. Vgl. https://www.datenschutzzentrum.de/presse/20110315-piwik.htm; Anders als bei vielen anderen Produkten zur Webanalyse findet die Verarbeitung hier nicht bei einer anderen Stelle oder bei einem Auftragsdatenverarbeiter statt, sondern auf dem Rechner des Webseitenanbieters selbst.
20 Art. 52 ff. und Art. 53 Abs. 2 KomG.
21 Art. 52b KomG.
22 Vgl. dazu Tätigkeitsbericht 2010, II. 1.1. und Landtagsprotokoll 19.5.2011 Seite 724 ff.
23 Vgl. Art. 26a ff. Sozialhilfegesetz.
24 Vgl. Bericht und Antrag Nr. 96/2011 und sowie das Protokoll zur Landtagssitzung vom 19. bis 21. Oktober 2011, http://www.landtag.li/Protokolle/xsl/Landtagsprotokoll_2011_10_19.pdf (Seite 1535).

wortung der Interpellation angegeben, dass auch *Richtlinien* für die Praxis geschaffen werden könnten. Dies jedoch erst nach der eingangs erwähnten Analyse der Sozialdatenflüsse. Wir sind nach wie vor für die Schaffung von praktikablen Lösungen, die den Gesetzen entsprechen. So stehen wir in Kontakt mit den AHV-IV-FAK Anstalten in Bezug auf *Grundsatzkontrollen* im Bereich der *Ergänzungsleistungen*.

Im Bereich der Brustkrebsvorsorge war seitens der FBP ein **Postulat** eingereicht worden. Insbesondere wurde darin eine mögliche **Teilnahme** liechtensteinischer Frauen am **Mammografie Screening Programm** des Kantons St. Gallen näher beleuchtet. Anlass war eine hohe Zahl der Brustkrebsmortalität liechtensteinischer Frauen. Bei den Mammographie Screening Programmen werden Frauen nach bestimmten Kriterien erfasst und zu gezielten Untersuchungen eingeladen. Diese Programme bezwecken die Senkung der Mortalität, der Gewinn von sonst verlorenen gesunden Lebensjahren und weniger grosse chirurgische Eingriffe bis zur Brustentfernung. Wir wurden zur Postulatsbeantwortung aus Datenschutzsicht angefragt. Hinsichtlich der Organisation der Einladungen kommen mehrere Möglichkeiten in Frage. Beispielsweise kann diese über das Amt für Gesundheit erfolgen, welches bereits derzeit Personendaten für ähnliche Zwecke bearbeitet. Bei einer Einladung der liechtensteinischen Patientinnen über die Krebsliga St.Gallen Appenzell müsste diese Namen, Wohnort und Alter der potenziellen Klientel erhalten, wofür erst eine gesetzliche Grundlage geschaffen werden müsste. Noch sind viele Fragen offen, insbesondere hinsichtlich der weiteren Bearbeitung der medizinischen Daten durch die Krebsliga.

Die Arbeitsgruppe elektronisches Gesundheitsnetz, in der wir vertreten sind, bekam den Auftrag der Erarbeitung einer **eHealth-Strategie für Liechtenstein** auf Basis der eHealth-Strategie Schweiz mit den Schwerpunkten *Gesundheitskarte* inklusive Anwendungen (mittelfristige Perspektive) sowie *ePatientendossier* (langfristige Perspektive). Die Strategie eHealth der Schweiz aus dem Jahr 2007 definiert eHealth als „den integrierten Einsatz von Informations- und Kommunikationstechnologien (IKT) zur Gestaltung, Unterstützung und Vernetzung aller Prozesse und Teilnehmer(innen) im Gesundheitswesen" bzw. ein „Anwendungskonzept zur Positionierung von IKT im Gesundheitswesen". Dabei wird der Informationssicherheit und dem Datenschutz höchste Priorität beigemessen,[25] dem kann nur zugestimmt werden. Die Artikel-29-Arbeitsgruppe äusserte sich im Übrigen bereits 2007 zum Thema Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA).[26] Selbst wenn es nicht um genau dasselbe Thema geht: Dennoch gilt die für EPA gemachte Hauptaussage auch für eine künftige eHealth Lösung in Liechtenstein: Die *ausdrückliche Einwilligung* der Patienten sollte eine grosse Rolle spielen. Weiters ist die Gewissheit, dass die Vertraulichkeit und der Schutz ihrer persönlichen Daten von allen medizinischen Fachkräften auch im EPA konsequent gewahrt werden, zentral. Auf den Aspekt differenzierter Zugriffsberechtigungen in diesem Zusammenhang wiesen wir im Rahmen einer Veranstaltung der Privaten Universität Triesen hin.[27]

1.5. Polizei, Sicherheit und Justiz

Wie bereits im Ausblick des letzten Tätigkeitsberichts angekündigt, war es im Frühjahr 2011 soweit und die **Schengen Datenschutz-Evaluation** wurde durchgeführt:[28]

Im schriftlichen Verfahren wurde von „Brüssel" zunächst ein umfassender Fragebogen an die befassten Stellen zur Beantwortung geschickt. Dabei ging es vor allem darum, den Nachweis zu erbringen, dass Liechtenstein die rechtlichen Rahmenbedingungen geschaffen und die Vorgaben umgesetzt hat. Dann galt es, zu überprüfen, inwieweit die schriftlichen Ausführungen in die Praxis umgesetzt worden sind. Diese Prüfung fand im April 2011 statt. Dabei mussten wir einem international zusammengesetzten Expertenteam Rede und Antwort stehen. Verschiedene Aspekte, wie unsere Unabhängigkeit, Struktur oder gesetzlichen Aufgaben und Kompetenzen sowie die Rechte der Bürger wurden geprüft. Unsere Unabhängigkeit war bereits durch die Zuordnung zum

25 Vgl. Strategie „eHealth" Schweiz, S. 12 und 15, unter http://www.e-health-suisse.ch

26 Vgl. Tätigkeitsbericht der Stabsstelle für Datenschutz 2007, 7.1.: http://www.llv.li/pdf-llv-sds-taetigkeitsbericht_2007.

27 Vgl. 2.1.

28 Vgl. Tätigkeitsbericht 2010, III. Da der Kern der Abkommen von „Schengen" und „Dublin" im Zugriff liechtensteinischer Behörden auf Tausende von Datensätzen besteht, müssen diese entsprechend geschützt werden. Um den Schutz dieser Daten zu gewährleisten, müssen sich die Beitrittskandidaten im Vorfeld eines Beitritts einer Evaluation unterziehen. Mit dieser wird die „Schengen-Reife" eines Beitrittslandes geprüft.

Landtag, welche im Hinblick auf den bevorstehenden Schengen-Beitritt erfolgt war, gestärkt worden.

Neben der Datenschutzstelle wurden auch die datenschutzrelevanten Aspekte der *Polizeikooperation* sowie der *Visa-Angelegenheiten* beim Ausländer- und Passamt evaluiert. Insgesamt verlief die Evaluation positiv, was in einem Bericht festgehalten wurde. Im Evaluationsbericht wurden auch Empfehlungen festgehalten, die Liechtenstein umsetzen muss. Eine Empfehlung besteht beispielsweise darin, eine Informationskampagne im Zuge des Schengenbeitritts durchzuführen, um die breite Bevölkerung über dieses Thema und insbesondere über ihre damit verbundenen Rechte zu informieren. Zudem hielten die Experten fest, dass wir in der Datenschutzstelle zusätzliche Ressourcen benötigen, um den neuen und zusätzlichen Aufgaben nachkommen zu können.

Ein weiterer Pfeiler der internationalen polizeilichen Zusammenarbeit stellt der Abschluss eines **Abkommens mit dem Europäischen Polizeiamt, Europol,**[29] dar. Bereits 2008 waren diesbezüglich erste Gespräche geführt worden. Europol wurde gegründet, um die Arbeit der Nationalen Polizeibehörden Europas zu koordinieren und deren Informationsaustausch untereinander zu fördern. Es soll eine engere und effizientere Zusammenarbeit der Mitgliedstaaten bei der Verhütung und Bekämpfung der internationalen Kriminalität ermöglichen. Nachdem ein Fragebogen zu den gesetzlichen Rahmenbedingungen an die Landespolizei ergangen war, den wir gemeinsam beantwortet hatten, fand im Mai 2011 eine **Datenschutzevaluation** vor Ort statt. Dabei wurden Theorie und Praxis zu den schriftlichen Ausführungen von Experten geprüft. Neben der Unabhängigkeit und den Befugnissen der Datenschutzstelle war auch die Abänderung des DSG, nach der in Zukunft hängige Straf- und Rechtshilfeverfahren nicht mehr vom Anwendungsbereich des DSG ausgenommen werden sollen, von zentralem Interesse.[30]

Das DSG sieht für **Videoüberwachungen** im öffentlichen Raum eine **Genehmigungspflicht** vor.[31] Gemäss Art. 6a Abs. 7 DSG sind die hierbei aufgezeichneten Daten „unverzüglich, spätestens jedoch nach 30 Tagen zu löschen, wenn a) sie zur Erreichung des Zwecks nicht mehr erforderlich sind; oder b) schutzwürdige Interessen der betroffenen Personen einer weiteren Aufbewahrung entgegenstehen." Wir hatten in den verfügten Genehmigungen die im Gesetz genannte **30-Tage-Speicherfrist** so ausgelegt und angewandt, dass die 30-Tagesfrist als eine ab Speicherbeginn laufende, in jedem Fall geltende, d.h. bedingungslose bzw. absolute Höchstfrist zu verstehen ist. Aus diesem Grund hatten wir alle Anträge, die eine längere Speicherdauer vorsahen, auf diese 30 Tage als maximale Frist begrenzt.

Gegen diese Begrenzung hatten vier Antragsteller bei der Datenschutzkommission (DSK) Beschwerde eingelegt, mit dem Argument, dass die 30 Tage erst mit Eintritt einer der in Bst. a) oder b) genannten Bedingungen zu laufen beginne und somit Speicherfristen von über 30 Tagen zulässig und auch notwendig seien.[32] Die DSK hat in allen Fällen unsere Auslegung und Anwendung bestätigt, wonach die 30-Tagesfrist als absolute Höchstfrist zu verstehen ist, und die Beschwerden insofern abgewiesen: *„Zusammenfassend ist festzuhalten, dass insbesondere die systematische, einschliesslich der verfassungskonformen, die rechtsvergleichende und die teleologische Auslegung des Art. 6a Abs. 7 DSG eindeutig zum Ergebnis führen, dass die 30-Tagesfrist als bedingungsunabhängige, in jedem Fall geltende absolute Höchstfrist zu verstehen ist. Tritt demzufolge nicht bereits vorher eine der in lit. a) oder b) geregelten Alternativbedingungen ein, sind gespeicherte Daten spätestens nach 30 Tagen ab Speicherbeginn zu löschen."*[33]

29 Kern auch dieses Abkommens ist der Zugriff der Polizei auf Tausende von Datensätzen, welche entsprechend geschützt werden müssen. Wie auch bei den Abkommen zu Schengen und Dublin ist die Prüfung der Sicherstellung eines angemessenen Datenschutzes wichtig.

30 Vgl. 3.

31 Zur Videoüberwachung allgemein vgl. Tätigkeitsbericht 2010, 1.5

32 Es wurden Speicherfristen zwischen 60 Tagen und zwei Jahren beantragt.

33 Vgl. beispielgebend die Entscheidung der DSK vom 26.01.2011, DSK 2010/4, S. 24, http://www.llv.li/pdf-llv-dss-entscheid_dsk_2010-4_public.pdf.

1.6. Wirtschaft und Finanzen

Die **Bearbeitung von Personendaten** im Auftrag („Outsourcing") hat in den letzten Jahren stark an Bedeutung gewonnen. In diesem Zusammenhang waren wir auch verstärkt mit Fragen rund um das sogenannte **Cloud Computing**[34] konfrontiert, welches aus rechtlicher Sicht eine Auftragsdatenbearbeitung darstellt. Gerade im grenzüberschreitenden Dienstleistungssektor, aber auch bei Behörden ist die Auftragsdatenbearbeitung mittlerweile zum Alltag geworden. Cloud Computing ist eher eine Evolution als eine Revolution. Es geht somit nicht um etwas grundsätzlich Neues, sondern um die Weiterentwicklung bestehender Technologien. Richtig verstanden und gemäss den in Liechtenstein geltenden Datenschutzbestimmungen und den Bedürfnissen der Unternehmen eingesetzt, kann Cloud Computing einen wichtigen Wettbewerbsvorteil bringen.[35] Durch die Nutzung von Cloud Diensten entstehen jedoch spezifische Risiken, da von den Cloud-Anwendern *Computerressourcen genutzt werden*, auf die sie selbst keinen direkten Zugriff bzw. über die sie *keine Kontrolle* haben.

Das DSG regelt die Voraussetzungen, unter denen eine Datenbearbeitung im Auftrag zulässig ist: Entscheidend ist, dass der Auftraggeber immer für die Daten und deren rechtmässige Bearbeitung verantwortlich bleibt mit der Folge, dass gegen ihn Haftungsansprüche nicht nur auf Grund seines eigenen Verhaltens, sondern auch auf Grund des Verhaltens des Auftragsbearbeiters möglich sind. Der Auftraggeber hat daher Sorge dafür zu tragen, dass der Auftragsdatenbearbeiter die Personendaten nur so bearbeitet, wie er es selbst tun dürfte. Cloud-Computing-Systeme müssen somit bestimmten infrastrukturellen Rahmenbedingungen unterliegen und den Schutzzielen Verfügbarkeit, Vertraulichkeit, Integrität, Revisionssicherheit und Transparenz genügen. Schon allein aus diesem Grund empfiehlt es sich, eine *vertragliche Vereinbarung* zu treffen, in der nicht nur die Datenbearbeitung an sich, sondern auch die Datensicherheit, Haftung, Möglichkeit von Kontrollen, etc. klar geregelt werden. Eine Dokumentation der datenschutzrelevanten Elemente des Vertrags und der Anforderungen an die Datensicherheit zu Zwecken der Beweissicherung ist sogar gesetzlich vorgesehen.

