DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

TÄTIGKEITSBERICHT 2013

Datenschutzstelle des Fürstentums Liechtenstein

INHALTSVERZEICHNIS

EINLEITUNG

Auch im vergangenen Jahr konnten wir wieder zahlreiche Anfragen von Bürgern, Behörden und Unternehmen beantworten. Die Zunahme auf 669 Anfragen stellt erneut einen Höchstwert dar und zeigt, dass die **Beratung** einen hohen Stellenwert hat. Einige dieser Anfragen werden im Bericht ausführlich dargestellt, da sie aus unserer Sicht für die Öffentlichkeit von Interesse sind. Darüber hinaus war unsere Arbeit von folgenden Schwerpunkten gekennzeichnet:

Gemäss unserer repräsentativen Umfrage von 2012 weiss die Bevölkerung nur wenig über Datenschutz. Dies bestätigte uns darin, bei unserer Arbeit die **Sensibilisierung** in den Mittelpunkt zu stellen. Dementsprechend verstärkten wir unsere Tätigkeiten: Neben dem von uns organisierten *Europäischen Datenschutztag* nahmen wir an einer Podiumsdiskussion des Vereins Sicheres Liechtenstein zum *NSA-Skandal* wie auch an verschiedenen *Schulungen*, u. a. zur *Sensibilisierung von Jugendlichen* teil (siehe 2.2).

Unser **Angebot an Hilfsmitteln** für die Bevölkerung und für einzelne Zielgruppen haben wir weiter ausgebaut. Dazu gehören z. B. *Tipps für den Selbstdatenschutz*, die *Richtlinie für die Bearbeitung von Personendaten im Arbeitsbereich*, eine *Muster-Datenschutzerklärung für Betreiber von Internetseiten* sowie weiteres Informationsmaterial zu aktuellen Themen. Diese Hilfsmittel stellen wir jeweils auf unserer Internetseite zur Verfügung (siehe 2.3).

Eine veränderte und intensivere Nutzung von technischen Instrumenten – hierzu gehört z. B. das Thema *Bring Your Own Device (BYOD)* – und neue **technologische Entwicklungen** wie beispielsweise *Mikrodrohnen* oder *Google Glass* stellen den Schutz der Privatsphäre und der persönlichen Daten vor neue, grosse Herausforderungen. *Das Recht auf das eigene Bild* wird dadurch zusätzlich gefährdet (siehe 1.2 und 1.5).

Wir sehen es als sehr wichtig an, dass wir – je nach Thema national oder in internationaler Zusammenarbeit – die Datenschutz-Anliegen möglichst frühzeitig in die Entwicklung mit einbringen können. Dies gilt insbesondere für die **Mitarbeit bei der Gesetzgebung**. Einen Schwerpunkt stellte die *Abänderung des Gesetzes über die Durchführung der internationalen Amtshilfe in Steuersachen (SteAHG)* dar (siehe 3.).

Eine unserer Aufgaben ist es, **Kontrollen** durchzuführen. Diese helfen, die Einhaltung des Datenschutzes durchzusetzen. Wir informieren im vorliegenden Bericht über den Abschluss einiger Kontrollen und das positive Ergebnis dieser Arbeit (siehe 4.).

Im Rahmen der **Zusammenarbeit mit anderen Datenschutzbehörden** stand natürlich der *NSA-Skandal* im Fokus. Dazu beschäftigten wir uns in der Artikel-29-Datenschutzgruppe u. a. mit der *neuen Geldwäscherei-Richtlinie* sowie mit dem Risiko, das die weit verbreitete Nutzung von *Apps* mit sich bringt, oder der laufenden *Datenschutzreform in Europa* (siehe 5.).

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

Vaduz, im April 2014

Dr. Philipp Mittelberger
Datenschutzbeauftragter

BERICHTERSTATTUNG 2013

Die Zahl der Anfragen, die an uns gerichtet wurden, nahm erneut zu und erreichte im vergangenen Jahr einen neuen Höchststand von 669[1]. Einige Fragen und deren Beantwortung, die für die Öffentlichkeit interessant sein dürften, werden im Folgenden dargestellt.

1. Fälle aus unserer Beratungspraxis

1.1. Wahrnehmung gesetzlicher Rechte, Beschwerden

In einer Kassensturz-Sendung wurde über die **Praktiken von Moneyhouse** berichtet.[2] Daraufhin meldeten sich bei uns Personen aus Liechtenstein, die sich darüber beschwerten, dass auch Angaben über Mitbewohner und Nachbarn erfasst werden. Moneyhouse stand bereits im Mittelpunkt von Verfahren beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).[3] Da Moneyhouse den Sitz in der Schweiz hat, ist grundsätzlich der EDÖB für Beschwerden zuständig. Deshalb wendeten wir uns an den EDÖB mit der Bitte, vor allem die Verhältnismässigkeit und Richtigkeit der Daten bei privaten Personen zu prüfen. Im Rahmen einer Stichprobe hatte sich herausgestellt, dass die Daten nicht immer aktuell waren. Wir wiesen in einer Pressemitteilung darauf hin, dass sich betroffene Personen über ein *kostenloses Auskunfts- und Lösch- bzw. Berichtigungsbegehren* selbst mit Moneyhouse in Verbindung setzen sollten.[4]

Allgemein konnte ein deutlicher **Anstieg bei den Anfragen** im Zusammenhang mit der Wahrnehmung von Rechten – insbesondere das Recht auf Auskunft und das Recht auf Löschung – verzeichnet werden.[5]

Es gab allerdings keine nennenswerten Fälle, in denen wir weiter einschreiten mussten. Diese Entwicklung ist grundsätzlich positiv, da unser Ansatz darin besteht, vorwiegend durch *Sensibilisierung und Beratung* für die Wahrung der Privatsphäre zu sorgen. Es ist allerdings auch möglich, dass wir nicht von allen Beschwerden Kenntnis erhalten haben, da insbesondere Beschwerden gegen behördliche Verfügungen direkt bei der Datenschutzkommission eingereicht werden können,[6] ohne dass wir zuvor mit der Angelegenheit befasst gewesen sind.

Die **Datenschutzkommission (DSK)** wurde mit der Schaffung des Datenschutzgesetzes im Jahr 2002 ins Leben gerufen. Sie kann im öffentlichen Bereich Entscheide fassen; wir handeln zum Teil als Vorinstanz. Die Bestimmungen über die Aufgaben der DSK und insbesondere über die Zuständigkeit und den Rechtsmittelhinweis in Verfügungen hat in der Praxis immer wieder zu Problemen geführt, denn im Gesetz ist nicht klar genug abgegrenzt, für welche konkreten „Datenschutzfragen" die DSK zuständig ist.[7] Auf diese Problematik hatten wir schon vor einigen Jahren hingewiesen. Wir erkundigten uns auf informellem Weg in Bern, wie diese Problematik in der Schweiz gehandhabt wird. Leider erhielten wir keine befriedigende Antwort, was wohl damit zu tun hat, dass sich die Rechtslage in der Schweiz geändert hatte. Die Eidgenössische Datenschutzkommission war vor einigen Jahren abgeschafft worden. Auch in Liechtenstein scheint uns eine Klärung der Zuständigkeit und der Ausgestaltung der DSK notwendig, da sie offensichtlich nur wenige Fälle erhält: Wir haben 2013 von der DSK keinen einzigen Entscheid zugestellt bekommen.[8] Im Zuge der Regierungs- und Verwaltungsreform II[9] werden alle Kommissionen vor ihrer Neubestellung auf Notwendigkeit, Aufgaben und Zusammensetzung geprüft. Dies schreibt die Regierung auch in der Beantwortung der *Interpellation zu Kommissionen*. Aus Anlass dieser Prüfung könnte eine neue Lösung gesucht werden. Wir regten bei der Regierung die Klärung der erwähnten Problematik an.