Der Auftragsdatenbearbeitung dürfen darüber hinaus keine gesetzlichen oder vertraglichen Geheimhaltungspflichten entgegenstehen. Umgekehrt sollte der Auftragsdatenbearbeiter auch zur Geheimhaltung verpflichtet werden. In diesem Zusammenhang empfiehlt es sich daher immer, den Auftragsdatenbearbeiter eine Geheimhaltungserklärung unterzeichnen zu lassen.[36]

2009 wurde im Rahmen einer Revision des DSG die Institution des **Datenschutzverantwortlichen** als ein Instrument der Selbstregulierung geschaffen. Das Gesetz, wie auch die allgemeine Datenschutzrichtlinie, sieht einen **behördlichen** bzw. **betrieblichen Datenschutzverantwortlichen** als Erleichterung der Registrierungspflicht von Datensammlungen vor.[37] Wir begrüssen dies. Damit fördert der Gesetzgeber ähnlich wie beim Datenschutzberater[38] die Selbstregulierung, aber auch das Datenschutzbewusstsein. Nachdem erst Anfang 2011 der erste Datenschutzverantwortliche bei uns angemeldet worden war, ergriffen wir die Initiative und erklärten die Förderung der Benennung von Datenschutzverantwortlichen zu einem Jahresziel. So führten wir eine Informationsveranstaltung durch, zu der wir die Verantwortlichen und Interessierte einluden.[39] Bis Ende des Jahres konnten insgesamt 25 Datenschutzverantwortliche in der öffentlich zugänglichen Liste verzeichnet werden.[40]

Im Gegensatz zur Schweiz gibt es in Liechtenstein noch keinen *Verein von unternehmensinternen Datenschutzverantwortlichen*. Die Gründung eines solchen Vereins wäre gewiss sinnvoll. Diese Veranstaltung

34 Definition: „Ein Modell, welches universellen, komfortablen und bei Bedarf über ein Netzwerk Zugriff auf einen gemeinsamen Pool von informationstechnischen Ressourcen ermöglicht (z.B. Netzwerke, Server, Speichersysteme, Anwendungen und Dienste), die schnell und mit minimalem Verwaltungsaufwand oder ohne Interaktion durch den Diensteanbieter bereitgestellt und freigegeben werden können." http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

35 Vgl. Veranstaltung an der Universität Liechtenstein mit Teilnahme des Datenschutzbeauftragten auf dem Podium, http://www.uni.li/tabid/1791/Default.aspx.

36 Über den Online-Schalter unserer Internetseite kann die Mustervorlage einer Datenschutz- und Geheimhaltungserklärung abgerufen werden. http://www.llv.li/form-llv-dss-mustervorlage

37 Vgl. Art. 4a DSV.

38 Vgl. Art. 23 DSV.

39 Vgl. unten, 2.1.

40 http://www.llv.li/pdf-llv-dss-liste_datenschutzverantwortliche.pdf.

ist als ein erster Schritt zu sehen. Wir werden den Kontakt zu den Verantwortlichen weiterhin pflegen.

1.7. Arbeitsbereich

Die Frage, ob ein **Arbeitgeber Zugriff** auf die **E-Mails** eines **Arbeitnehmers** nehmen darf, wurde wiederholt gestellt. Die Grundregeln hierzu haben wir in unserer *Richtlinie über Internet- und E-Mail-Überwachung am Arbeitsplatz* festgehalten. Das Wichtigste soll hier wiedergegeben werden.[41]

Die Erstellung eines *Nutzungs- und Überwachungsreglements*, in dem die Nutzung von E-Mail, Internet und Telefon sowie die Folgen von etwaigen Verstössen geregelt wird, ist zentral. Dabei sollte das Nutzungsreglement vorsehen, ob die erwähnten Kommunikationsmittel neben der geschäftlichen Nutzung auch für die private Nutzung zum Teil zulässig sind. In unserer Beratungspraxis zeigt sich immer wieder, dass viele Arbeitgeber hierzu keine konkreten Regelungen getroffen haben, was eine Problemlösung erschwert. Ein Überwachungsreglement stellt eine zwingende Voraussetzung für die personenbezogene Auswertung bzw. für den Zugriff auf persönliche E-Mail-Accounts dar. Diese Reglemente sollten den Arbeitnehmern zudem nachweislich zur Kenntnis gebracht werden, z.B. durch eine schriftliche Bestätigung des Erhalts, die danach im Personalakt abgelegt werden kann. Ebenfalls sollten die Voraussetzungen und die Vorgehensweise bei einer personenbezogenen Auswertung oder der Zugriff während Abwesenheitszeiten (z.B. Krankheit, Urlaub) geregelt werden. Besteht keine interne Regelung, gilt grundsätzlich Folgendes: Eine anonyme oder stichprobenartige pseudonymisierte Auswertung von Protokollen ist jederzeit zulässig. Auch eine anonyme Auswertung des „Betreffs" von geschäftlichen E-Mail-Accounts der Mitarbeiter ist mit Ausnahme der als ausdrücklich *„privat"/„vertraulich"/ „persönlich"* gekennzeichneten E-Mails zulässig. [42]

Denn auch am Arbeitsplatz geniesst private Post uneingeschränkten Schutz mit der Folge, dass als privat gekennzeichnete E-Mails wie die klassische Papierpost zu behandeln sind. Findet sich kein privater Zusatz, kann davon ausgegangen werden, dass die E-Mail einen geschäftlichen Bezug hat. Eine Auswertung sollte immer nach dem *Vier-Augen-Prinzip* erfolgen, z.B. der Vorgesetzte oder ein Vertreter der Geschäftsleitung zusammen mit dem Datenschutz- oder Personalverantwortlichen. Darüber hinaus sollten für den Fall von Abwesenheiten klare Stellvertretungen vorgesehen werden. Die **Weitergabe von Passwörtern** darf von Arbeitgeberseite nicht verlangt werden.

Die an uns gestellten Fragen, zu welchem Zweck und in welchem Umfang ein **Arbeitgeber Daten** über den **Arbeitnehmer** bearbeiten darf, betrafen die gesamte Bandbreite von der Bewerbung bis hin zur Datenbearbeitung nach Beendigung des Arbeitsverhältnisses: Grundsätzlich darf ein Arbeitgeber Personendaten des Arbeitnehmers bzw. Bewerbers nur bearbeiten, soweit sie dessen **Eignung für das Arbeitsverhältnis** betreffen oder zur **Durchführung des Arbeitsvertrages** erforderlich sind.[43] Es ist daher zu prüfen, ob die fraglichen Daten unter Berücksichtigung des Arbeitsverhältnisses als notwendig zu betrachten sind. Es muss ein direkter Bezug zwischen der Frage und der beruflichen Eignung vorliegen.[44]

41 http://www.llv.li/richtlinien_ueber_internet-_und_e-mail-ueberwachung_am_arbeitsplatz.

42 Eine personenbezogene Auswertung ist hingegen nur in Ausnahmefällen zulässig, wenn konkrete Anhaltspunkte für einen Missbrauch oder gar eine Straftat vorliegen. In diesen Fällen dürften im Rahmen einer Interessensabwägung die Interessen des Arbeitgebers überwiegen. In der Regel sind die betroffenen Arbeitnehmer über eine namentliche Auswertung von Internet-Protokollierungen/Telefonanrufen bzw. einen Zugriff auf den E-Mail-Account zu informieren. Diese Information hat zu erfolgen, bevor ein Missbrauch bzw. ein solcher Verdacht überhaupt vorliegt und nicht erst vor der personenbezogenen Auswertung. Daran dürfte es in den meisten Fällen scheitern. Nur ganz ausnahmsweise, wenn ein schwerer Missbrauch vorliegt, kann die vorherige Information auch erst vor der personenbezogenen Auswertung erfolgen. Der Arbeitgeber sollte daher grundsätzlich ein entsprechendes Nutzungs- und Überwachungsreglement schaffen.

43 Vgl. Art. 28a des Einzelarbeitsvertragsrechts zu § 1173a des Allgemeinen Bürgerlichen Gesetzbuchs (ABGB). Daten zur Durchführung des Arbeitsvertrages müssen in einem sachlichen Zusammenhang zum Arbeitsverhältnis stehen. Darunter fallen Daten, die aus organisatorischen und administrativen Gründen zum Zweck der Durchführung des Arbeitsverhältnisses gesammelt werden, wie z.B. Angaben über Lohn, alle sozialversicherungsrechtlich notwendigen Angaben, Angaben über Auslagenersatz und Aufzeichnungen über Leistungen und Verhalten des Arbeitnehmers im Hinblick auf die Zeugnis- und Referenzpflicht. Daten aus dem Privatbereich fallen grundsätzlich nicht darunter.

44 Vgl. Martin Winterberger-Yang, in: DSG – Basler Kommentar, Maurer-Lambrou / Vogt (Hrsg.), 2. Auflage, Basel, Genf, München, 2006, Rn. 5 zu Art. 328b. Daten zur Eignung für das Arbeitsverhältnis sind etwa Angaben über den schulischen und beruflichen Werdegang, Auslandsaufenthalte und Sprachkenntnisse, Zusatzausbildungen und Berufsbewilligungen, soweit sie für die konkrete Arbeitsstelle von Bedeutung sind.

Die Daten zur Eignung für das Arbeitsverhältnis sind dabei nicht auf die Phase der Vertragsanbahnung zu beschränken, sondern betreffen auch das *laufende Arbeitsverhältnis*, z.B. mit Blick auf Beförderungen oder Sanktionen, und wirken auch nach Beendigung des Arbeitsverhältnisses weiter, z.B. Datenbearbeitung im Rahmen der betrieblichen Altersversorgung. Die Zulässigkeit einzelner Fragen kann oftmals nicht pauschal beantwortet werden, sondern hängt hierbei vom konkreten Arbeitsverhältnis ab. Grundsätzlich gelten die allgemeinen Datenschutzrechte auch im Rahmen des Arbeitsverhältnisses, wie insbesondere das Auskunftsrecht oder das Recht auf Berichtigung und Löschung. So kann zum Beispiel auch ein Bewerber Auskunft verlangen[45] und die Weitergabe seiner Daten an Dritte darf zulässigerweise nur bei Vorliegen einer Einwilligung von Seiten des Bewerbers/Arbeitnehmers oder auf Grundlage einer einschlägigen Rechtsvorschrift erfolgen.

Ein Unternehmen fragte uns zu einem **Zeiterfassungssystem** mit Gesichtserkennung an, welches der *Zugangskontrolle* dienen soll. Erfasst werden sollen alle Angestellten des Unternehmens. Die Erfassung biometrischer Daten wird damit begründet, dass alternative Massnahmen nicht mehr empfehlenswert erscheinen, da durch diese weder Verlust von Badges noch Missbrauchsmöglichkeiten definitiv ausgeschlossen werden könnten.

Die zur Identifikation von Personen erforderlichen biometrischen Angaben – gegenständlich das Gesicht des Betroffenen – sind höchstpersönlich und unveränderbar, wodurch die Bearbeitung biometrischer Daten grundsätzlich ein schwerer Eingriff in die Privatsphäre der Betroffenen darstellt. Jeder Eingriff benötigt einen *Rechtfertigungsgrund* und muss so *gering wie möglich* gehalten werden. Der Dateninhaber darf wie erwähnt nur diejenigen Daten bearbeiten, die für die Erfüllung seiner Aufgabe unbedingt notwendig und geeignet sind *(Verhältnismässigkeitsprinzip)*. Daher dürfen auch nur diejenigen Daten erhoben werden, die für die Erreichung des Ziels unentbehrlich sind.[46] Unter anderem ist zu klären, zu welchem Zweck die biometrischen Daten erfasst und bearbeitet werden. Werden die Daten ausschliesslich zur Zeiterfassung bearbeitet oder ist eine weitere Nutzung (z.B. Zugangskontrolle) angedacht? Der betroffene Personenkreis ist zu berücksichtigen. Wurden alternative, weniger in die Privatsphäre der Betroffenen eingreifende Massnahmen geprüft?

Wir teilten dem Unternehmen mit, dass das anvisierte Zeiterfassungssystem mit Gesichtserkennung datenschutzrechtlich *nicht verhältnismässig und deshalb unzulässig wäre*.[47]

1.8. Bildung

Im Rahmen der Erstellung der **Bildungsstatistik** stellte sich die Frage, ob es eine gesetzliche Verpflichtung von Bildungsinstitutionen gibt, dem Amt für Statistik personenbezogene Daten zu liefern. Da das Amt sowieso keine Personendaten publizieren darf, sei dies nicht nötig, so das Argument. Zudem sehe das Statistikgesetz dies auch nicht vor. Dieses kenne allgemein keine klaren Bestimmungen, aus denen hervorgeht, welche Angaben das Amt anfordern darf. Demgemäss bestehe die Gefahr, dass teils sogar willkürlich Daten angefordert werden. Zudem seien personenbezogene Angaben im Ausland auch nicht üblich.

Informationen in Bezug auf das schweizerische Bundesamt für Statistik (BfS) zufolge bearbeitet das Bundesamt sehr wohl personenbezogene Daten. Dies sei im Rahmen der Bildungsstatistik auch notwendig, um Bildungsverläufe darstellen zu können, so das Amt für Statistik. Im Rahmen der Diskussionen schlug das Amt vor, die Daten neu pseudonymisiert zu speichern. Wir begrüssten diesen Vorschlag, da somit eine erhöhte Datensicherheit gegeben ist.