1 2012 waren es 640; siehe auch Details im Anhang.
2 Moneyhouse veröffentlichte auf seiner Internetseite zusätzlich zu den Handelsregister- und Firmendaten über acht Millionen Einträge von Privatpersonen (u. a. Name, Adresse und Staatsangehörigkeit). Diese Personendaten werden (ohne das explizite Einverständnis der betroffenen Personen) aus unterschiedlichen Quellen gesammelt, miteinander verknüpft und, teilweise gegen Gebühr, öffentlich zur Verfügung gestellt. Somit sind sie geeignet, die Persönlichkeit einer grossen Anzahl von Leuten zu verletzen.
3 Siehe hierzu die ausführliche Darstellung des EDÖB unter http://www.edoeb.admin.ch/dokumentation/00153/01073/01097/index.html?lang=de mit weiteren Verweisen auf ergangene Empfehlungen des EDÖB und Entscheidungen des Schweizer Bundesverwaltungsgerichts.
4 Das entsprechende Formular kann hier heruntergeladen werden: http://www.edoeb.admin.ch/datenschutz/00626/00747/01022/index.html?lang=de.
5 2013 gab es insgesamt 58 Anfragen zur Geltendmachung von Rechten, 2012 waren es 44.
6 Vgl. Art. 34 Bst. b DSG.
7 Vgl. Art. 34 Bst. b DSG sowie Tätigkeitsbericht 2010, 1.1. und Tätigkeitsbericht 2011, 1.1.
8 Der Gesetzgeber hat bestimmt, dass die DSK uns alle Entscheide bekanntgibt, vgl. Art. 35 Abs. 2 DSV.
9 Gesetz über die Regierungs- und Verwaltungsreform, RVOG, Art. 47.

1.2. Technologischer Datenschutz

Durch die technologische Entwicklung ist es immer einfacher, Daten zu sammeln und zu bearbeiten. Uns wurde die Frage gestellt, inwiefern **(Mikro-) Drohnen** ein datenschutzrechtliches Problem darstellen. Mikro-Drohnen eröffnen eine neue Dimension: mit ihnen können aus der Luft Fotos bzw. Filme aufgenommen werden, ohne selbst am Ort anwesend zu sein. Dies entspricht dem Trend „weg von Big Brother, hin zu Small Brothers".[10] Früher war es vor allem der Staat, der Daten sammelte; später kam die Sammelwut von Unternehmen dazu. Heute ist es zur Regel geworden, dass private Personen Daten über Andere bearbeiten. Auch mit dem Mobiltelefon, das man heute praktisch immer dabei hat, kann man überall Fotos und Videos aufnehmen und diese dann sehr einfach im Internet veröffentlichen. Somit muss man heute ständig und überall darauf gefasst sein, aufgenommen zu werden. Auch *Google Glass* geht in diese Richtung. Das *Recht am eigenen Bild* und damit generell der Schutz der Privatsphäre werden vor neue Herausforderungen gestellt.[11] Aus Sicht des Datenschutzes verheisst die Technisierung der Gesellschaft nichts Gutes für die Zukunft.

Bring Your Own Device (BYOD) bezeichnet eine bewusste Strategie von Institutionen, wonach Mitarbeiter private Endgeräte wie Smartphones und Notebooks auch im Arbeitsumfeld nutzen dürfen. Die Kernproblematik liegt in der Vermischung von geschäftlichen und privaten Daten. Die privaten Daten des Mitarbeiters geniessen einen besonderen Schutz; der Arbeitgeber darf nur unter strengen Voraussetzungen auf diese zugreifen. Mitarbeiter dürfen auf der anderen Seite Unternehmensdaten nur im Rahmen ihrer beruflichen Tätigkeit bearbeiten. Daher ist eine (technische) Lösung für die *Trennung von privaten und geschäftlichen Daten* unabdingbar und die Nutzung privater Geräte in einem betrieblichen Umfeld auf jeden Fall zu reglementieren; eine blosse Duldung von BYOD ist zu vermeiden. In einem Reglement muss mindestens festgelegt werden, welche Daten auf die privaten Geräte übertragen und dort bearbeitet werden dürfen. Ebenfalls ist zu klären, wie bei einem Verlust des Gerätes vorgegangen wird, also ob das Unternehmen via Fernwartung auch private Daten auf dem Gerät des Mitarbeiters löschen darf. Auch die Datensicherheit stellt bei BYOD eine grosse Herausforderung dar, z. B. bezüglich fehlender Sicherheitssoftware für Smartphones, unkontrollierbaren Datenflüssen bei App-Installationen (z. B. App Store), der Foto-Funktion oder der Synchronisation mit *Public-Cloud-Diensten*. Ausserdem sind zahlreiche Endgeräte nicht für den professionellen Einsatz konzipiert, was die Durchsetzung von betrieblichen Sicherheitsrichtlinien und insbesondere die geforderte Trennung der Daten schwierig macht. Zur Unterstützung für Unternehmen bei der Erstellung von Reglementen haben wir eine entsprechende **Checkliste** erarbeitet und auf unserer Internetseite veröffentlicht. Neben technischen und organisatorischen Massnahmen ist die *Schulung von Nutzern* zentral.[12]

Wir wurden gebeten, die **Datensicherheit eines Internetauftritts** zu prüfen, auf welchem mehrere Tausend Personendatensätze verwaltet werden. Bei dieser Prüfung konnten wir direkt einhundert Personendatensätze von registrierten Benutzern einsehen, ohne Sicherheitsprüfungen überwinden zu müssen. Der Grund für diesen offensichtlich unbeabsichtigten Zugang zu den Benutzerdaten und für weitere aufgefundene Schwächen ist wahrschein-

10 Vgl. Tätigkeitsbericht 2009, I. bzw. 1.

11 Das Schweizerische Bundesgericht äusserte sich im Fall zu Google Street View auch zum Recht am eigenen Bild. Im Allgemeinen soll das Recht auf Achtung der Privatsphäre verhindern, dass jede private Lebensäusserung, die in der Öffentlichkeit stattfindet, wie zum Beispiel ein Abschiedskuss auf der Strasse oder die Beerdigung eines Menschen der Allgemeinheit bekannt wird. Der Einzelne soll sich nicht dauernd beobachtet fühlen, sondern – in gewissen Grenzen – selber bestimmen dürfen, wer welches Wissen über ihn haben darf bzw. welche personenbezogenen Begebenheiten und Ereignisse des konkreten Lebens einer weiteren Öffentlichkeit verborgen bleiben sollen. Da mit Hilfe elektronischer Datenverarbeitung personenbezogene Informationen in beliebigem Umfang gespeichert, verknüpft und reproduziert werden können, lassen sich auch an sich harmlose Informationen, die ohne Weiteres der Öffentlichkeitssphäre zuzurechnen wären, zu eigentlich schützenswerten Persönlichkeitsprofilen verdichten. Gemäss Bundesgericht stellt die Veröffentlichung des individualisierenden, das heisst nicht rein zufälligen Bildes ohne Einwilligung des Betroffenen immer eine Persönlichkeitsverletzung dar, und zwar unabhängig davon, ob bereits die Aufnahme unrechtmässig erfolgte (E 8.3.). Auch gemäss der Rechtsprechung des österreichischen Obersten Gerichtshofs (6Ob256/12h vom 27.02.2013) kann bereits die Herstellung von Bildnissen einer Person in der Öffentlichkeit zugänglichen Bereichen und ohne Verbreitungsabsicht einen unzulässigen Eingriff in das Persönlichkeitsrecht darstellen. Dies gelte insbesondere in Anbetracht der Verbreitungs-, aber auch Manipulationsmöglichkeiten durch die moderne (Digital-) Technik, kann doch der Aufgenommene im Vorhinein nie wissen, wie der Fotografierende die Aufnahme in der Folge verwenden wird (E 6.2.).

12 http://www.llv.li/#/1619/mobile-datenbearbeitung.

lich darin zu sehen, dass praktische Überlegungen den Sicherheitsaspekten vorgezogen wurden. Wir machten darauf aufmerksam, dass entsprechende Qualitätssicherungsmassnahmen sowie eine verschlüsselte Datenübertragung zu implementieren sind. Weiters haben wir die Trennung zwischen Produktivsystem und Testsystem sowie die Einführung eines Mechanismus zur Erkennung von Missbrauchsversuchen thematisiert. Es ist wichtig, dass Internetseiten, über die eine Datenbearbeitung stattfindet, bezüglich Datensicherheit eingehend geprüft werden und dass mit organisatorischen und technischen Massnahmen sichergestellt wird, dass keine Daten an Unberechtigte gelangen.

Betreiber von Internetseiten verwenden häufig Analysewerkzeuge, um das Klickverhalten der Besucher auszuwerten und Statistiken zu erstellen. Dabei wird typischerweise gespeichert, woher die Besucher kommen, welche Bereiche bzw. Unterseiten wie oft aufgerufen und wie lange die Unterseiten angesehen werden. Zwei weit verbreitete Werkzeuge zur **Webanalyse** sind die kostenlosen Lösungen *Piwik*[13] und *Google Analytics*. Auf unserer Internetseite haben wir am Beispiel dieser beiden Lösungen die Bedingungen für eine datenschutzkonforme Anwendung von solchen Auswertungstools beschrieben. Bei der Speicherung und Auswertung von Nutzerdaten gilt insbesondere das Gebot der Datensparsamkeit. Die über ein Webanalyse-Tool gesammelten Nutzerdaten dürfen nicht für andere Zwecke missbraucht werden.[14] Auch muss auf der Internetseite ein leicht auffindbarer Hinweis darüber eingebaut werden, dass Webanalysewerkzeuge verwendet werden und was mit den aufgezeichneten Daten geschieht. Sofern die Auswertung der Nutzungsdaten ausserhalb des eigenen Unternehmens erfolgt,[15] müssen die Besucher der Internetseite darauf hingewiesen werden und eine Möglichkeit erhalten, der Erstellung von Nutzerprofilen zu widersprechen *(Opt-Out)*. Für die aufbereiteten Nutzerdaten und für die Zugriffsprotokolle der Webserver müssen feste Löschfristen vorgesehen und die entsprechenden Dateien, vorzugsweise automatisiert, gelöscht werden. Einige der genannten Punkte scheinen bei der Verwendung von Google Analytics schwer umsetzbar zu sein. Deshalb ist es *fraglich, ob eine datenschutzkonforme Verwendung von Google Analytics überhaupt möglich* ist. Zusätzlich erschwerend ist der Umstand, dass Google per 1. März 2012 die Richtlinien für mehr als 60 einzelne Google-Dienste vereinheitlicht hat und seither eine neue Datenschutzerklärung gilt. Damit kann Google die Nutzerdaten aller Dienste verknüpfen und gesamthaft auswerten, was zu viel aussagekräftigeren Nutzerprofilen führt. Nach einer Voruntersuchung der Artikel-29-Datenschutzgruppe ist dies mit dem europäischen Recht nicht vereinbar und es wird hier das Endergebnis abzuwarten sein. Behörden der Mitgliedstaaten Frankreich, Deutschland, Italien, Spanien, Grossbritannien und Niederlande entschieden, gegen die Geschäftspraktiken von Google vorzugehen. Spanien hat dem Internet-Konzern wegen Verstosses gegen das Datenschutzgesetz bereits eine Geldstrafe auferlegt. Im Unterschied zu Google Analytics kann Piwik datenschutzfreundlich betrieben und so konfiguriert werden, dass keine Daten an externe Datenbearbeiter weitergegeben werden.[16]

Liechtensteiner Bürger können weltweit bei Schweizer Auslandvertretungen, die konsularische Dienstleistungen anbieten, Reisepässe beantragen. Diese Möglichkeit wird jährlich von ca. 50 bis 150 Auslandliechtensteinern genutzt. Seit dem 1. Oktober 2011 werden neben den bereits seit 2006 erfassten Informationen im **biometrischen Reisepass**[17] zusätzlich auch Fingerabdrücke auf dem Chip gespeichert.[18] Wir wurden um Unterstützung bei der Erstellung eines *Bearbeitungsreglements* gebeten, wobei insbesondere die Datenbearbeitungs- und Kontrollverfahren im Zuge des elektronischen Datenaustauschs nach Liechtenstein im Vordergrund standen. An den EDA-Standorten[19] können biometrische Daten nur erfasst, jedoch nicht bearbeitet werden. Die Daten werden dann per E-Mail dem Ausländer- und Passamt (APA) zugestellt, wobei durch geeignete Massnahmen wie digitale Signatur und Verschlüsselung die Integrität und Vertraulichkeit gewahrt bleibt.[20]

13 http://www.piwik.org.
14 Siehe auch unter 5.1, Zweckbindung.
15 Dies ist z. B. bei Google Analytics der Fall. Deshalb liegt hier eine Datenbearbeitung im Auftrag vor, was unter die Bestimmungen von Art. 19 DSG fällt. Siehe dazu auch unter http://www.llv.li/#/11479/datenbearbeitung-im-auftrag-outsourcing.
16 http://www.llv.li/#/188/auswertungstools-von-internetseiten-anhand-der-beispiele-piwik-und-google-analytics.
17 Siehe Tätigkeitsbericht 2006, 4.4.
18 http://www.llv.li/#/11350/daten-im-reisepass.
19 Eidgenössisches Departement für auswärtige Angelegenheiten (EDA).
20 Siehe unter http://www.eda.admin.ch/eda/de/home/reps/eur/vesp/rkcmad/tralis.html#ContentPar_0014 und http://www.llv.li/#/12662/antragsstellung-im-ausland.

1.3. Telekommunikation

Nach *Kontrollen von Telekommunikationsprovidern*[21] hatten sich Fragen ergeben, inwieweit eine **Datenbearbeitung durch die Provider und durch das Amt für Kommunikation (AK)** zu statistischen Zwecken zulässig ist. Insbesondere ging es um die Erstellung der Marktanalyse.[22] Aufgrund der engen gesetzlichen Vorgaben zur Zweckbindung und insbesondere zur Einhaltung der unterschiedlichen Löschfristen ergab sich aus Sicht der Provider ein vermeintlicher Widerspruch zu den gesetzlichen Informationspflichten gegenüber dem AK. Das AK veröffentlicht nun auf seiner Internetseite Informationen, wie die Datenflüsse von den Providern an das AK mit den Datenschutzbestimmungen in Einklang gebracht werden können.[23]

Wir bekamen Anfragen betreffend die Nutzung von **WLANs**.[24] Die Vorteile eines drahtlosen Netzwerks liegen auf der Hand – die Nachteile allerdings auch. Ein Funknetz lässt sich nicht durch Hausmauern begrenzen. Ist es also nicht (genügend) geschützt, können Dritte in Reichweite des Netzes unerkannt auf Kosten des WLAN-Betreibers mitsurfen und eventuell illegale Inhalte herunterladen. Je nach Inhalt verstösst der Trittbrettfahrer unter Umständen gegen das Urheberrechtsgesetz oder das Strafgesetzbuch. Zudem können Drittpersonen den Datentransfer abhören oder die beteiligten Rechner manipulieren, was eine Verletzung der Privatsphäre und damit des Datenschutzgesetzes darstellt. In einem Fall ging es konkret darum, dass sich die Kinder der anfragenden Person in ein ungeschütztes WLAN aus der Nachbarschaft eingeloggt und so ungehindert Zugang zu allen Internetseiten hatten. Damit konnten sie jegliche Einschränkungen und Jugendschutzprogramme umgehen, die die Erziehungsberechtigten zu Hause installiert hatten. Um dies zu verhindern, sollte jeder sein *WLAN auf dem höchstmöglichen Niveau verschlüsseln*.[25]

21 Siehe unter 4.
22 Vgl. Art. 21 und 44 KomG.
23 http://www.llv.li/#/11710/datenerhebung.
24 WLAN steht für Wireless Local Area Network, ein drahtloses lokales Netzwerk, dessen angeschlossene Geräte (Rechner, Drucker etc.) via Funk untereinander und oft auch mit dem Internet kommunizieren.
25 Erziehungsberechtigte stehen in der Verantwortung, die Probleme beim Umgang mit fremden Netzwerken mit den Kindern zu diskutieren, so dass diese ein entsprechendes Bewusstsein entwickeln können.