Was das *Statistikgesetz* betrifft, hielten wir Folgendes fest: Wir waren bereits im Vernehmlassungsverfahren der Ansicht gewesen, dass der Entwurf des Statistikgesetzes sehr abstrakt formuliert war und aus Gründen der Rechtssicherheit konkretisiert werden sollte. Die Bildungsstatistik sollte sich in Liechtenstein nach derjenigen der Schweiz richten. Wenn man dazu die Rechtsgrundlagen vergleicht, fällt auf, dass die gesetzlichen Bestimmungen in der Schweiz

45 Art. 11 DSG.

46 „Richtlinien über die Rechte der betroffenen Personen bei der-Bearbeitung von Personendaten", Pkt. 3.4, S. 6, http://www.llv.li/pdf-llv-dss-rechte_betroffene_personen.pdf.

47 Vgl. zur Biometrie: http://www.llv.li/amtsstellen/llv-dss-spezialthemen/llv-dss-spezialthemen-biometrische_daten.htm.

konkreter gefasst sind.[48] Im Sinne der Rechtssicherheit schlugen wir deshalb vor, die Bestimmungen im Statistikgesetz *konkreter* zu fassen. Zudem haben wir mit einer *Kontrolle* der *Datensicherheit* beim Amt für Statistik begonnen.

Microsoft Live@edu ist eine für Bildungseinrichtungen kostenfreie Online-Plattform. Diese bietet sowohl für Lehrkräfte als auch für Schülerinnen und Schüler unter anderem kostenlose E-Mail-Konten sowie weitere Online-Werkzeuge für den Unterricht. In einer Anfrage zu diesem Programm stellten wir fest, dass grundsätzlich nichts gegen die Verwendung des Microsoft-Produkts spricht, solange eine auf Liechtenstein angepasste Vereinbarung getroffen wird und die entsprechenden Datenschutzbestimmungen im Zusammenhang mit Cloud Computing eingehalten werden.[49] Sehen die Nutzungsbedingungen eine Einwilligung der Endnutzer bzw. deren Erziehungsberechtigten vor, ist eine solche jedenfalls durch den Betreiber einzuholen. Wenn eine solche Einwilligung notwendig ist, kann diese durch den Endnutzer auch verweigert werden. Eine Verpflichtung zur Nutzung der Services können wir derzeit nicht erkennen.

1.9. Datenbekanntgabe im Inland

Bekanntlich gab es in Liechtenstein lange Zeit ein sogenanntes **Autonummerbüchlein**. In diesem Büchlein konnte nachgeschaut werden, wem eine Autonummer zuzuschreiben ist. Dieses Büchlein wurde in den 90er-Jahren durch die Verwaltungsbeschwerde-Instanz abgeschafft. Zur Veröffentlichung eines Autobüchleins hat die Regierung an einer Landtagssitzung im Rahmen einer Kleinen Anfrage festgehalten, dass in der Vergangenheit jedermann – ohne besonderen Interessennachweis – zu jeder Zeit und überall auf Grund der Kontrollschildnummer die Identität eines Fahrzeughalters herausfinden, diese Daten (auch) zu ungunsten der betroffenen Personen brauchen und sie in andere Datensammlungen einspeisen konnte. Damit war die Gefahr von *Missbräuchen und Persönlichkeitsverletzungen gegeben.*[50]
Wir erhielten eine Anfrage zur **Bekanntgabe von Baugesuchen durch die Gemeinden**. Auch diese Bekanntgabe war jahrelang üblich. Unseres Erachtens kann der Begriff des Datenschutzes mit dem Begriff des Rechtes gegen eine *unberechtigte Neugier* umschrieben werden. Wie bei Autonummern geht es auch bei Baugesuchen oftmals um die Befriedigung reiner Neugier. Die betroffenen Verfahrensparteien werden in Bauverfahren geschützt. In der Vergangenheit hatten wir verschiedentlich Rückmeldungen aus der Bevölkerung bekommen, wonach die Veröffentlichung von Baugesuchen zu unerwünschter Werbung geführt habe. Unsere Antwort auf die Frage einer Gemeinde zur Veröffentlichung von Baugesuchen lautete dahingehend, dass der Fall mit dem Autonummerbüchlein verglichen werden könne und es keinen sachlichen Grund gäbe, welcher die Veröffentlichung sämtlicher Gesuche rechtfertigen würde. Im Gegenteil führt eine Bekanntgabe häufig zu unerwünschter Werbung.

Immer wieder werden wir zur **Berichterstattung in den Medien** angefragt, ob hier nicht zu tief in die Privatsphäre von betroffenen Personen eingegriffen wird. Zwar ist der Schutz der Privatsphäre in einem so kleinen Land wie Liechtenstein nicht einfach, sodass es auf Grund der Kleinheit der Verhältnisse praktisch immer Personen gibt, die wissen, um wen es geht. Dennoch sollte eine Berichterstattung unseres Erachtens in der Regel die Sache und nicht die betroffene Person in den Vordergrund stellen. Dies teilten wir der Medienkommission mit und baten um Stellungnahme. Die **Medienkommission** hat uns gegenüber mitgeteilt, dass konkrete Überlegungen bestehen, auch in Liechtenstein einen Ombudsmann einzuführen, so wie es beispielsweise in der Schweiz üblich ist. Aus Anlass einer entsprechenden Empfehlung der Medienkommission an die Regierung setzte sich die Regierung in der *„Postulatsbeantwortung der Regierung an den Landtag des Fürstentums Liechtenstein betreffend die zukünftige Medienpolitik der Regierung"* mit der Schaffung einer Ombudsmannstelle auseinander.[51] Die Regierung befürwortet grundsätzlich die Einrichtung einer mit dem Schweizer Presserat[52] vergleichbaren Stelle in Liechtenstein.
Die Regierung befürchtet jedoch, dass die heimischen Medienschaffenden realistischerweise nicht für den Unterhalt eines zusätzlichen Presserats oder einer eigenen Ombudsstelle aufkommen könnten. Da auch die Anzahl der Fälle allein auf Grund der Grösse

48 Vgl. Art. 14 ff. des Bundesstatistikgesetzes.
50 Vgl. das Protokoll zur Landtagssitzung vom 14. bis 16. März 2007, http://www.landtag.li/Protokolle/xsl/Landtagsprotokoll_2007_3_14.pdf (Seite 71).
51 Vgl. Bericht und Antrag 108/2011, S. 58 ff.
52 www.presserat.ch

des Landes eher gering ausfallen dürfte, überlegt die Regierung, einige der Aufgaben und Befugnisse, die in der Schweiz dem Presserat zukommen, in Liechtenstein der Medienkommission zu übertragen. Eine zukünftige Erweiterung der Aufgaben und Funktionen der Medienkommission erscheint uns durchaus als eine machbare Lösung und wird daher von unserer Seite grundsätzlich begrüsst.

Die Medienkommission gelangte an uns mit der Anfrage, ob das Vorgehen der Zeitungen bei der **Veröffentlichung von Erstklässlerfotos** dem Datenschutz entspricht.[53] Hierzu haben wir festgehalten, dass die Eltern ausreichend informiert sein müssen und dem Vorhaben der Zeitungen ihre Einwilligung geben müssen. Dies gilt umso mehr, wenn Daten auch im Internet veröffentlicht werden, da eine Löschung von Daten aus dem Internet praktisch unmöglich ist. Ausserdem sind Fotos aus dem Internet auf der ganzen Welt einsehbar.

1.10. Datenbekanntgabe mit Auslandsbezug

Anfragen zum **Datentransfer ins Ausland** nehmen weiterhin zu.[54] Dies gilt auch für Anträge auf Genehmigung von verbindlichen unternehmensinternen Datenschutzvereinbarungen *(Binding Corporate Rules)*.[55] Im Zentrum stand dabei vorwiegend eine konzernweite IT-Softwarelösung oder *Cloud Computing*.[56]

Kritisch bei solchen Vertragsgestaltungen ist insbesondere, dass nicht nur die *allgemeinen Grundsätze* des Datenschutzes, sondern auch allgemeine Berufsgeheimnisse und das Datengeheimnis im Besonderen gewahrt werden müssen. Die Geheimnispflicht kann allerdings einer Auftragsbearbeitung generell entgegenstehen, wenn im Empfängerland z.B. der Umfang der Geheimhaltungspflicht von der liechtensteinischen Regelung derart abweicht, als dort staatliche Behörden gesetzliche Zugriffsrechte haben.[57] Wir haben deshalb unsere Mustervorlagen für Datenschutz- und Geheimhaltungserklärungen um Formulierungen, die einen Auslandsdatentransfer im Rahmen einer Auftragsdatenbearbeitung beinhalten, erweitert.[58]

2. Öffentlichkeitsarbeit

2.1. Veranstaltungen

Die Veranstaltung zum **5. Europäischen Datenschutztag** am 27. Januar 2011 mit dem Titel **„Schau mal, wer da spricht" – Was Handys, Notebooks & Co alles erzählen** stand ganz im Zeichen von mobilen Geräten. Smartphones sind beispielsweise vollwertige Computer, mit denen man auch telefonieren kann. Was spielt sich hinter den Kulissen ab? Wir haben in Zusammenarbeit mit der Universität Liechtenstein einen Vortragsabend zum Thema *„Datenschutz und Mobilität"* veranstaltet. Handys, Notebooks und Tablet-PCs sind heutzutage aus unserem Alltag nicht mehr wegzudenken. Dank kompakter Geräte und schneller drahtloser Netzwerke kann überall kommuniziert und gearbeitet werden.

Eingangs wurden die Ergebnisse einer jüngst zu diesem Thema erstellten Umfrage an der Universität Liechtenstein präsentiert. Im Hauptreferat ging es um den *(scheinbaren) Widerspruch von Datenschutz und Mobilität*. Wesentliche Risikofaktoren werden im Verlust der Kontrolle der eigenen Daten und der informationellen Selbstbestimmung gesehen, vor allem aber in der mangelnden Transparenz der angebotenen Dienste. Gütesiegel für datensparsame mobile Systeme und Anwendungen könnten für den Verbraucher nützlich sein. Es braucht aber auch eine selektive Handhabung durch die Betroffenen. Dies kann manchmal auch zu einem Verzicht der Konsumenten auf bestimmte Technologien bzw. auf eine noch nicht erprobte oder bekannte Funktionalität führen.

53 Vgl. dazu unter anderem Tätigkeitsbericht 2010, 1.8.
54 Vgl. Anfragenstatistik im Anhang.
55 Für die Erteilung der Genehmigung ist das Ressort Justiz zuständig, vgl. Art. 6 DSV. Im Rahmen des Genehmigungsverfahrens geben wir jedoch Stellungnahmen ab, vgl. Tätigkeitsbericht 2009, 1.9.
56 Vgl. 1.6.
57 Aufsatz mit dem Titel „Datenschutzrechtliche Chancen und Risiken von Cloud Computing" von Philipp Mittelberger und Gabriele Binder, in: Jus & News 2011/2, S. 163 ff. Zugriffe durch staatliche Stellen auf Grund des jeweiligen nationalen Rechts sind denkbar in dem Land, in dem der Serviceanbieter und/oder ein möglicher Subunternehmer seinen Sitz hat, in dem Land, in dem das Unternehmen seinen Sitz hat, das den IT-Anbieter wirtschaftlich kontrolliert und/oder in dem Land, in dem die Daten bearbeitet und gespeichert werden. Dies kann je nach Empfängerland variieren und muss jeweils in einer auf den Einzelfall zugeschnittenen Lösung angemessen berücksichtigt werden. Pauschallösungen gibt es in diesem Zusammenhang nicht.
58 http://www.llv.li/form-llv-dss-mustervorlage.

Die Podiumsrunde wurde für Fragen und zur Diskussion rege genutzt. Auch praktische Tipps wurden den Nutzern gegeben, die im Arbeitspapier *„Mobile Verarbeitung personenbezogener Daten und Datensicherheit"* der Internationalen Arbeitsgruppe für Telekommunikation nachzulesen sind. Das Arbeitspapier entstand übrigens auf unsere Initiative hin.[59]

Die Diskussion hat auch gezeigt, dass der Nutzer den neuen Technologien nicht hilflos gegenübersteht. Technologien sind an und für sich weder gut noch schlecht. Es kommt immer darauf an, wie man sie nutzt. Dies erfordert Kompetenz und Eigenverantwortung des Einzelnen. So ist die Bewusstseinsbildung ein erster wichtiger Schritt zur Vorbeugung von Missbrauch, Datenverlust oder Diebstahl.

Auf Einladung der privaten Universität im Fürstentum Liechtenstein nahmen wir an einer **Podiumsdiskussion** zum Thema **„Der Zugriff des Staates auf private Daten am Beispiel der Vorratsdatenspeicherung"** teil. Das Thema ist nicht nur aktuell, sondern auch für die gesamte Bevölkerung relevant. Während in Deutschland die Vorratsdatenspeicherung durch das Bundesverfassungsgericht abgeschafft und sie in Österreich noch nicht eingeführt wurde, werden in Liechtenstein die Verkehrs- und Standortdaten aller Personen bei jeder Nutzung von Telefon oder Internet auf Vorrat gespeichert. Diesen erheblichen Eingriff in das Recht auf Privatsphäre aller Bürger bezeichnet der Europäische Datenschutzbeauftragte als die stärkste Massnahme, die je in der EU für einen Eingriff in die Privatsphäre geschaffen wurde.[60] In der Diskussion ging es um die Vor- und Nachteile einer solchen Speicherung. Auf der einen Seite wurde von verschiedenen Seiten darauf hingewiesen, dass eine solche Speicherung für Strafverfolgungsbehörden *sehr nützlich* sein kann. Auf der anderen Seite wurde erwähnt, dass es um einen *Präzedenzfall* geht, dem möglicherweise weitere Fälle folgen können. Denn einerseits ist es möglich, dass die Speicherung erweitert wird, andererseits ist es denkbar, dass nicht nur Strafverfolgungsbehörden Zugriff auf diese Daten möchten.[61] Wir betonten, dass die Aufgaben im Rahmen der Strafverfolgung nicht zulasten der Privatsphäre der Betroffenen führen dürfen. In diesem Sinne gilt es, die *goldene Mitte* zu finden.

Als positiv einzustufen ist der Umstand, dass die Vorratsdaten in Liechtenstein nicht länger als sechs Monate gespeichert werden, dass es für den Zugriff der Daten einen *Richter-Vorbehalt* gibt und dass bei der letzten Revision des Kommunikationsgesetzes eine ausdrückliche Befugnis für uns geschaffen wurde, die *Datensicherheit* zu *prüfen*. Das deutsche Bundesverfassungsgericht hat bekanntlich die Vorratsdatenspeicherung in Deutschland abgeschafft.[62] Ein Grund für diese Abschaffung war der Umstand, dass keine hinreichenden Datensicherheitsbestimmungen gegeben waren. Auch in Liechtenstein gibt es keine speziellen Vorschriften. Es wäre allenfalls Sache des Staatsgerichtshofes zu prüfen, ob die Gesetzgebung den Ansprüchen der Verfassung genügt. Auf alle Fälle sollte überprüft werden, ob die Gesetzgebung zur Vorratsdatenspeicherung in Liechtenstein den Erfordernissen des deutschen Bundesverfassungsgerichts entsprechen.[63]

Am *Networking Day der Universität Liechtenstein* wurden wir zur **Podiumsdiskussion** zum Thema **Cloud Computing** eingeladen.[64]

Vor zwei Jahren wurde die Möglichkeit geschaffen, einen **internen Datenschutzverantwortlichen** zu benennen.[65] Wir luden die uns gemeldeten Verantwortlichen sowie Interessierte zu einer **Informationsveranstaltung** zum Thema **„Aufgaben und Stellungen eines Datenschutzverantwortlichen"** ein. Nach einer Einführung referierte der Datenschutzverantwortliche der *Liechtensteinischen Kraftwerke* zum Thema und berichtete über seine Erfahrungen. Im Anschluss wurden Fragen zu dieser neu geschaffenen Institution diskutiert. Dabei ging es unter anderem um die Organisation, die Verantwortlichkeit

59 Vgl. Tätigkeitsbericht 2010, II., 4.6. und http://www.llv.li/pdf-llv-li-675.41.18-de.pdf

60 Vgl. Newsletter Januar 2011: „Angesichts des Anwendungsbereichs der Richtlinie und der Zahl der von ihr betroffenen Menschen hält der EDSB sie deshalb für die am stärksten in die Privatsphäre eingreifende Rechtsvorschrift, die jemals in der EU angenommen wurde": http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_27_DE.pdf und Tätigkeitsbericht 2010.

61 Dies war angeblich in Deutschland der Fall, wobei die Musikindustrie Zugriff auf Internetdaten wollt um illegalen Fällen des Runterladens von Daten nachgehen zu können.

62 Vgl. Tätigkeitsbericht 2010, 1.3.

63 Vgl. auch 3.

64 http://www.uni.li/tabid/1791/Default.aspx; vgl. zu Cloud Computing, 1.6.

65 Vgl. 1.7.

oder einen Eskalationsprozess bei Uneinigkeiten oder darum, wie das Thema Datenschutz intern kommuniziert und geschult werden soll.

Die private Universität im Fürstentum Liechtenstein veranstaltete ein **Symposium zum Thema „Gesundheitsrecht am Puls der Zeit – Der gläserne Patient",** an dem wir mit einem Vortrag teilnehmen konnten. Titel unseres Referates war: *„Das Arztgeheimnis aus verschiedenen Perspektiven: Vertrauensarzt, Klinikinformationssystem, eHealth, Versichertenkarte oder gar Cloud Computing?"*[66] Ziel dieses Referates war es, aufzuzeigen, wie sich auch die Datenbearbeitung im Gesundheitsbereich ändert. Während es sich bei der Datenbekanntgabe des Vertrauensarztes an die Verwaltung einer Krankenkasse um konkrete Einzelfälle handelt, die nicht unbedingt elektronisch stattfinden muss, geht es bei eHealth oder gar bei Cloud Computing darum, dass verschiedenste Stellen auf elektronisch vorhandene Daten zugreifen können. Letzteres wurde im Rahmen eines Vortrages zum eHealth in Dänemark klar. Patientendaten sind dort elektronisch verfügbar. Ein Schutz derselben vor missbräuchlichem Zugriff ist nur beschränkt gegeben. Wir wiesen darauf hin, dass Daten dort verfügbar sein sollen, wo dies nötig ist. Ist dies nicht der Fall, sind beispielsweise durch differenzierte Zugriffsrechte Schutzmechanismen zu treffen. Insgesamt war der Zusammenhang zum Projekt eHealth klar, auf das auch von uns hingewiesen wurde. Nach dieser öffentlichen Veranstaltung gilt es, unsere Anliegen im Rahmen der Arbeitsgruppe elektronisches Gesundheitsnetz (eGN) einzubringen.[67]

2.2. Neuigkeiten auf der Internetseite

Auf unserer **Internetseite** *„www.dss.llv.li"* informieren wir regelmässig über aktuelle Themen, die für die Öffentlichkeit relevant sind. Diese Themen können bereits an einer anderen Stelle dieses Berichts beschrieben worden sein.

Wir gaben **Urlaubstipps**. Besonders in den Ferien ist man häufig mit der Bearbeitung von Personendaten konfrontiert: Zahlungen mit der Kreditkarte, das Ausfüllen von Meldescheinen in Hotels, die Vorlage eines Ausweises zur Identitätsfeststellung sind nur einige Beispiele.

Die **Entscheidungen der Datenschutzkommission** zu den Themen Akteneinsicht und Videoüberwachung haben wir über unsere Internetseite der breiten Öffentlichkeit zugänglich gemacht. Des Weiteren sind **Rechtsgutachten** zu finden, die wir zu unterschiedlichen Datenschutzthemen in der Vergangenheit eingeholt hatten.[68] Wir berichteten zudem über unsere Veranstaltung zum 5. Europäischen Datenschutztag unter dem Titel **„Schau mal, wer da spricht" – Was Handys, Notebooks & Co alles erzählen.**

Da die **Bearbeitung** von **Personendaten im Auftrag** („Outsourcing") in den letzten Jahren stark an Bedeutung gewonnen hat, haben wir nähere Informationen zu diesem Thema veröffentlicht. Gerade auch im grenzüberschreitenden Dienstleistungssektor, aber auch bei Behörden ist die Auftragsdatenbearbeitung mittlerweile zum Alltag geworden.[71] Zu diesem Thema haben wir zum sogenannten Cloud Computing, welches einen Anwendungsfall der Datenbearbeitung im Auftrag darstellt, einen Aufsatz in der Zeitschrift *„Jus & News"* sowie Antworten auf häufig gestellte Fragen (FAQ) erarbeitet.[69]

Durch eine datenschutzkonforme und ordnungsgemässe Umsetzung von **technischen und organisatorischen Massnahmen (TOMs)** gemäss Art. 9 bis 11 DSV soll sichergestellt werden, dass die Personendaten von Betroffenen während einer Datenbearbeitung in Informationssystemen korrekt bearbeitet und deren Rechte entsprechend berücksichtigt werden. Dazu haben wir eine **Empfehlung** veröffentlicht.[70] Systemgestalter und Entwickler sollen mit diesem Dokument einfacher beurteilen und feststellen können, in welchem Umfang sie die Rahmenbedingungen des Datenschutzes berücksichtigen müssen. Darin werden insbesondere die Begrifflichkeiten der besonderen Massnahmen,[71] wie die Zugangs-,

66 Die Folien zum Vortrag sind verfügbar unter: http://www.ufl.li/tasks/render/file/?fileID=01175490-5056-A765-BB87E60016B49FC4.

67 Vgl. oben, 1.4.

68 http://www.llv.li/amtsstellen/llv-dss-datenschutzkommission/llv-dss-entscheiddatenbank-dsk.htm http://www.llv.li/amtsstellen/llv-dss-gerichtsentscheide_aufsaetze/llv-dss-rechtsgutachten.htm

69 http://www.llv.li/amtsstellen/llv-dss-spezialthemen/llv-dss-spezialthemen-technisches/llv-dss-cloud-computing.htm sowie http://www.llv.li/pdf-llv-dss-jn-2011-2-cloud-computing.pdf.

70 http://www.llv.li/amtsstellen/llv-dss-richtlinien/llv-dss-empfehlung-tom.htm.

71 Art. 10 DSV.

Personendatenträger- (Datenträger-), Transport-, Bekanntgabe-, Speicher-, Benutzer-, Zugriffs- und Eingabekontrolle konkretisiert und mit Massnahmenvorschlägen verständlich beschrieben.
Da das **Internet** einige datenschutzrechtliche **Gefahren für Kinder und Jugendliche** birgt, haben wir für diese Zielgruppe nähere Informationen und Tipps gegeben: Schliesslich findet man im Internet selbst viele Quellen, die diese Probleme aufzeigen und Lösungsvorschläge anbieten.[72]

Nachdem wir im letzten Jahr **zwei Mustervorlagen für Geheimhaltungs- und Datenschutzvereinbarungen** neu auf unserer Internetseite zur Verfügung gestellt hatten, haben wir die wiederholten Anfragen zur grenzüberschreitenden Auftragsdatenbearbeitung (insbesondere Cloud Computing) zum Anlass genommen, um diese Geheimhaltungs- und Datenschutzvereinbarungen zunächst auf eine Vorlage zu reduzieren und diese mit Passagen für eine Auftragsdatenbearbeitung im Ausland zu ergänzen.[73]

Das DSG und die DSV unterscheiden bei der **Datenbearbeitung** zwischen **privaten Personen** und **Behörden.** Um die Grundsätze der Bearbeitung im Einzelnen verständlich und praxisgerecht darzustellen, haben wir auf unserer Internetseite entsprechende **Richtlinien** zur Verfügung gestellt. Die Richtlinie für die Bearbeitung von Personendaten im privaten Bereich wurde in den vergangenen Jahren erst neu erarbeitet und wird ständig aktualisiert. Die entsprechenden Richtlinien für die Bearbeitung von Personendaten bei Behörden bzw. für die Bekanntgabe durch Behörden stammten hingegen aus dem Jahr 2006 und bedurften infolge der in der Zwischenzeit stattgefundenen Revisionen des DSG und der DSV sowie der technischen Weiterentwicklung dringend einer Überarbeitung. Dies konnte nunmehr in 2011 realisiert werden. Herausgekommen sind **jetzt drei neue Richtlinien**: Neben den bereits genannten haben wir auch eine Richtlinie über die **Pflichten des Inhabers der Datensammlung** erarbeitet.[74]

3. Mitarbeit bei der Gesetzgebung

Die Mitarbeit bei der Gesetzgebung ist eine weitere unserer Kernaufgaben. Dabei haben wir darauf zu achten, dass der Gesetzgeber die Privatsphäre der Bürger beim Erlass neuer Vorschriften respektiert. Es hat sich sehr bewährt, wenn wir in einem *möglichst frühen Verfahrensstadium* einbezogen werden. Insgesamt gaben wir zu 24 Gesetzesvorhaben in verschiedenen Stadien des Gesetzgebungsverfahrens eine Stellungnahme ab. Exemplarisch soll im Folgenden auf Grund besonderer datenschutzrechtlicher Relevanz nur auf ein paar wenige Gesetzesvorhaben näher eingegangen werden:

Zur Umsetzung des *Rahmenbeschlusses über den Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit* wurde insbesondere das **DSG** und die **Strafprozessordnung** (StPO) revidiert. Bei dieser Revision waren wir durch die Regierung frühzeitig eingebunden worden. Wir nutzten die Gelegenheit der Revision der StPO für einen Vorschlag, der eigentlich nicht zur Umsetzung des Rahmenbeschlusses gehört, der aber dennoch im Rahmen der *Vorratsdatenspeicherung* wichtig ist: *die Frage des Strafmasses*, d.h. ab wann Daten gespeichert und ausgewertet werden dürfen. Diese Anregung hatten wir bereits bei der Vorbereitung der Landtagsvorlage auf informellem Weg eingebracht. Sie wurde nicht berücksichtigt, weshalb wir dies auf formellem Weg wiederholten. Es geht darum, dass nach der Richtlinie zur Vorratsdatenspeicherung nur „schwere Straftaten" erfasst sind.[75] An verschiedenen Stellen ist in der Richtlinie die Rede von der Bekämpfung des Terrorismus[76] oder der organisierten Kriminalität.[77] Betont wird ausdrücklich, dass Massnahmen zur Umsetzung der Richtlinie im Sinne der Landesverfassung und der Europäischen Menschenrechtskonvention (EMRK) verhältnismässig sein müssen.[78] Dabei sollte auf die schwere Straftat im Sinne von Art. 2 Abs. 2 des Rahmenbeschlusses des Rates über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten[79] verwiesen wer-