1.4. Gesundheit und Soziales

In Gesprächen mit dem Krankenkassenverband, dem Amt für Gesundheit (AG) und einer Vertretung der Ärzte setzten wir uns für eine **Stärkung der Stellung des Vertrauensarztes** ein. Dies hatten wir schon vor einigen Jahren vorgeschlagen. Der Vertrauensarzt nimmt im System der obligatorischen Krankenversicherung aus Sicht des Datenschutzes eine zentrale Stellung ein. Das Krankenversicherungsgesetz (KVG) weist etliche Parallelen zu demjenigen der Schweiz auf. Zudem ist es in der Praxis so, dass die meisten Vertrauensärzte in der Schweiz tätig sind. Deshalb, und weil die Schweiz eine bessere gesetzliche Stellung des Vertrauensarztes vorsieht, haben wir vorgeschlagen, dass die schweizerischen Bestimmungen in Liechtenstein übernommen werden.

Das Gesetz über die Invalidenversicherung (IVG) verpflichtet Leistungsempfänger zu umfassenden Mitwirkungs- und Auskunftspflichten. Insbesondere müssen IV-Berechtigte alle Personen und Stellen, die über Informationen verfügen, welche für die Abklärung von Leistungsansprüchen notwendig sind, zur **Auskunftserteilung gegenüber der IV** ermächtigen.[26] Aufgrund eines Entscheids des Schweizerischen Bundesgerichts zu einer unserer Meinung nach inhaltlich vergleichbaren Regelung des Sozialhilfegesetzes des Kantons Bern[27] haben wir die Verfassungsmässigkeit dieser weitreichenden Pflicht zur Vollmachterteilung geprüft. Das Bundesgericht hat als Voraussetzung, dass eine Vollmachterteilung rechtmässig ist, ein Stufensystem entwickelt. Gemäss diesem sind die erforderlichen Informationen in einer ersten Stufe bei der betroffenen Person selbst zu erheben. Ist dies nicht möglich, ist in einem zweiten Schritt die Datenerhebung auf ein Gesetz zu stützen. Erst in einem dritten und letzten Schritt ist auf die Pflicht zur Vollmachterteilung zurückzugreifen. Im Gegensatz zur Rechtsvorschrift des Kantons Bern enthält die liechtensteinische Bestimmung zur Vollmachterteilung[28] jedoch kein vergleichbares Stu-

26 Art. 35 Abs. 3 IVG lautet: „Personen, die Leistungen (Eingliederungsmassnahmen oder Renten) beanspruchen, haben alle Personen und Stellen, insbesondere Arbeitgeber, Ärzte, Versicherungen sowie Amtsstellen im Einzelfall zu ermächtigen, die Auskünfte zu erteilen, die für die Abklärung von Leistungsansprüchen erforderlich sind. Diese Personen und Stellen sind gegenüber der Anstalt zur Auskunft verpflichtet."
27 BGE I 138 331.
28 Art. 35 Abs. 3 IVG.

fensystem. In Liechtenstein kann sich die Behörde vielmehr von vornherein auf eine Vollmacht berufen. Dies wäre bei konsequenter Auslegung der Entscheidung des Bundesgerichts jedoch rechtswidrig. Wir haben daher gegenüber der Regierung unsere Zweifel an der Rechtmässigkeit dieser Bestimmung vorgebracht. Die Regierung kam zu einem anderen Ergebnis und erachtet die Gesetzesbestimmung aus verschiedenen Gründen als rechtmässig. Dennoch zu begrüssen und hervorzuheben ist die in diesem Zusammenhang durch die IV gemachte Zusicherung, dass die genannte Vollmacht mit Zurückhaltung genutzt werde.

Wir wurden darauf aufmerksam gemacht, dass auf **Rechnungen**, welche an das AG oder an die Landespolizei (LP) gestellt werden und von diesen an die Landeskasse (LK) zur Zahlung weitergeleitet werden, auch **Gesundheitsdaten** aufscheinen können. Dies war vor allem bei Rechnungen von Spitälern an das AG oder bei Rechnungen des Landesspitals an die LP (Alkoholkontrollen) der Fall. Natürlich muss die Rechnungsstellung korrekt erfolgen und einer folgenden internen und externen Rechnungskontrolle standhalten. Dazu sind jedoch Gesundheitsangaben nicht nötig. Bei Rechnungen, die vom AG an die LK weitergegeben werden, wurde das Problem so gelöst, dass generell keine Personendaten mehr aufscheinen. Die LP hingegen schwärzt Personendaten auf Rechnungen, die sie an die LK weiterleitet.

Ein Arzt wurde verdächtigt, Methadon ohne Bewilligung an einen Patienten abgegeben zu haben. Um diesen Verdacht zu bestätigen, forderte das AG bei einer Krankenkasse, einem Kantonsarzt und einer Apotheke **Patientendaten** ein. Wir wurden auf dieses Vorgehen aufmerksam gemacht. Eine Prüfung der rechtlichen Grundlagen führte zum Ergebnis, dass diese für das beschriebene Vorgehen nicht ausreichen. Die Möglichkeit des AG, die benötigten Informationen direkt beim betroffenen Arzt zu beschaffen, ist vorzuziehen. Daraufhin wurde im AG eine Weisung erlassen, wonach zukünftig Informationen, die im Zusammenhang mit der Kontrolle der Einhaltung des Betäubungsmittelgesetzes stehen, grundsätzlich *direkt bei den betroffenen Ärzten* eingeholt werden müssen.

Wir erarbeiteten zusammen mit dem AG Mustervorlagen für **Vollmachten**, die im **Krankenversicherungsbereich** eingesetzt werden. Ziel ist es, eine Anpassung an geltende rechtliche Vorgaben und eine gewisse Einheitlichkeit in der Verwendung zu erreichen. Zwei Varianten an Textbausteinen wurden erstellt. Beide sollten im Falle einer Datenerhebung bei Dritten dem Betroffenen vorgelegt werden. Die erste Variante stellt eine Pauschaleinwilligung dar. Bei der zweiten Variante, einer Einzeleinwilligung, kann der Betroffene verlangen, dass die Versicherung in jedem Einzelfall darüber informiert, von welchen Personen oder Einrichtungen und zu welchem Zweck eine Auskunft eingeholt wird.

1.5. Polizei, Sicherheit und Justiz

Wir waren bei der ersten **Sicherheitskonferenz** eingeladen, welche die Regierung zusammen mit schweizerischen Behörden organisiert hatte. Dabei wurden verschiedene Aspekte in Bezug auf Sicherheitsbedrohungen thematisiert. Aus unserer Sicht sind vor allem die Bedrohungen aus dem *Cyberraum* zu nennen. In der heutigen Informationsgesellschaft hat sich auch die Kriminalität zum Teil ins Internet verlagert. Identitätsdiebstahl und Wirtschaftsspionage stehen dafür, dass wichtige Informationen aus der Wirtschaft gestohlen werden. Dabei spielt der Cyberraum eine wichtige Rolle. Man liest immer wieder, dass staatliche Internetseiten oder Internetseiten von Unternehmen angegriffen werden. Dagegen gilt es sich zu schützen. Natürlich steht hier die Netzwerksicherheit im Vordergrund. Es geht aber auch um den Datenschutz: nämlich um den Schutz unternehmensinterner Daten.[29] Und um den Schutz der Kunden und Angestellten. Der *Sicherheitsbericht der Regierung* vom November 2012 enthält diesbezüglich kaum Informationen. Es wird aber auch festgehalten, dass der Bericht nicht vollständig ist; dementsprechend sollte er unseres Erachtens ausgebaut werden. Es wird wichtig sein, in Zusammenarbeit mit der Wirtschaft einen ganzheitlichen Ansatz in diesem Thema zu wählen sowie Unternehmen und Behörden in Liechtenstein zu sensibilisieren. Bedrohungen aus dem Cyberraum machen nicht an unserer Landesgrenze Halt.

29 In Liechtenstein fallen ja auch juristische Personen unter den Schutz des Datenschutzgesetzes.

1.6. Wirtschaft und Finanzen

Wir haben unsere **Checkliste für Benutzungsreglemente betreffend mobile Geräte** überarbeitet und dem aktuellen Stand der Technik angepasst.[30] Beispielsweise wurden Aspekte von *Bring Your Own Device (BYOD)* mit aufgenommen. Die Checkliste erlaubt es, sowohl Nutzungs- als auch Überwachungsreglemente auf inhaltliche Vollständigkeit zu überprüfen und richtet sich speziell an IT-Verantwortliche, die Reglemente oder Dienstvorschriften erstellen. Konkret konnten wir Unternehmen bei der Erstellung notwendiger Nutzungs- und Überwachungsreglemente unterstützen und dabei auf verschiedene Berührungspunkte mit dem Datenschutz, wie beispielsweise die Klassifizierung von Dokumenten, die Verwendung von Poolgeräten, Social Media im Unternehmen usw., hinweisen.[31]

1.7. Arbeitsbereich

Eine Anfrage beschäftigte sich mit der Zulässigkeit einer **doppelten Aktenführung von Personaldossiers**. Was zu einer Personalakte gehört, bestimmt sich nicht nach dem äusseren Erscheinungsbild, sondern nach dem Zweck.[32] Es ist grundsätzlich zulässig, Personalakten an mehreren Stellen parallel zu führen (z. B. beim Vorgesetzten und bei der Personalabteilung). Nicht zulässig sind dagegen die sogenannten „grauen Dossiers", also Akten, deren Vorhandensein und Inhalt den Mitarbeitern verheimlicht wird. Über den Inhalt einer parallelen Aktenführung sollte jeweils abhängig von den Zuständigkeiten entschieden werden. Um den Anforderungen des Datenschutzes gerecht zu werden, sollten die Personalakten regelmässig auf ihre Richtigkeit und Vollständigkeit überprüft und die nicht mehr für die Durchführung des Arbeitsvertrags erforderlichen Unterlagen entfernt werden. Auch ist darauf zu achten, dass – gerade bei paralleler Aktenführung – keine Widersprüchlichkeiten auftreten. Von absoluter Wichtigkeit ist ausserdem, dass der betroffene Arbeitnehmer Kenntnis von der doppelten Führung der Personalakten hat. Der Arbeitgeber hat die Personalakten deshalb so zu führen, dass den Arbeitnehmern grundsätzlich über alle ihre Daten *Auskunft* erteilt werden kann, unabhängig davon, an welchen Orten die Personaldossiers geführt werden.

Die Frage, ob die von einem **Bewerber** vorgelegten Unterlagen und im Lebenslauf gemachten Angaben tatsächlich zutreffen, kann mit Hilfe des Internets und der internationalen Vernetzung immer leichter überprüft werden. Es hat sich in den letzten Jahren sogar ein Markt von Dienstanbietern entwickelt, die sich darauf spezialisiert haben, im Auftrag von künftigen Arbeitgebern die Angaben von Bewerbern auf ihre Richtigkeit und Vollständigkeit hin zu verifizieren. Hierbei werden beispielsweise die von den Bewerbern angegebenen Referenzen überprüft, die früheren Arbeitgeber kontaktiert oder man lässt sich von Universitäten den Abschluss bestätigen. Dieses sogenannte *Candidate Screening* ist nur mit dem ausdrücklichen Einverständnis der betroffenen Bewerber zulässig, das diese auch jederzeit ohne Drohung von Nachteilen widerrufen können müssen. Eine direkte Verknüpfung mit dem Vertragsabschluss wäre unrechtmässig, da die Einverständniserklärung freiwillig erteilt werden muss. Im Gegensatz zum Candidate Screening wird beim *allgemeinen Screening* versucht, über Suchmaschinen oder soziale Netzwerke auf dem Internet einen ersten Eindruck des Bewerbers zu erhalten. Ein solches Vorgehen stellt ein grosses Risiko dar, dass die Persönlichkeit eines Arbeitnehmers verletzt wird, da der Arbeitgeber sehr wahrscheinlich auch dazu verleitet wird, Daten des Bewerbers zu bearbeiten, welche in keinem Zusammenhang mit dem zukünftigen Arbeitsverhältnis stehen. Denn grundsätzlich darf ein Arbeitgeber nur diejenigen Daten bearbeiten, die entweder für die Durchführung des Arbeitsvertrages oder für die Eignung des Bewerbers erforderlich sind.

Mit diesen und vielen anderen Fragen in Zusammenhang mit dem Persönlichkeitsschutz am Arbeitsplatz setzt sich unsere neue **Richtlinie für die Bearbeitung von Personendaten im Arbeitsbereich** auseinander, welche wir nach einer langen Vorbereitung abschliessen und veröffentlichen konnten. Sie

30 Siehe Tätigkeitsbericht 2011, 5.7.

31 Die Checkliste für Benutzungsreglemente betreffend mobile Geräte findet sich unter http://www.llv.li/files/dss/pdf-llv-dss-checkliste_mobile_geraete.pdf.

32 Der Begriff der Personalakte umfasst jene Personendaten, die vom Arbeitgeber im Hinblick auf sein Verhältnis zum Arbeitnehmer mit Bezug auf Entstehung, Abwicklung und Beendigung des Arbeitsverhältnisses bearbeitet werden oder über eine strukturierte Suche abrufbar sind. Dabei ist es nicht von Bedeutung, ob die Personendaten in einem einheitlichen Dossier zusammengefasst oder an verschiedenen Stellen aufbewahrt werden. In ihrer Gesamtheit werden also alle vom Arbeitgeber über einen Arbeitnehmer bearbeiteten Daten als Personalakte angesehen.

ergänzt unsere *Richtlinie über Internet- und E-Mail-Überwachung am Arbeitsplatz*.[33] Die neue Richtlinie stellt die Rechtslage dar und ermöglicht so eine erste Übersicht über die wesentlichen Datenschutzaspekte im Arbeitsleben. Viele der darin abgehandelten Beispiele sind aus *Fällen aus unserer Beratungspraxis* entstanden und erstrecken sich von der Bewerbung über das bestehende Arbeitsverhältnis bis hin zur Beendigung des Arbeitsvertrages und die Aufbewahrungspflichten darüber hinaus. Der Tenor besteht darin, dass der Arbeitgeber nur die für die Eignung und für die Durchführung des Arbeitsvertrages notwendigen Personendaten bearbeiten darf. Und: hiervon darf zu Ungunsten des Arbeitnehmers – selbst mit dessen Einverständnis – nicht abgewichen werden. Diesen starken Schutz übernahm der Gesetzgeber aus der Schweiz, weshalb wir uns in der Richtlinie stark auf Rechtsprechung und Literatur aus der Schweiz abgestützt haben. Neben diesen rechtlichen Aspekten wird auch auf moderne Entwicklungen wie Cloud Computing, aber auch BYOD oder soziale Netzwerke eingegangen. Die Richtlinie soll einen Beitrag zu einem konstruktiven Verhältnis zwischen Arbeitgeber und Arbeitnehmer leisten und Klarheit in einem wichtigen Gebiet schaffen. Datenschutz ist auch Schutz von Vertrauen.[34]

1.8. Datenbekanntgabe im Inland

Im Rahmen einer **Kleinen Anfrage** im Landtag zu **Mietpreisen von Verwaltungsgebäuden** wurden wir angefragt, ob die Bekanntgabe der Mietpreise datenschutzrechtlich erlaubt ist. Dies konnten wir bejahen: Es geht um die *Transparenz* bei der Verwendung öffentlicher Gelder, gerade in der aktuell angespannten Haushaltslage. Hier ist das öffentliche Interesse an staatlichen Ausgaben höher zu bewerten als das Interesse eines einzelnen Vermieters. Ausserdem sind gewisse Zahlen bereits öffentlich zugänglich.[35]

Nicht das erste Mal beschäftigte uns die **Medienberichterstattung** (zu Gerichtsprozessen). Das Land ist klein, Gerichtsverfahren öffentlich. Dennoch muss die Privatsphäre von Gerichtsparteien geachtet werden. Unseres Erachtens sollte sich die Berichterstattung auf die Sache konzentrieren, die Person sollte in den Hintergrund treten (bei einer Person des öffentlichen Lebens mag die Situation anders sein). Im betreffenden Fall wurde die angeklagte Person mit einigen *unnötigen Details* in der Zeitung umschrieben, was sie sehr leicht identifizierbar machte. Im Medienbericht war ersichtlich, dass es sich um einen bemitleidenswerten Fall handelte. Die leichte Identifizierbarkeit der angeklagten Person in der Zeitung trug leider eher zu einer Verschlechterung ihrer Situation bei. Dies hätte durch eine entsprechende Achtsamkeit in der Berichterstattung vermieden werden können. Wir haben das entsprechende Medienunternehmen darauf aufmerksam gemacht.