72 http://www.llv.li/amtsstellen/llv-dss-spezialthemen/llv-dss-kinder-jugendliche.htm
73 http://www.llv.li/form-llv-dss-mustervorlage; vgl. auch 1.10.
74 http://www.llv.li/amtsstellen/llv-dss-richtlinien.htm

75 Art. 1 Abs. 1 der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung bestimmt, dass „die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten … zur Verfügung stehen [müssen]" .
76 Erwägung 4 und 9.
77 Erwägung 7 und 9.
78 Erwägung 9.
79 Rahmenbeschluss 2002/584/JI vom 13. Juni 2002. Im Anhang zur Stellungnahme zur ersten Lesung betreffend die Abänderung des Gesetzes über die Landespolizei (Polizeigesetz; PolG, Bericht und Antrag 2010/108) findet sich ein Katalog mit Straftaten nach liechtensteinischem Recht, die denjenigen des Rahmenbeschlus-

den, im Sinne der Erklärung des Europäischen Rates anlässlich der Annahme der Richtlinie 2006/24/EG.[80] Diese Orientierung am Europäischen Haftbefehl wird auch in der Literatur empfohlen.[81]

In Liechtenstein ist die Verwendung der Vorratsdaten nach § 103 StPO jedoch schon dann zulässig, wenn dadurch die Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten, strafbaren Handlung gefördert werden kann. Dies lässt mehr Überwachungen zu als die Richtlinie vorsieht und scheint unverhältnismässig. Zu diesem Schluss kam auch das deutsche Bundesverfassungsgericht, als es am 2. März 2010 über eine Massenbeschwerde zur Vorratsdatenspeicherung urteilte.[82] Dabei bestimmte es, dass angesichts des schweren Grundrechteingriffs, den die Vorratsdatenspeicherung darstellt, eine Verwendung der vorsorglich gespeicherten Daten nur dann verhältnismässig ist, wenn sie der Erfüllung überragend wichtiger Aufgaben des Rechtsgüterschutzes dient, d.h. zur Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen oder zur Abwehr von Gefahren für solche Rechtsgüter. Für die Strafverfolgung konkretisierte es hierzu, dass ein Abruf der Daten einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt und dass der Gesetzgeber abschliessend festlegen muss, welche Straftatbestände hiervon betroffen sind. Eine Generalklausel (wie sie in § 103 StPO zu finden ist) oder lediglich die Verweisung auf besonders schwere Straftaten reichen gemäss Bundesverfassungsgericht hingegen nicht aus.[83]

Wie bereits im letzten Tätigkeitsbericht festgehalten, beurteilt der Vizepräsident des Staatsgerichtshofes die Vorratsdatenspeicherung in Liechtenstein in einem Aufsatz „grundrechtlich jedenfalls als problematisch". Und: „Ob sie der Staatsgerichtshof als verfassungswidrig qualifizieren wird, dürfte auch wesentlich von der zukünftigen einschlägigen ausländischen Grundrechtssprechung abhängen."[84] Mit der Entscheidung des deutschen Bundesverfassungsgerichts liegt eine solche Grundrechtssprechung vor. Die Vorratsdatenspeicherung wurde dabei aber nicht per se als unverhältnismässig beurteilt. Vielmehr bestand das Problem darin, dass keine genügenden Schutzmassnahmen getroffen worden waren für diesen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt".[85] Eine dieser Massnahmen besteht eben in einer abschliessenden Auflistung der Straftatbestände.

Ergebnis: Somit ist zur Berücksichtigung der Anforderungen des Bundesverfassungsgerichts unter anderem eine Anpassung des Begriffs „strafbare Handlungen, die mit mehr als einjähriger Freiheitsstrafe bedroht sind" in § 103 StPO durch einen Hinweis auf diesen Katalog (Anhang zum Polizeigesetz) nötig, um die Verhältnismässigkeit dieses staatlichen Eingriffs in die Privatsphäre der Bürger zu wahren.[86] Mit einer Anpassung hätte ein weiterer Schritt zu einer gesamthaft daten- und grundrechtsfreundlichen Lösung gefunden werden können. Unser Anliegen, das nach der 1. Lesung eingebracht worden war,[87] wurde nicht für die 2. Lesung berücksichtigt. Erst auf Nachfrage erhielten wir eine Stellungnahme. Darin wurde festgehalten, dass die Einführung eines Deliktskatalogs nicht zum gewünschten Ergebnis führen würde.

Bei der **Totalrevision des Versicherungsaufsichtsgesetzes** (VersAG) wurden wir ebenfalls bereits vor dem offiziellen Vernehmlassungsverfahren beigezogen. Wir fokussierten uns insbesondere auf die Bestimmungen zum *Versicherungs- und Amtsgeheimnis sowie zur behördlichen (grenzüberschreitenden) Zusammenarbeit*. Das Modell, wonach der Versicherungsnehmer selbst vom Versicherungsgeheimnis entbinden kann, wurde bereits in der letzten Revision

ses 2002/584/JI entsprechen oder gleichwertig sind. Der Katalog bezieht sich auf die neu einzuführenden Art. 35f Bst. b und 35m Abs. 1 Polizeigesetz. Die Regierung bestimmt deren Inkrafttreten, hat sich aber soweit ersichtlich noch nicht festgelegt.

80 Vgl. Ratsdokument 6598/06 ADD 1, S.4; vgl. weiter Siegfried Schwab, Vorratsdatenspeicherung – Das BVerfG schützt die Freiheit der Bürger, 1. Auflage 2010.

81 Vgl. Birgit Kolb, Vorratsdatenspeicherung, Salzburg 2011, S. 83.

82 BVerfG Verfahren 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html. Vgl. dazu Tätigkeitsbericht 2010, 1.3.

83 BVerfG Verfahren 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Rn. 227f.

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

85 Randnummer 210.

86 Auch die Schweiz kennt einen abschliessenden Straftatenkatalog, siehe Art. 269 Abs. 2 StPO.

87 Diese unübliche Vorgangsweise war unseres Erachtens dadurch gerechtfertigt, als es im Sinne des Bundesverfassungsgerichts um einen Präzedenzfall ging.

des VersAG eingeführt[88] und sollte aus unserer Sicht unbedingt beibehalten werden. Die Wirksamkeit einer Entbindungserklärung steht und fällt mit einer wirksam erklärten Einwilligung.[89] Aus unserer Sicht sollte auch im Versicherungsbereich die betroffene Person, und damit der Kunde, im Vordergrund stehen. Der Kunde sollte so gut wie möglich informiert sein und seine Rechte wahrnehmen können. Die Stellung des Kunden ist aus unserer Sicht gerade auf einem Finanzplatz zentral. Deshalb waren wir gegen eine Aufweichung des Versicherungsgeheimnisses.

Weiters haben wir zu folgenden Gesetzesprojekten eine Stellungnahme abgegeben:

- E-Governmentgesetz
- Elektrizitätsmarktgesetz
- Evaluation trilateraler Polizeikooperationsvertrag FL-A-CH
- Gasmarktgesetz
- Gemeindegesetz
- Gesetz über das Öffentliche Auftragswesen
- Gesetz über das Öffentliche Auftragswesen im Bereich der Sektoren
- Gesetz über das Zentrale Personenregister
- Glaubensgenossenschaftsgesetz
- Konsumkreditgesetz[90]
- Patientenverfügungsgesetz
- Schulgesetz
- Schulzahnpflegegesetz
- Sozialhilfegesetz
- Stipendiengesetz
- Verordnung über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro (N-SIS-Verordnung)
- Verordnung über die Informationssysteme der Landespolizei
- Verordnung über die Melde- und Taxpflicht bei Beherbergungen
- Verordnung über elektronische Kommunikationsnetze und -dienste
- Verordnung zum Gesetz über die Krankenversicherung
- Verordnung zum Patientenverfügungsregister
- Waffengesetz

88 Vgl. Tätigkeitsbericht 2009, 1.6. zu der zuvor geltenden Regelung.
89 Vgl. Art. 3 Abs. 1 Bst. m) und Art. 4 Abs. 4 DSG. Zu den Voraussetzungen an eine datenschutzrechtlich wirksame Einwilligungserklärung, vgl. unter 5.1.
90 Vgl. dazu ausführlich Tätigkeitsbericht 2010, II. 3.

4. Kontrollen

Das **Zentrale Personenregister (ZPR)**[91] wurde Ende der Neunzigerjahre erstellt und wird seither laufend ausgebaut. Die zentral geführte Datenbank wird von zahlreichen Amtsstellen genutzt und enthält Daten sämtlicher Einwohner Liechtensteins und Daten von im Ausland wohnhaften Personen, die mit der Landesverwaltung in Kontakt getreten sind, sowie Daten von juristischen Personen. Sie stellt damit ein besonders wichtiges Arbeitsinstrument in der Landesverwaltung dar.[92]

Auf Grund der Beschaffenheit des ZPR wurden von uns bereits verschiedenste Anpassungen gefordert.[93]

So findet z.B. bisher nur eine eingeschränkte Protokollierung der Nutzung statt, wobei lediglich Benutzeranmeldungen und Datenmutationen (Änderungen) im System dokumentiert werden. Die von uns geforderte Leseprotokollierung und somit die Erfassung einzelner Abfragen im System beschränkt sich auf die im ZPR gespeicherten Fotos.[94] Die fortgeschrittene Diskussion um die Schaffung des Gesetzes über das ZPR[95] nahmen wir deshalb zum Anlass, im Rahmen unserer Kontrolltätigkeit die derzeit bestehende Protokollierungsfunktion auf das Foto zu prüfen und über den Zeitraum eines Jahres (01. August 2010 bis 01. August 2011) *pseudonymisiert* auszuwerten.

Es konnte festgestellt werden, dass im Auswertungszeitraum Benutzer aus insgesamt fünf verschiedenen Organisationseinheiten auf das Foto zugegriffen haben. Das Ergebnis der pseudonymisierten Auswertung wurde den zuständigen Amtsleitern bzw. Verantwortlichen der jeweiligen Organisationseinheit zur Kenntnis gebracht.

91 Vormals Zentrale Personenverwaltung der Liechtensteinischen Landesverwaltung (ZPV).
92 Vgl. Tätigkeitsbericht 2005, 5.1.1.1, Tätigkeitsbericht 2004, 5.1.1.1 und Tätigkeitsbericht 2003, 4.1.2
93 Vgl. Tätigkeitsbericht 2008, 3.1.
94 Vgl. Tätigkeitsbericht 2006, 5.1.1.1. Im ZPR werden Fotos sämtlicher Einwohner Liechtensteins und von im Ausland wohnhaften Personen gespeichert, sofern ein solches im Zusammenhang mit der Ausstellung eines Reisepasses oder eines anderen amtlichen Lichtbildausweises (z.B. Ausländerausweis) vom Ausländer und Passamt (APA) erfasst wurde.
95 LGBl. 2011 Nr. 574.

Wir regten bei dieser Gelegenheit zur Schaffung von Rechtssicherheit an, die Vorgehensweisen und Verantwortlichkeiten bei einer personenbezogenen Auswertung von ZPR- oder auch anderen Protokollen (z.B. Internet- und E-Mail-Verkehr) nach einer möglichen Feststellung von Abweichungen im ordentlichen Dienstbetrieb, z.B. durch eine auffallend hohe Anzahl von Zugriffen auf Personendaten, in den einschlägigen Nutzungsreglementen der IT-Sachmittel klar zu regeln. Diese Regelungen wären jedem Mitarbeiter im Vorfeld zur Kenntnis zu bringen. Wir werden bei der Ausgestaltung und Formulierung unterstützen.

5. Internationale Zusammenarbeit

5.1. Artikel-29-Datenschutzgruppe

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

Als wichtigstes Thema ist die **Revision der Datenschutzrichtlinie** zu nennen.[96] Auch im vergangenen Jahr beschäftigte sich die Arbeitsgruppe mit verschiedenen Aspekten, zu denen eine Stellungnahme der Europäischen Kommission gewünscht worden war, so zur Frage der Zukunft der Registrierungspflicht von Datensammlungen, zur Frage der Stärkung der Datenschutzbehörden oder der Artikel-29-Datenschutzgruppe selbst. Vonseiten der Kommission war wiederholt zu vernehmen, dass sie eine stärkere Harmonisierung anstrebt, da die bestehende allgemeine Datenschutzrichtlinie den Mitgliedstaaten offenbar zu viel Spielraum gelassen hatte. Dies führte dazu, dass es zu viele einzelstaatliche Lösungen gab, was z.B. ein gewisses „forum shopping" ermöglichte.

Eine Harmonisierung ist auch auf Grund der Globalisierung wichtig. So wirft z.B. *Facebook* immer wieder Fragen zum Umgang mit der Privatsphäre auf. Da Facebook den europäischen Hauptsitz in Irland hat, fand dort eine Prüfung durch die irische Datenschutzbehörde statt.[97] Diese Kontrolle kann als ein Test für künftige vergleichbare Fälle der Datenbearbeitung durch aussereuropäische Unternehmen angesehen werden. Bei einer stärkeren Harmonisierung des Rechts sollten einzelstaatlich unterschiedliche Lösungen wie bei Google *Street View* vermieden werden können. Eine einheitliche Lösung dient nicht nur dem in Frage stehenden Unternehmen, sondern auch den betroffenen Personen und somit der Rechtssicherheit. Auch wenn dies noch nicht formell entschieden wurde, gab es doch Anzeichen dafür, dass der neue Rechtstext die Form einer *Verordnung* und nicht einer Richtlinie annehmen wird. Verordnungen müssen nicht in innerstaatliches Recht umgesetzt werden und sind unmittelbar anwendbar. Dies wird für uns in der Praxis einen entscheidenden Vorteil haben: Wir würden uns noch stärker auf die Praxis, insbesondere in Österreich oder Deutschland, stützen können. Bis es aber so weit ist, wird es wohl auf Grund der Gesetzgebungsverfahren auf europäischer Ebene noch einige Jahre dauern.