Im Rahmen einer Anfrage zur Datenbearbeitung im Auftrag von Gemeinden haben wir eine **Abgrenzung** zwischen **Datenbekanntgabe** und **Datenbearbeitung im Auftrag** gezogen, was auch in den entsprechenden Richtlinien Niederschlag gefunden hat. Grundsätzlich impliziert eine Datenbearbeitung im Auftrag auch eine Datenbekanntgabe. Es ist dennoch zwischen beiden Arten zu unterscheiden. Bei der Datenbearbeitung im Auftrag werden die Daten durch Externe bearbeitet, jedoch bleibt die *Datenhoheit* beim Auftraggeber. Der Externe darf Daten nur gemäss Auftrag bearbeiten. Bei der Datenbekanntgabe ist dies anders: Der Bekanntgeber verliert die Hoheit über die bekanntgegebenen Daten.

33 http://www.llv.li/files/dss/richtlinien_ueber_internet-_und_e-mail-ueberwachung_am_arbeitsplatz.
34 http://new.llv.li/#/1157/bearbeitung-von-personendaten-im-arbeitsbereich.
35 Im Bericht und Antrag (BuA) Nr. 121/2012 auf S. 93 sind die Hauptpositionen der Mieten im Verwaltungsbereich nach Gebäuden einzeln aufgeschlüsselt dargestellt.

2. Öffentlichkeitsarbeit
2.1. Allgemeines

Der **NSA-Abhörskandal** war auch ein Thema für uns, vor allem in der *Artikel-29-Datenschutzgruppe*.[36] Wir wurden von der Presse um unsere Meinung gebeten und stellten dabei fest, dass in der Öffentlichkeit ein Gefühl der Verunsicherung und Ohnmacht herrscht. Tätigkeiten von Geheimdiensten sind grundsätzlich sehr schwer zu überwachen; noch schwieriger wird es, wenn es sich um den Geheimdienst der USA handelt. Kritisch sehen wir die *Tendenz, immer mehr Daten sammeln zu wollen.* Hierbei sollte unseres Erachtens vermehrt der Grundsatz *Qualität statt Quantität* gelten. Offenbar hätte schon der Fall des sogenannten „Unterhosenbombers" verhindert werden können, wenn die entsprechenden US-Behörden die *vorhandenen* Informationen ausgetauscht hätten. In diesem Sinne ist es wie so oft eine Frage des goldenen Mittelweges zwischen Freiheit und Sicherheit, was auch eine Demokratie auszeichnet. Auf die Frage, was Liechtenstein in diesem Fall tun kann, antworteten wir, dass dies nicht einfach so hingenommen und auf die Einhaltung des Rechts bestanden werden soll. Der einzelne Nutzer sollte die betroffenen Dienste von US-Unternehmen (wie Google, Facebook, Apple, Microsoft oder Amazon) weniger nutzen. Offenbar gab es für diese Dienste tatsächlich spürbare wirtschaftliche Folgen. Liechtenstein könnte speziell Massnahmen zur *Förderung des Infrastrukturbereichs Informations- und Kommunikationstechnologie* schaffen, wie dies der Infrastrukturreport 2012 der Regierung auch fordert.[37]

Zu folgenden Themen veröffentlichten wir Stellungnahmen in der **Presse**:

Soziale Medien erfreuen sich grosser Beliebtheit. Hiesige Unternehmen haben erkannt, dass bei Facebook über 12 000 Nutzer aus Liechtenstein registriert sind. Dementsprechend wird versucht, hieraus wirtschaftlichen Nutzen zu generieren. Eine Idee, die wir in einem Zeitungsartikel aufzeigten, besteht darin, ein **liechtensteinisches soziales Netzwerk** zu schaffen (das allenfalls einem definierten Zweck gewidmet würde). Natürlich wäre der Aufbau eines solchen Netzwerkes mit Aufwand verbunden. Die Zahlen zeigen aber, dass der Liechtensteiner gerne in sozialen Netzwerken präsent ist. Sogar ein Teil des Wahlkampfes fand dort statt. Das Potenzial scheint also da zu sein. Die Wege sind kurz. Solch ein Vorhaben würde sich auch rasch herumsprechen und Mitglieder könnten rasch gewonnen werden. Die Idee eines sozialen Netzwerks, das die Interessen der Nutzer ernst nimmt, sich klar zum bestehenden Gesetzesrahmen bekennt und zudem noch eine Einnahmequelle im Land schafft, sollte gerade in Zeiten, in denen der Ruf nach neuen Geschäftsideen immer lauter wird, verfolgt werden. Schliesslich könnte dies auch den *Datenstandort Liechtenstein* berücksichtigen, für den wir schon länger eintreten.[38]

Wir schrieben eine kleine **Anleitung** zum Thema **Soziale Medien und Datenschutz**. Insbesondere Facebook wird immer wieder von Nutzern und Datenschutzbehörden kritisiert. Dabei liegt es oft am Nutzer, frühzeitig darauf zu achten, was er veröffentlicht, und zu bedenken, ob auch Dritte davon betroffen sein können und dies gar nicht wollen (z. B. bei Fotos). Auch die Prüfung der eigenen Daten auf dem Internet gehört dazu. Das Internet vergisst nichts, daran sollte immer gedacht werden. Einem kurzfristigen Nutzen (Spass?) kann ein längerfristiger Nachteil entgegenstehen.[39]

Mit einem Presse-Beitrag zum Thema **„Der Schutz der Privatsphäre hat seinen Preis"** wollten wir zum Nachdenken anregen. Viele Menschen sind sich noch immer nicht bewusst, wie viele und welche Daten sie regelmässig im Internet preisgeben. Ungenügende Sensibilisierung und fehlende Transparenz sind häufige Gründe für eine ungewollte oder unüberlegte Bekanntgabe persönlicher Daten. Oft bewerten Nutzer aber einfach auch den Komfort und praktische Überlegungen höher als den Schutz ihrer eigenen Personendaten. Aktiver Datenschutz erfordert manchmal etwas Zeit, lohnt sich aber durchaus. So führt beispielsweise die Verwendung von www.ixquick.com an Stelle von Google als Meta-Suchmaschine oder www.piwik.org als Webanalyse-Tool[40] zu deutlich weniger virtuellen Spuren im Internet.

36 Siehe auch unter 5.1.
37 http://www1.regierung.li/index.php?id=98.
38 http://www.llv.li/files/dss/pdf-llv-dss-soziales-netzwerk-au-fl.pdf.
39 http://www.llv.li/files/dss/pdf-llv-dss-pece-2013-05-social-media.pdf.
40 Siehe auch 1.2 unter Webanalyse.