Informationen in Bezug auf einen geografischen Standort (Standortdaten) werden immer wichtiger. Durch die rasche technologische Entwicklung und die weitverbreitete Nutzung von intelligenten mobilen Endgeräten entsteht eine ganz neue Kategorie standortbezogener Dienste. Mithilfe der Stellungnahme 13/2011 der Artikel-29-Datenschutzgruppe zu den **„Geolokalisierungsdiensten von intelligenten mobilen Endgeräten"**[98] soll für Klarheit hinsichtlich des für Geolokalisierungsdienste geltenden Rechtsrahmens gesorgt werden. Beispiele für solche Dienste sind: Karten und Navigation, geopersonalisierte Dienste (einschliesslich der Sehenswürdigkeiten der Umgebung), Augmented Reality, Georeferenzierung von Inhalten im Internet (Geotagging), Lokalisierung des Aufenthaltsortes von Freunden, Überwachung von Kindern und standortbezogene Werbung. Die Stellungnahme befasst sich mit den drei wichtigsten Arten der Infrastruktur, die zur Bereitstellung von Geolokalisierungsdiensten verwendet werden, nämlich GPS, GSM-Basisstationen und Wi-Fi. In der Stellungnahme wird zuerst die Technologie beschrieben, dann werden die Risiken für den Datenschutz herausgearbeitet, bewertet und schliesslich Schlussfolgerungen zur Anwendbarkeit der einschlägigen Artikel in der Richtlinie gezogen.
Die Stellungnahme 15/2011 zur **Definition der Einwilligung**[99] bietet eine gründliche Analyse des

96 Vgl. Tätigkeitsbericht 2010, 4.1.
97 Vgl. oben, 1.2.
98 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_de.pdf.
99 http://ec.europa.eu/justice/data-protection/article-29/documenta-

Konzepts der Einwilligung. Das Papier bestätigt unser bisheriges Verständnis.[100] Eine wirksame datenschutzrechtliche Einwilligung muss demnach folgende Merkmale erfüllen: Die Einwilligung muss ohne Zwang, d.h. freiwillig, sein. Ein irgendwie geartetes Abhängigkeitsverhältnis z.B. die Beziehung zwischen Arbeitgeber und Arbeitnehmer steht dem entgegen. Sie muss für den konkreten Fall vorliegen, d.h. für einen (oder mehrere) klar definierte(n) Zweck(e); sie muss in Kenntnis der Sachlage, d.h. nach angemessener Information gegeben werden. Die Willensbekundung, mit der die betroffene Person ihre Einwilligung zum Ausdruck bringt, darf keinen Zweifel an ihrer Einwilligungsabsicht erkennen lassen.[101] Beide Formulierungen zielen aber auf dasselbe ab. Denn eine Akzeptanz bedeutet eine eindeutige und klare, mithin zweifelsfreie Zustimmung zu etwas. Der einzige Unterschied zu unserem bisherigen Verständnis ist darin zu sehen, dass nach dieser Stellungnahme eine *Willensbekundung* in Form einer *aktiven Handlung* vorliegen muss. Demnach kann ein passives Verhalten keine Einwilligung begründen; eine blosse Unterrichtung entspricht diesem Erfordernis gerade nicht.[102] Damit wird die Möglichkeit der konkludenten oder stillschweigenden Einwilligung in Frage gestellt. Im Zweifel empfahlen wir bisher eine ausdrückliche Einwilligung, allein um im Zweifel nachweisen zu können, dass eine Einwilligung vorliegt. Eine ausdrückliche Einwilligung sollte daher im Zweifel am besten schriftlich erteilt werden; sie kann aber auch mündlich erfolgen oder z.B. im Internet durch aktives Anklicken einer Schaltfläche (z.B. bei der Online-Einwilligung). Die Stellungnahme der Artikel-29-Datenschutzgruppe zur Einwilligung führt viele praxisrelevante Beispiele an, gerade auch in Bezug auf die Schwierigkeiten, die sich bei einer Online-Einwilligung ergeben. Ein weiterer Schwerpunkt betraf eine Mitteilung der Kommission über die **Modalitäten zur Errichtung eines European Terrorist Finance Tracking Systems (TFTS).** [103] Da das sogenannte SWIFT-Abkommen[104] zwischen der EU und den USA seit einiger Zeit in der Kritik steht, schlägt die EU vor, ihr eigenes System zur Ermittlung von Terrorismus-Finanzierungen zu entwickeln. Die Mitteilung bietet einen allgemeinen Überblick über mögliche Hauptmassnahmen des TFTS. Drei Szenarien werden darin dargestellt. Die Absicht der Kommission scheint unklar: Möchte die Kommission nun den Status Quo beibehalten und die Mängel des geltenden US-TFTP abändern oder beabsichtigt sie, ein völlig neues EU-TFTS zu erarbeiten. Auf Grund dieser Ungewissheit war es der Arbeitsgruppe zum gegebenen Zeitpunkt unmöglich, eine voll umfängliche Überprüfung der Datenschutzpunkte vorzunehmen, bis das TFTS ausreichend definiert ist, insbesondere im Bezug auf dessen rechtliche Basis, Architektur und Funktionen.[105]

5.2. Gemeinsame Kontrollinstanz Schengen

Zur Vorbereitung des Schengenbeitritts nahmen wir in der **Gemeinsamen Kontrollinstanz Schengen** weiterhin den Status als Beobachter wahr.[106] Die Kontrollinstanz überwacht, ob die Verwendung der Daten im Schengen Informationssystem (SIS) mit dem Schengen Durchführungsübereinkommen übereinstimmt. Dazu werden regelmässig **gemeinsame Untersuchungen** durchgeführt, die von den nationalen Kotrollinstanzen vorgenommen werden. Die Tätigkeiten konzentrierten sich dabei auf eine

tion/opinion-recommendation/files/2011/wp187_de.pdf

100 Vgl. hierzu Philipp Mittelberger, Die Einwilligung als zentrales Element des Datenschutzrechts, in: LJZ 4/06 (S. 135ff.), dessen Ausführungen nichts an ihrer Gültigkeit eingebüsst haben, http://www.llv.li/pdf-llv-li-die_einwilligung_als_zentrales_element_des_datenschutzrechts.pdf. Die Legaldefinition der Einwilligung ist in Art. 3 Abs. 1 Bst. m DSG geregelt, die lautet: „Jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass Daten, die sie betreffen, bearbeitet werden." Diese Definition wird in Art. 4 Abs. 2 DSG ergänzt: „Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung ausdrücklich erfolgen."

101 Diese Formulierung findet sich in der RL 95/46/EG mit diesem Wortlaut zwar nicht. Die RL 95/46/EG sieht aber vor, dass die Einwilligung „ohne jeden Zweifel" abgegeben worden sein muss (Art. 7 Bst. a).

102 Vgl. hierzu Urteil des EuGH vom 09. November 2010, verb Rs C-92/09 und C-93/09, Schecke und Eifert, Randziffer 62 ff.; http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=de&num=79898890C19090092&doc=T&ouvert=T&seance=ARRET.

103 http://ec.europa.eu/home-affairs/news/intro/docs/110713/1_EN_ACT_part1_v15.pdf

104 Vgl. dazu auch „SWIFT", Tätigkeitsbericht 2007, 3.2.

105 Die Ziele eines EU-Systems zum Aufspüren der Terrorismusfinanzierung bestehen in einem wirksamen Beitrag zur Bekämpfung von Terrorismus und seiner Finanzierung innerhalb der EU und in einem Beitrag zur Begrenzung der in Drittstaaten übermittelten Menge personenbezogener Daten. Die Kommission müsste nach Ansicht der Arbeitsgruppe in ihrer Folgenabschätzung den überzeugenden Beweis erbringen, dass das TFTS für die Zwecke der Terrorismus-Bekämpfung nachweislich notwendig und verhältnismässig ist, um bestimmte Probleme zu lösen.

106 Vgl. beispielsweise Tätigkeitsbericht 2010, 4.2.

Follow-up-Untersuchung zu Art. 99 SDÜ[107] und eine erstmalige Untersuchung zu Art. 95 SDÜ. Letztere betrifft Ausschreibungen von Personen, die von Justizbehörden zum Zwecke der Auslieferung gesucht werden. Diese soll voraussichtlich im Frühjahr 2012 abgeschlossen sein. Eine solche Ausschreibung darf nur unter bestimmten Voraussetzungen erfolgen. Beispielsweise hat die ausschreibende Stelle vor der Ausschreibung zu prüfen, ob eine Festnahme nach dem Recht der ersuchten Behörde zulässig ist. Die Arbeit ist in diesem Zusammenhang wichtig, da wir den Experten im Rahmen der Datenschutzevaluation die Durchführung solcher Kontrollen zugesagt hatten.[108] Ausserdem finden solche Evaluationen wiederholt statt.

Darüber hinaus befasste sich die Gemeinsame Kontrollinstanz Schengen unter anderem mit der systematischen Abfrage von Hotelmeldungen im SIS, über welche eine Delegation berichtet hatte. Es stellte sich dabei die Frage, ob eine automatisierte, systematische Überprüfung von Hotelmeldungen mit dem SDÜ vereinbar sei.[109] Nach Auffassung der Gemeinsamen Kontrollinstanz Schengen widerspricht der voraussetzungslose, systematische Abgleich dem Sinn des SDÜ. Es braucht stets einen Grund, eine bestimmte Person zu kontrollieren bzw. für einen Abgleich mit den SIS-Daten. Sofern ein nationales Gesetz den Abgleich von Hotelmeldungen mit dem SIS vorsieht, müsste es verhältnismässig ausgestaltet sein. Wir haben die Landespolizei über diese Auslegung informiert und dazu angehalten, sie bei der allfälligen Schaffung gesetzlicher Bestimmungen zu berücksichtigen.

5.3. Eurodac Supervision Coordination Group

Wie bereits im Vorjahr geplant, hat das Aufsichtsgremium über die Eurodac eine gemeinsame **Untersuchung zur vorzeitigen Löschung der Fingerabdruck-Daten** durchgeführt.[110] Das Eurodac-System sieht strikte zeitliche Fristen für die Speicherung von Daten vor. Diese Fristen differieren zwar je nach Kategorie von Daten, der Grundsatz jedoch sieht eine automatische Löschung der Daten aus der Zentraleinheit spätestens zehn Jahre nach Abnahme der Fingerabdrücke vor. Zusätzlich zu diesem System der automatischen Löschung sieht die Eurodac-Verordnung eine vorzeitige Löschung in bestimmten Fällen vor, etwa wenn sich der Status eines Asylsuchenden geändert hat. Beispielsweise ist das der Fall, wenn ein Asylsuchender die Staatsbürgerschaft eines EU Mitgliedstaates erlangt. Dies entspricht auch dem allgemeinen Grundsatz, dass Daten nicht länger als notwendig aufbewahrt werden dürfen, um den Zweck zu erreichen, für den sie gesammelt wurden.

Bei der Untersuchung ging es um die korrekte Umsetzung und auch um Verbesserungsmöglichkeiten.

Die meisten Mitgliedstaaten haben etablierte Verfahren für die vorzeitige Löschung. Die Eurodac Verordnung sieht als Zeitrahmen für die Löschung „so bald wie möglich" vor. In manchen Mitgliedstaaten werden die Daten sofort gelöscht, in manchen einmal täglich, in wieder anderen dauert es bis zu einem Monat. Eine Empfehlung lautet dahingehend, Verfahren zur vorzeitigen Löschung sowie klare und kurze Fristen festzulegen.

Auffallend war im Rahmen der Untersuchung, dass es insgesamt nur wenige Anfragen von den betroffenen Personen zur vorzeitigen Löschung gibt. Das könnte auch mit dem Umstand zusammenhängen, dass nur wenige Mitgliedstaaten über eine rechtliche Grundlage für Information verfügen. Die Gruppe empfiehlt deshalb, den Betroffenen entsprechende Informationen im Hinblick auf die vorzeitige Löschung zu geben, ebenso wie zu den Datenschutzbestimmungen. Die Information der Betroffenen über ihre Rechte ist wesentlich dafür, dass diese ihre Rechte wahrnehmen können.

Darüber hinaus sollen in den Mitgliedstaaten bessere Statistiken geführt werden. Adäquate und vergleichbare Statistiken sind eine wesentliche Voraussetzung für Entscheidungen und Aktionen sowie zur Überprüfung der Effektivität.

107 Bei Art. 99 SDÜ geht es um Ausschreibungen zur verdeckten Registrierung oder der gezielten Kontrolle im Zusammenhang mit der Verfolgung schwerer Straftaten oder der Abwehr von Gefahren für die öffentliche Sicherheit.
108 Vgl. oben, 1.5.
109 Art. 45 SDÜ.
110 Vgl. Tätigkeitsbericht 2010, 4.3.

5.4. Europarat

Das von Liechtenstein ratifizierte Datenschutzabkommen des Europarates stammt aus dem Jahr 1981 und somit aus einer Zeit, in der die heutige Vernetzung noch gar nicht möglich war. Somit überrascht es nicht, dass neben einer Überarbeitung der Datenschutzrichtlinie auch eine **Revision des Abkommens** angegangen wurde. Diese Revision war der hauptsächliche Gegenstand der jährlichen Sitzung des Konventionsausschusses, in dem wir Liechtenstein vertreten. Der Entwurf des neuen Abkommens sollte sich am neuen Text aus Brüssel anlehnen, der jedoch zur Zeit der Sitzung noch nicht bekannt war. Dennoch konnten einige grundsätzliche Punkte behandelt werden. So soll das neue Abkommen auch Nicht-Mitgliedstaaten des Europarates für einen Beitritt offen stehen. Dadurch erhofft man sich unter anderem eine Verbreitung der Datenschutzgrundsätze in Gebiete ausserhalb Europas. Es steht jedoch noch viel Arbeit vor der Tür, bis mit einem neuen Abkommen des Europarates gerechnet werden kann. Für Liechtenstein als EWR-Mitglied steht die Überarbeitung der Datenschutzrichtlinie klar im Vordergrund.

Daneben wird unter anderem die Aktualität der **Empfehlung des Europarates über die Nutzung personenbezogener Daten im Polizeibereich (87) 15** geprüft. Dazu war ein umfassender Fragebogen über die Umsetzung der Empfehlung in den Mitgliedstaaten verschickt worden, den wir zusammen mit der Landespolizei beantwortet haben. Das genannte Datenschutzabkommen wie die allgemeine Datenschutzrichtlinie sehen Ausnahmen im Polizeibereich vor. Die Empfehlung ist zwar nicht rechtlich verbindlich, hat aber einen Standard im Polizeibereich gesetzt und wird deshalb bis heute insbesondere bei Schengen als ein Referenzdokument verwendet. Da Schengen-Evaluationen wiederholt stattfinden, kann davon ausgegangen werden, dass eine Überarbeitung der Empfehlung in der Praxis von Bedeutung sein wird.

5.5. Europäische Datenschutzkonferenz

Die **Working Party on Police and Justice (WPPJ)** beschäftigte sich unter anderem mit einem Assessment von Datenschutzrisiken im Strafverfolgungsbereich. In der polizeilichen Arbeit haben sich fünf Knackpunkte herauskristallisiert. Diese betreffen Daten, die ohne Kenntnis der Betroffenen erhoben werden, Daten über nicht Verdächtige, sensitive Daten, Profiling oder den internationalen Datenaustausch (v.a. im Rahmen von Schengen, Interpol und Europol). Insbesondere die Datenbearbeitung über unverdächtige Personen soll im Rahmen der WPPJ näher untersucht werden. Die WPPJ hat auch die Entwicklungen der genannten Rechtsinstrumente des Europarates für den Polizeibereich verfolgt. Hinsichtlich einer verstärkten Zusammenarbeit mit dem Europarat in diesem Bereich ist bereits eine Kontaktaufnahme erfolgt.

Daneben war die WPPJ aber auch mit ihrer eigenen Zukunft beschäftigt, da sich die Struktur der Arbeitsgruppe durch den Wegfall der Drei-Säulen-Struktur mit dem Vertrag von Lissabon ändern wird.

5.6. Internationale Datenschutzkonferenz

Die **International Working Group on Data Protection in Telecommunications (IWGDPT)** ist der Internationalen Datenschutzkonferenz unterstellt[111]. 2011 wurde unter anderem ein Arbeitspapier zu Smart Metering[112] ausgearbeitet und angenommen. Datenschutzrechtliche Probleme ergeben sich insbesondere dadurch, dass durch den **Einsatz von Smart Metern** bis zu achtmal mehr Daten generiert werden als heute üblich. Die permanente Beobachtung des Stromverbrauchs könnte die ungefähre Anzahl der Bewohner in einem Haushalt verraten, wann sie anwesend sind, sowie wann sie wach sind oder schlafen. Dies gefährdet die Unverletzlichkeit der Wohnung, und solche intimen Details des täglichen Lebens erfordern ein hohes Schutzniveau. Die Gruppe empfiehlt demgemäss,

111 Die „International Working Group on Data Protection in Telecommunications" wurde im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten im Jahr 1983 auf Initiative des Berliner Datenschutzbeauftragten gegründet. Seither wurde eine Vielzahl von Empfehlungen zur Verbesserung des Datenschutzes in der Telekommunikation erarbeitet. Teilnehmer sind Datenschutzbehörden, aber auch Regierungsstellen, Vertreter internationaler Organisationen oder Wissenschaftler aus aller Welt. http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt.

112 Als Smart Meter („intelligente Stromzähler") werden Messgeräte zur Stromverbrauchsmessung bezeichnet, deren gemeinsame Charakteristik es ist, in bestimmten Zeitabständen (Minuten- oder Stundentakt) den Energieverbrauch von Haushalten zu bestimmen und aufzuzeichnen. Daneben sind die Stromzähler tendenziell mit einer bidirektionalen Kommunikationsfunktionalität ausgestattet; Versorgungsunternehmen können die Messgeräte z.B. aus der Ferne ablesen oder der Verbraucher kann über ein Online-Web-Portal auf seine eigene Energieverbrauchsstatistik zugreifen.

dass *der Datenschutz ein wesentlicher Bestandteil bei der Ausgestaltung von Smart-Meter-Systemen und -Anwendungen sein sollte.*[113]

5.7. Privatim – Vereinigung der Schweizer Datenschutzbeauftragten

Als langjähriges Mitglied des Vereins der schweizerischen Datenschutzbeauftragten *privatim* luden wir den Verein für das Frühjahrsplenum nach Vaduz ein. Neben den statutarischen Geschäften wurden auch für Liechtenstein wesentliche Themen diskutiert, wie die *Rolle der Datenschutzbeauftragten oder die Herausforderungen für die Weiterentwicklung des Datenschutzrechts.*

Die Kernaufgabe der „Arbeitsgruppe-ICT" (AG-ICT) besteht in der Beobachtung und Beurteilung von technischen Entwicklungen. Bei der Erarbeitung einer „Checkliste für Benutzungsreglemente betreffend mobile Geräte" haben wir massgeblich mitgewirkt. Diese Checkliste dient der Hilfestellung zur Prüfung und Erstellung von Reglementen über die Benutzung und Handhabung mobiler Endgeräte. Sie soll insbesondere ermöglichen, Reglemente auf inhaltliche Vollständigkeit zu überprüfen und richtet sich speziell an Verantwortliche im Bereich der Informationstechnologie, die Benutzungsreglemente und Dienstvorschriften für die Nutzung von mobilen Arbeitsplätzen (z.B. Notebooks, Tablets, Smartphones, Mobiltelefone, PDAs) erstellen.

5.8. Arbeitskreis Technik

Unter der Leitung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Mecklenburg-Vorpommern besteht ein Arbeitskreis „Technische und organisatorische Datenschutzfragen" (AK Technik) als Gremium der Konferenz der deutschen Datenschutzbeauftragten des Bundes und der Länder. Das Thema Cloud Computing beschäftigte auch den Arbeitskreis, der hierzu eine Orientierungshilfe annahm, die auch für unsere Arbeit hilfreich war.[114]

6. In eigener Sache

Datenschutz, und damit der Schutz der Privatsphäre ist eine Querschnittsmaterie, die alle möglichen Lebensbereiche betreffen kann, wenn Personendaten betroffen sind. Dies ist die Regel, geht es doch vor allem bei Behörden, aber oft auch bei Unternehmen darum, irgendein Verhältnis zu betroffenen Personen zu definieren; sei dies nun als Bürger, Kunde, Arbeitnehmer oder sonst wie betroffener Dritter. Mit anderen Worten ist die Bearbeitung von Personendaten, in der einen oder anderen Form, wohl die Regel. Dieser breite Geltungsbereich des Gesetzes bringt mit sich, dass es in der Praxis nicht immer berücksichtigt wird. Dazu kommt, dass der Begriff „Datenschutz" nicht sehr greifbar ist.

So wurde 2009 eine allgemeine Pflicht zur Bewilligung von Videoüberwachungsanlagen im öffentlich zugänglichen Bereich eingeführt, ohne aber Sanktionen vorzusehen. Diese allgemeine Pflicht führte wohl mit dem letztgenannten Umstand dazu, dass bis heute dieser Pflicht nicht in einem befriedigenden Masse nachgekommen wurde. Wir hätten gewisse Möglichkeiten, darauf zu achten, dass das Gesetz eingehalten wird. Doch abgesehen von der Ressourcenfrage stellt sich auch diejenige der *Durchsetzung*. Im Unterschied zu anderen Datenschutzbehörden in Europa können wir nur Empfehlungen erlassen und nicht selbst entscheiden. Dieses Verfahren ist schwerfällig.[115] In diesem Zusammenhang der Durchsetzung ist ein Ungleichgewicht festzustellen: So ist beispielsweise der Versand einer unerbetenen Nachricht mit einer Busse bis zu CHF 20'000 zu bestrafen.[116] Die Strafbestimmungen des DSG greifen demgegenüber meist nur, wenn besonders schützenswerte Daten bzw. Persönlichkeitsprofile betroffen sind[117] (wobei es zudem an einer klaren Definition des Begriffs des Persönlichkeitsprofils fehlt). Hier fehlt es schon an abschreckenden Bestimmungen.

Das Beispiel der 2009 geschaffenen Institution des Datenschutzverantwortlichen zeigt ein weiteres Element: Dem Gesetz bzw. einigen Bestimmungen wird oft erst nachgekommen, wenn wir die Initiative er-

113 „Privacy by Design und Smart Metering: Minimierung personenbezogener Informationen zur Wahrung der Privatsphäre", http://www.datenschutz-berlin.de/attachments/856/675.43.35.pdf.

114 http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf; s. weiters 1.6.

115 Was die Frage der Videoüberwachung angeht, kommt dazu, dass wir nur denjenigen eine Empfehlung zulassen kommen könnten, die die Videoüberwachung so führen, dass sie sichtbar ist. Diejenigen, die sie nicht transparent führen, würden solchen Massnahmen entkommen.

116 Art. 70 Abs. 1 Buchstabe f KomG.

117 Art. 39 und 41 DSG.

greifen. So gab es bis Ende 2010 keinen einzigen Datenschutzverantwortlichen. Wir erklärten es 2011 zu einem unserer Ziele, diese Institution bekannt zu machen und bei Behörden und Unternehmen die Schaffung eines Datenschutzverantwortlichen zu fördern. Bis Ende des Jahres konnten wir 25 Datenschutzverantwortliche auf unserer Internetliste verzeichnen.[118] Dies in den meisten Fällen dank unserer Initiative. Dies mag wiederum mit dem sehr weiten Anwendungsbereich des Gesetzes zu tun haben. Die Schaffung eines Datenschutzverantwortlichen ist in Liechtenstein freiwillig. Für alle. Unserer Ansicht nach müsste der Gesetzgeber differenzierende Bestimmungen schaffen. Für Grossunternehmen und solche, die mit „problematischen" Daten arbeiten, sollten gewisse Aufgaben (Meldung zum Register der Datensammlungen, Schaffung eines Datenschutzverantwortlichen, etc.) zur Pflicht werden. KMUs sollten dagegen im Sinne der Agenda 2020 der Regierung möglichst wenig verpflichtet werden, ausser wenn sie mit „problematischen" Daten zu tun haben. Eine solche Konkretisierung des Anwendungsbereichs würde allen dienen.

Im vergangenen Jahr wurden wir auf Grund unserer Sachkenntnisse in einer noch nicht abgeschlossenen Sache unbeabsichtigt mit *legislativen* Aufgaben betraut. Dies muss ein Einzelfall bleiben. Wir begrüssen es, wenn wir frühzeitig in Vorhaben einbezogen werden. Damit sinkt das Risiko, dass im Nachhinein Anpassungen notwendig werden. Das Gesetz hält jedoch explizit fest: „Die Datenschutzstelle nimmt Stellung zu Vorlagen und Erlassen, die für den Datenschutz erheblich sind und überprüft insbesondere deren Übereinstimmung mit den Bestimmungen der Richtlinie 95/46/EG".[119] Mit anderen Worten sind wir nicht zuständig für die Ausschaffung von rechtlichen Grundlagen.