Beide Alternativen sind nach den Kriterien des europäischen *Datenschutz-Gütesiegels EuroPriSe* zertifiziert.[41]

Zum Thema **„40 Jahre Mobiltelefonie"** versuchten wir einen Blick in die Zukunft zu werfen. Nicht mit Hilfe der Kristallkugel, sondern durch aufmerksame Beobachtung von neuen Trends, wie z. B. *Google Glass*, *Bring Your Own Device (BYOD)* oder allgemein der Manipulation von Menschen durch Unternehmen. Besonders problematisch scheint das systematische Sammeln, Analysieren und Aufbereiten von Daten durch Unternehmen, um damit (potenziellen) Kunden personalisierte Angebote zu unterbreiten. In den Worten von Eric Schmidt, dem ehemaligen CEO von Google: „Ich glaube, dass die meisten Menschen eigentlich nicht wollen, dass Google ihnen ihre Fragen beantwortet. Sie wollen, dass Google ihnen sagt, was sie als nächstes tun sollen." Das hört sich zwar praktisch an, ist aber gleichzeitig äusserst beunruhigend, denn durch diese Filterfunktion droht der Verlust der eigenen Entscheidungsgewalt an eine Software, welche dem Benutzer nur noch die „am besten geeigneten" Produkte und Dienstleistungen vorschlägt. Über weitere Alternativen wird man gar nicht mehr informiert.[42]

2.2. Veranstaltungen

Nach wie vor ist für uns die Sensibilisierung der Öffentlichkeit für den Schutz der Privatsphäre eine zentrale Aufgabe. Dies auch oder gerade weil die im letzten Jahr durchgeführte repräsentative Umfrage zum Datenschutz in Liechtenstein gezeigt hatte, dass die Befragten nur wenig darüber wissen.[43]

Anlässlich des **7. Europäischen Datenschutztages** am 28. Januar haben wir wieder eine Veranstaltung, gemeinsam mit der Universität Liechtenstein, durchgeführt. Der Vortragsabend fand unter dem Motto **„Habe ich wirklich nichts zu verbergen? – Vom Preis der Privatsphäre im Zeitalter des Internets"** statt. Während an den letzten Veranstaltungen die Technik im Fokus stand (wie Suchmaschinen, soziale Netzwerke oder jüngst das sogenannte Online Targeting), wurde dieses Mal ein allgemeiner Ansatz gewählt. Das Schein-Argument „Ich habe nichts zu verbergen" sollte entlarvt werden. Denn jeder hat seine kleinen Geheimnisse. Die Frage ist meist nur, vor wem man etwas zu verbergen hat. Der IT Crowd Club Liechtenstein führte wieder eine interaktive Umfrage zum Thema durch.[44] Der Hauptvortrag mit dem Titel „Das Geheimnis, die Sünde und die Freiheit" ging auf die Frage im Veranstaltungsmotto ein. Ein Fazit bestand darin, dass eine Gesellschaft, in der man wirklich nichts zu verbergen hat, eine Gesellschaft ohne wirkliche Freunde wäre. Denn Vertraulichkeiten und Geheimnisse sind Gegenstand einer echten Freundschaft. Zudem wäre das Leben auch völlig uninteressant, wenn alles offenliegen würde. Diese Aussagen wurden durch Tatsachen in der Industrie oder beim Staat gestützt. So ist z. B. das Rezept von Coca Cola viel Geld wert. Auch der Staat hat seine Geheimnisse – und das ist gut so.

Zusammen mit dem Verein Sicheres Liechtenstein organisierten wir eine Veranstaltung zum **NSA-Skandal**. Es ging dabei darum, das Thema in Bezug auf das Land zu diskutieren. In der Schweizer Presse wurde ja gemeldet, dass auch Liechtenstein für die NSA interessant sei, worauf die Regierung die USA um detaillierte Auskunft über Art und Umfang allfälliger Abhörmassnahmen durch die NSA in Liechtenstein ersucht hatte. Bei dieser Podiumsdiskussion wurde erwähnt, dass wohl – wenn überhaupt – eher liechtensteinische Firmen für die USA interessant seien; die Landesverwaltung oder die Regierung eher weniger. Es sei wichtig, dass sich die Unter-

41 http://www.llv.li/files/dss/pdf-llv-dss-pece-2013-03-datenschutz.pdf.
42 http://www.llv.li/files/dss/pdf-llv-dss-pece-2013-10-40-jahre-mobiltelefonie.pdf.
43 Siehe Tätigkeitsbericht 2012, 2.1.

44 Auf die Frage, ob man sein Einverständnis abgeben würde, damit die eigene Adresse anhand der Autonummer im Internet abrufbar ist, antworteten 31 % der Befragten mit ja, 64 % verneinten dies. Die Frage, ob es in Ordnung wäre, wenn die eigene Steuererklärung im Internet abrufbar wäre, antworteten 22 % mit ja und 69 % mit nein. Auf die Frage „Wie viel wäre ich bereit, monatlich für Facebook zu bezahlen?" antworteten 43 % dahingehend, dass sie Facebook gar nicht benutzen und 46 % gaben an, Facebook nur benutzen zu wollen, wenn es gratis ist; lediglich 9 % wären bereit, einen bis fünf Franken pro Monat zu bezahlen. In der heutigen Informationsgesellschaft spielt auch die Flut von Informationen und damit auch von allgemeinen Geschäftsbedingungen für den Gebrauch von Internetseiten eine grosse Rolle. Die Frage „Lese ich die Datenschutzbestimmungen, wenn ich mich auf einer Webseite registriere?" bejahten lediglich 17 %. 27 % gaben an, die ersten paar Sätze zu lesen und 53 % verneinten diese Frage. Auf die Frage „Weiss ich noch, wo ich im Internet meine persönlichen Daten angegeben habe?" antworteten 26 % mit ja und 35 % mit nein. Die Umfrage zeigt, dass es vor allem in Bezug auf die Datenschutzerklärungen Handlungsbedarf gibt. Das ist ein international bekanntes Phänomen. Hierzu hatte im Übrigen die Artikel-29-Datenschutzgruppe ein Papier zu sogenannten Layered Information Notices entwickelt.

nehmen selbst schützen. Von unserer Seite wurde erwähnt, dass amerikanische Dienste wie Facebook, Google, Amazon usw. in Folge des Skandals von vielen gemieden wurden und dass man besser europäische Alternativen nutzen sollte. Hier würde sich möglicherweise eine Gelegenheit bieten, *Lösungen in Liechtenstein* zu entwickeln, was auch zum Wirtschaftsziel Datenstandort Liechtenstein passen würde. Wir wiesen das Publikum darauf hin, dass wir in diesem Zusammenhang *Tipps zum Selbstschutz* veröffentlicht haben.[45] Das Thema NSA wurde auch in der Artikel-29-Datenschutzgruppe diskutiert.[46]

Im Jahr 2011 hatten wir erstmals alle **Datenschutzverantwortlichen** zu einer Informationsveranstaltung eingeladen. Daraus wurde ein jährliches Treffen, bei dem wir einerseits die Datenschutzverantwortlichen von *Behörden* und andererseits diejenigen von *Unternehmen* zu einem Gedankenaustausch einluden. Da zudem die Anzahl der Datenschutzverantwortlichen in der jüngsten Vergangenheit zugenommen hatte, entschieden wir uns für eine *Einführungsveranstaltung*. Bei dieser wurden die gesetzlichen Anforderungen an Datenschutzverantwortliche sowie Praxisaspekte beleuchtet. Hintergrund dieser Einführungsveranstaltung war vor allem die ungenügende Praxis zur Anmeldung von Datensammlungen oder Datenschutzverantwortlichen.[47]

Weiters wurden wir zu verschiedenen **Vorträgen** eingeladen. Im Rahmen einer Weiterbildung konnten wir zum Thema „Datenschutz am Arbeitsplatz" referieren. Wir nutzten diese Gelegenheit, um auf unsere neue Richtlinie hinzuweisen.[48] Zudem konnten wir an verschiedenen Veranstaltungen *Jugendliche* im Umgang mit sozialen Medien und dem Internet sensibilisieren. Wir wurden beispielsweise von einer grossen Bank als Vortragende zu einer Sensibilisierungsveranstaltung mit den dortigen Lernenden eingeladen. Auch an einer Präsentation mit dem Titel „Wo sind die Daten?! Wenn Menschen ihr Leben mit Smartphones öffentlich machen" mit anschliessender Podiumsdiskussion, organisiert von der Jugendkommission Triesen, nahmen wir aktiv teil. Zwei Veranstaltungen führten wir im Rahmen des Aus- und Weiterbildungsprogramms der Landesverwaltung durch. Schliesslich sind noch unsere Teilnahme am Wirtschaftsforum sowie zwei Mitarbeiterfortbildungen, organisiert vom Verein für Betreutes Wohnen in Liechtenstein, zu nennen. Die Möglichkeit, bei Veranstaltungen auf die Wichtigkeit des Schutzes der Privatsphäre hinzuweisen, begrüssen wir sehr; denn unsere repräsentative Umfrage im Vorjahr zeigte, dass die Bevölkerung diesbezüglich nur wenig sensibilisiert ist.