Im Rahmen der Diskussion unseres Tätigkeitsberichtes gab es im Landtag die Anregung der *Schaffung einer regelmässigen und fixen Rubrik in den Tageszeitungen*.[120] Wir haben diesbezüglich Abklärungen getroffen und kamen zum Ergebnis, dass als erster Schritt ein Beitrag im dreimal jährlich erscheinenden PeCe Magazin erscheinen soll. Das PeCe Magazin scheint auf Grund der auch in diesem Tätigkeitsbericht behandelten Themen wie Cloud Computing, Google Analytics und ähnlichem eine gute Plattform zu sein. Wir möchten zuerst abwarten, wie sich dies entwickelt, ehe wir diese Idee im Sinne der Anregung ausbauen. Zudem ist daran zu erinnern, dass unsere Internetseite die Hauptinformationsplattform darstellt. Ausserdem verfügen wir über eine bescheidene Präsenz auf Facebook.[121] Die Frage einer Rubrik in den Tageszeitungen soll aber später wieder aufgegriffen werden. Eine weitere Anregung bestand darin, Informationen über uns, wie Organigramm, personelle Besetzung sowie Information über den finanziellen Hintergrund aufzunehmen. Das Organigramm, aus dem auch die personelle Besetzung ersichtlich ist, ist weiter hinten zu finden[122] und der finanzielle Hintergrund im Finanzgesetz 2011, das ebenfalls im Internet zugänglich ist.[123]

118 Vgl. oben, 1.6.
119 Art. 32 Abs. 1 Buchstabe d DSG.
120 Landtagsprotokoll vom 19.05.2011, Seite 728.

121 https://www.facebook.com/pages/Datenschutzstelle-Liechtenstein/364340615234
122 Vgl. Anhang.
123 http://www.gesetze.li/Seite1.jsp?LGBlm=2011535
Auch die Tätigkeitsberichte des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und des deutschen Bundesbeauftragten für den Datenschutz und die Informationssicherheit enthalten Informationen zur Organisation, nicht aber zu den Finanzen, vgl.: http://www.edoeb.admin.ch/dokumentation/00445/00509/01732/index.html?lang=de bzw. http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23_TB_09_10.pdf?__blob=publicationFile

7. Ausblick

Mit der erneuten *Revision des DSG* wurde dessen Anwendungsbereich weiter ausgedehnt. Nachdem bereits 2009 der Vorbehalt in Bezug auf „Daten, die im Rahmen des Sorgfaltspflichtgesetzes anzulegen sind“[124] und die Ausnahme öffentlicher Register des Privatrechtsverkehrs vom Geltungsbereich des DSG weggefallen sind, ist das DSG mit der letztjährigen Revision nun auch im Bereich von „Straf- und Rechtshilfeverfahren“ anwendbar.[125] Dem bleibt anzufügen, dass auch vor allem die Ausnahme der hängigen Zivilverfahren von der Richtlinie nicht abgedeckt sind. Mit der *Schaffung des ZPR-Gesetzes* wurde einer langjährigen Forderung nachgekommen.[126] Wir sind in der ZPR-Kommission vertreten, die Datenzugriffe bewilligen kann. Zudem werden wir das neu geschaffene Amt für Informatik bei der Schaffung der technischen Neuerungen zur Gewährleistung der Verhältnismässigkeit des Zugriffs auf Daten begleiten. Hier sieht das Gesetz keine Übergangsregelung vor. Somit sind die Massnahmen sofort zu treffen. Unseres Wissens ist bisher noch nichts geschehen. Wir werden darauf schauen, dass der Wille des Gesetzgebers umgesetzt wird.[127] Im privaten Bereich wird zudem die *Meldepflicht von Datensammlungen* generell eingeführt. Diese Meldepflicht sollte sich unseres Erachtens auf die „problematischen“ Datenbearbeitungen beschränken. Im Rahmen der Datenschutzevaluation zu *Schengen* wurde von europäischen Experten ein Ausbau unserer Ressourcen gefordert, damit wir unseren (neuen) Aufgaben nachkommen können. Dies ist bis heute nicht erfolgt. In Liechtenstein gibt es keine Institution, die wie das deutsche Bundesamt für Informationssicherheit[128] oder die schweizerische Melde- und Analysestelle Informationssicherung (MELANI)[129] *vor Gefahren im Internet warnt*. Diese Lücke sollte geschlossen werden. Im Sinne verschiedener Voten bei der Diskussion unseres Tätigkeitsberichtes 2010 sind wir der Ansicht, dass dies eine neue, für die betroffenen Personen sehr sinnvolle Aufgabe, wäre.[130]

Ergebnis: Die wiederholte Ausdehnung des Anwendungsbereichs des Gesetzes, internationale Verpflichtungen wie der erfolgte Schengen-Beitritt, die erwähnten Übergangsmassnahmen im Rahmen des ZPR oder die rasanten technischen Entwicklungen in einer Welt der Globalisierung führen zu einer stetigen Arbeitszunahme.

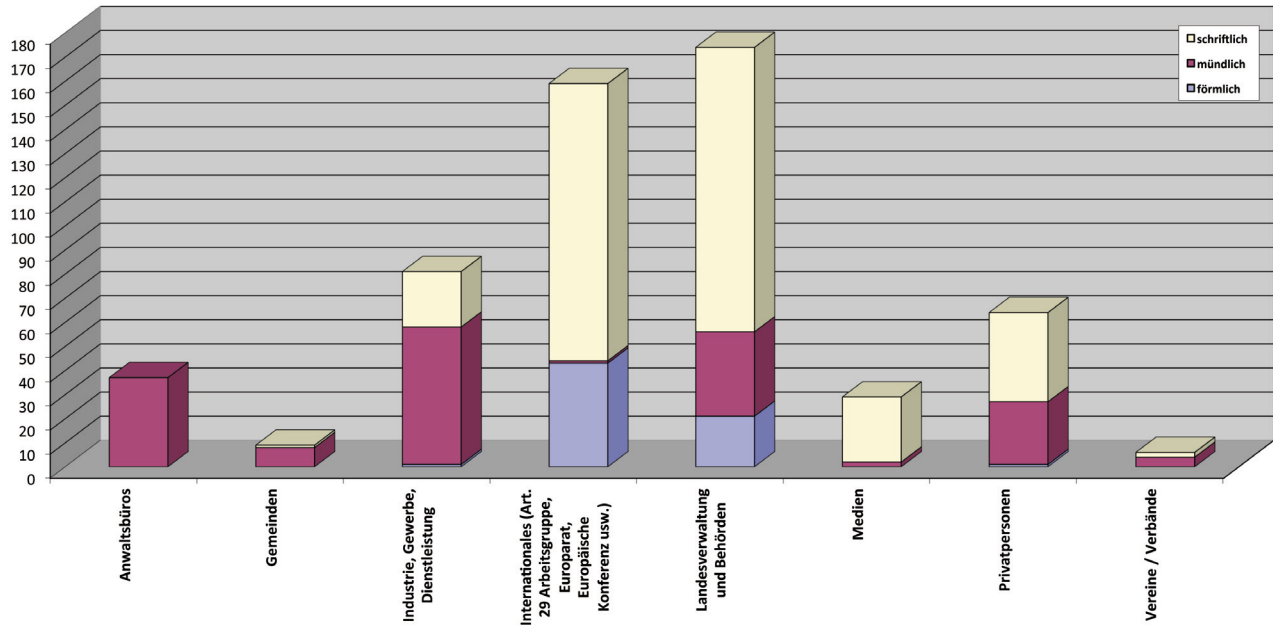
Dies alles soll in einem für Liechtenstein vernünftigen Mass angegangen werden. Der Ende Januar 2012 durch die Europäische Kommission vorgeschlagene neue Rechtsrahmen[131] bestätigt diesen Eindruck: Der Datenschutz, und damit der Schutz der Privatsphäre, der in Liechtenstein immer wieder betont wird, wird noch wichtiger. Wir leisten dazu unseren bestmöglichen Beitrag.

124 Vgl. auch Tätigkeitsbericht 2009, 1.6.
125 Diese Änderungen des DSG treten gleichzeitig mit der revidierten StPO am 1.10.2012 in Kraft.
126 Vgl. dazu bereits Tätigkeitsbericht 2003, 4.1.2.
127 Gemäss der Regierung (Bericht und Antrag Nr. 67/2011, S. 9ff) sowie einem Rechtsgutachten eines ausländischen Experten sind zumindest folgende Massnahmen nötig: 1.) Einschränkung des Zugriffs auf Vergangenheitsdaten; 2.) Herstellung der Verhältnismässigkeit im Sinne des DSG; Schaffung eines Mechanismus, der einem Sachbearbeiter lediglich die für dessen Tätigkeit erforderlichen Datenbestände und Informationen bereit stellt. 3.) Implementierung des gesetzlich vorgesehenen Sperrrechts; Zukünftig muss ein Datensatz einer Person mit einem im DSG vorgesehenen Sperrhinweis markiert werden können. 4.) Anonymisierung von Testdaten; Diese Forderung des Experten ist unserer Ansicht nach ebenfalls umzusetzen.Gemäss der Regierung soll auf Grund der damit verbundenen hohen Entwicklungskosten auf eine Anonymisierung zu Test- und Schulungszwecken vorerst verzichtet werden. Ein Eingriff in die Privatsphäre kann nicht mit Kosten gerechtfertigt werden. Gerade in Test- und Schulungsumgebungen greifen die üblichen Kontrollmechanismen nicht und der mögliche Missbrauch ist hier besonders hoch.
128 https://www.bsi.bund.de/DE/Home/home_node.html
129 https://www.melani.admin.ch
130 Schliesslich geht es hierbei um den vorbeugenden Schutz in Bezug auf Gefahren im Internet. Dies mag zwar keine eigentliche Kernaufgabe einer Datenschutzbehörde sein; doch sollte die in Liechtenstein bestehende Lücke unbedingt geschlossen werden. So lange es hier keine andere Institution gibt, nehmen wir diese Aufgabe gerne wahr.
131 http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

8. Anhang

8.1. Statistik: Beratung privater Personen und Behörden

Die Beratung privater Personen und Behörden ist eine Kernaufgabe. Im Berichtsjahr gingen insgesamt 559 Anfragen ein, so viele Anfragen wie nie zuvor. Gegenüber dem Vorjahr bedeutet das eine Zunahme um 36 Anfragen. Wie die nachfolgende Übersicht zeigt, stammen die meisten Anfragen nach wie vor von der Landesverwaltung.

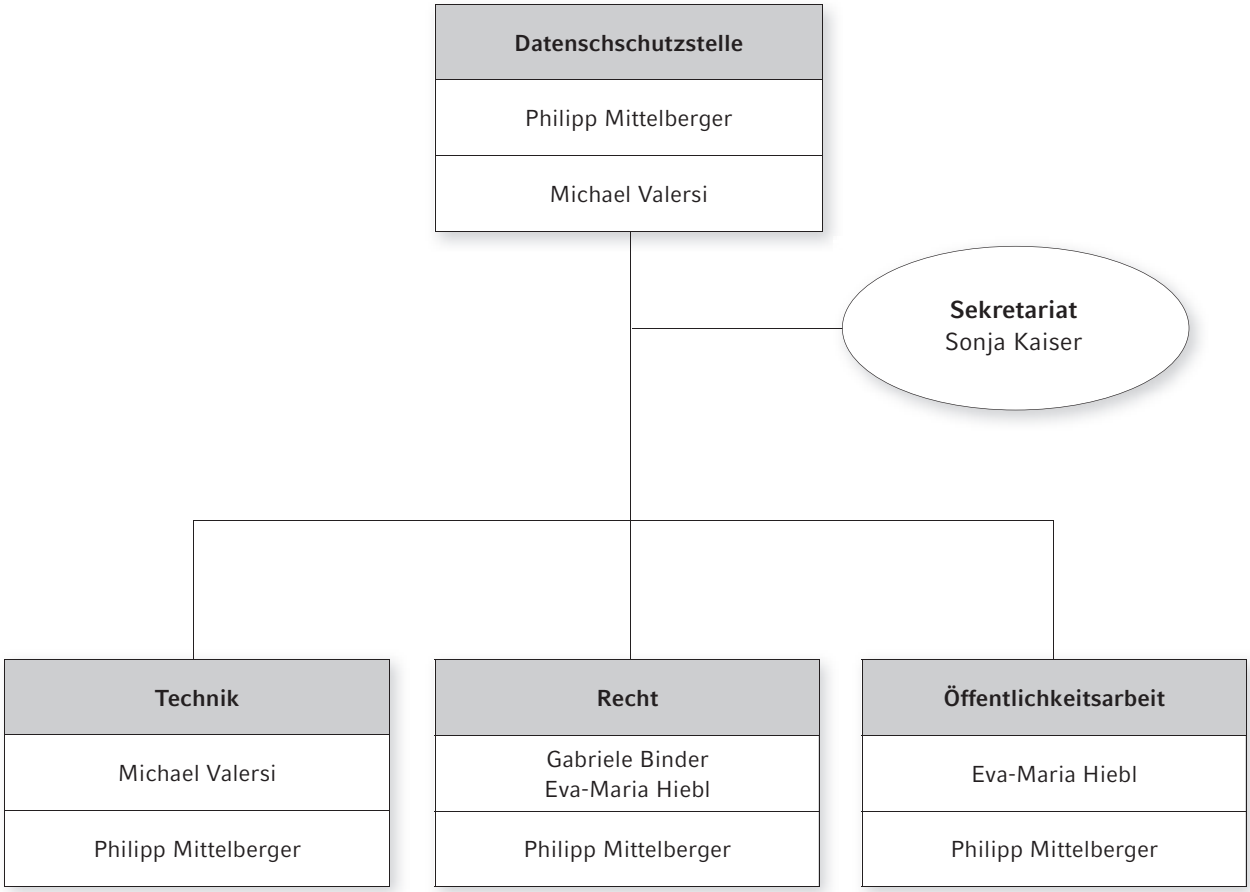


Gesetzesthemen

Aufgegliedert nach Sachgebieten standen allgemeine Datenschutzthemen, dicht gefolgt von Anfragen zur Datenbekanntgabe im Inland, im Vordergrund. Vertikal sind die Themen und Sachgebiete aufgeführt, auf horizontaler Ebene, wer angefragt hat.

	Anwaltsbüros	Gemeinden	Industrie, Gewerbe, Dienstleistungen	Internationales	Landesverwaltung und Behörden	Medien	Private Personen	Vereine / Verbände
Datenschutz allgemein	8	2	29	45	46	8	21	2
andere Gesetzesvorhaben					19			
Arbeitsbereich			3		2		4	1
Datenbekanntgabe Inland		3	5		33	3	2	1
Datenbekanntgabe Auslandsbezug	22	2	15	1	7		1	
Geltenmachung gesetzlicher Rechte	4	1	1		3	6	17	
Gesundheit / Soziales							1	
Keine Zuständigkeit DSS							6	
Polizei / Sicherheit		1		110	5	1		
Register der Datensammlungen	1		12		17	4	2	2
Schengen / Dublin				2	11		1	
Technologischer Datenschutz			4		3	7	6	
Telekommunikation			1		2			
Umsetzung / Anwendung europäischen Rechts				1				
Vernehmlassung ohne Stellungsnahme					14			
Videoüberwachung			4		3		3	
Wirtschaft / Finanzen Gewerbe / Versicherungen	2		5		1			
Gesamtergebnis	**37**	**9**	**81**	**159**	**174**	**29**	**64**	**6**

8.2. Organigramm



DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Kirchstrasse 8
FL-9490 Vaduz

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

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