2.3. Neuigkeiten auf der Internetseite

Auf unserer **Internetseite** informieren wir regelmässig über aktuelle Themen, die für die Öffentlichkeit relevant sind, und stellen Hilfsmittel wie Richtlinien oder Musterdokumente zur Verfügung. Nachfolgend berichten wir über Themen, die nicht schon in einem anderen Kapitel erwähnt sind.

Aufgrund der Wichtigkeit, die Öffentlichkeit zu sensibilisieren, schufen wir eine neue Rubrik auf unserer Internetseite. Dabei wird gut sichtbar auf **Veranstaltungen** hingewiesen, die wir selbst durchführen oder zu denen wir eingeladen wurden, einen Beitrag zu leisten.

Das DSG regelt bekanntlich eine Querschnittsmaterie. Daten werden praktisch überall in der einen oder anderen Form bearbeitet. Der Anwendungsbereich des Gesetzes ist somit enorm. Das DSG tritt jedoch in seiner Geltung in den Hintergrund, wenn es andere Regelungen gibt, die einen Bereich speziell regeln, was in vielen Fällen des öffentlichen Rechts der Fall ist. Es kommt in solchen Spezialgesetzen immer wieder vor, dass das DSG „im Übrigen" gilt. Diese Aussage ist jedoch nicht einfach zu verstehen. Aus diesen Gründen veröffentlichten wir einen Aufsatz in der Liechtensteinischen Juristen-Zeitung zur Frage des **Verhältnisses des DSG zu Spezialgesetzen**. Als Beispiel diente der Sorgfaltspflichtbereich, der auch in einer Entscheidung des Staatsgerichtshofs (StGH) im Vordergrund gestanden hatte. In diesem Aufsatz analysierten wir den einschlägigen Entscheid des StGH.[49]

45 Siehe 2.3.
46 Siehe 5.1.
47 Siehe Tätigkeitsbericht 2012, 6. Diese ungenügende Praxis wurde auch im Landtag kritisiert, siehe Landtagsprotokoll zur Sitzung vom Mai 2013, Traktandum 11: Tätigkeitsbericht 2012 der Datenschutzstelle.
48 Siehe 1.7.
49 http://www.llv.li/files/dss/pdf-llv-dss-aufsatz-ljz-2013-03.pdf.

Für automatisierte Datensammlungen ist unter bestimmten Voraussetzungen ein **Bearbeitungsreglement** zu erstellen.[50] Ein solches Reglement dokumentiert insbesondere die Datenbearbeitungs- und Kontrollverfahren. Verantwortlich für die Erstellung ist der Inhaber der jeweiligen Datensammlung. Inhaltlich sollte sich das Dokument auf die wesentlichen Aspekte der gemäss DSV vorgeschriebenen Punkte beschränken; die für das Verständnis und die Beurteilung der Abläufe notwendigen Erläuterungen müssen jedenfalls enthalten sein. Organisationseinheiten, die ihre Aufbau- und Ablauforganisation sowie die verwendeten Systeme zur Datenbearbeitung bereits angemessen dokumentiert haben, werden durch die Erstellung des Bearbeitungsreglements kaum grossen zusätzlichen Mehraufwand haben, da für das Reglement benötigte Informationen häufig in anderen Dokumenten bereits vorhanden sind. Zur Unterstützung der Dateninhaber entschieden wir uns für die Veröffentlichung einer entsprechenden **Mustervorlage** mit Beispielen und Erläuterungen.[51]

Die Protokollierung der Bearbeitung von Datensammlungen[52] stellt *eine* Massnahme im Sinne der Datensicherheit dar. Dabei wird geregelt, unter welchen Voraussetzungen verpflichtend Protokolle erstellt werden müssen. Hierzu erarbeiteten wir eine **Empfehlung zur Protokollierung**. Eine Protokollierung ist erst dann Pflicht, „wenn die präventiven Massnahmen den Datenschutz nicht gewährleisten können". Somit ist zuerst zu klären, ob der Zweck der Protokollierung nicht durch andere Massnahmen, die weniger in die Privatsphäre der Betroffenen eingreifen, erreicht werden kann. Denn durch die Protokollierung werden neue Datenbestände geschaffen. Im Vorfeld ist auch stets abzuwägen, ob die Sensitivität der entstehenden Protokolldaten in einem angemessenen Verhältnis zum Schutzbedarf der überwachten Verfahren steht. Eine Protokollierung ersetzt keine Zugriffskontrollen[53] (Berechtigungskonzept), sondern ergänzt diese bei Bedarf. In der Empfehlung kommen wir unter anderem zum Schluss, dass auch unabhängig dieser gesetzlichen Bestimmung eine Protokollierung für die Nachvollziehbarkeit oder zur Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmungen angezeigt sein kann, wenn beispielsweise aufgrund der Ausgestaltung der Datenbearbeitung oder anderer Umstände ein erhöhtes Risiko der Verletzung des Zweckbindungsprinzips besteht.[54]

Datenschutzerklärungen sind für Betreiber von Internetseiten *das* Instrument, um Besucher darüber zu informieren, welche Daten im Zusammenhang mit dem Besuch der Seite bearbeitet werden. Die Datenschutzerklärung muss in jedem Fall auf der Hauptseite, grundsätzlich jedoch über einen direkten Link auf allen Seiten des Internetauftritts zur Verfügung stehen. Dieser Informationspflicht wird jedoch nicht bei allen Internetauftritten nachgekommen. Um Seitenbetreiber bei der Erstellung einer Datenschutzerklärung zu unterstützen, haben wir ein entsprechendes Muster erarbeitet. Unsere **Muster-Datenschutzerklärung** schlägt – dem Mehrebenen-Prinzip gemäss Artikel-29-Datenschutzgruppe folgend[55] – zwei Ebenen vor: den *Datenschutzhinweis* (Kurzfassung der Datenschutzerklärung) und die *vollständige Datenschutzerklärung*. Ergänzt werden diese beiden Musterdokumente mit Formulierungsvorschlägen und Hinweisen für spezifische Fälle, z. B. Newsletter-Anmeldungen. Die Muster-Datenschutzerklärung muss auf jeden Fall vom Betreiber der Internetseite an seine tatsächlich durchgeführten Datenbearbeitungen angepasst und ergänzt werden.[56]

WhatsApp ist eine populäre und für verschiedene Plattformen verfügbare Nachrichten-App (Instant Messaging) für Mobiltelefone. Die Datenbearbeitung von WhatsApp wurde in einer gemeinsamen *Datenschutzkontrolle der Datenschutzbehörden in Kanada und in den Niederlanden* überprüft. Es konnte unter anderem festgestellt werden, dass sämtliche WhatsApp-Versionen – ausgenommen unter iOS ab Version 6.0 – ohne Einwilligung der Nutzer stets das komplette Adressbuch des Mobiltelefons an WhatsApp übermittelt wird. Auch wurden bis zu dieser Version der App sämtliche Textnachrichten im Klartext übertragen, was insbesondere in öffentlichen WLAN-Netzen das Mitlesen von Nachrichten mit einfachen Mitteln zuliess. Ein weiterer Kritikpunkt

50 Vgl. Art. 12 bzw. Art. 21 DSV.
51 http://www.llv.li/#/11440/bearbeitungsreglement.
52 Art. 11 DSV.
53 Art. 10 Abs. 1 Bst. g DSV.
54 http://www.llv.li/files/dss/pdf-llv-dss-protokollierung_art_11_dsv.pdf.
55 Stellungnahme 10/2004 zu einheitlicheren Bestimmungen über Informationspflichten, November 2004, WP 100, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_de.pdf.
56 http://www.llv.li/#/11884/musterdatenschutzerklarung-fur-internetseitenbetreiber.

im Bericht besteht darin, dass WhatsApp die Daten inaktiver Nutzer für ein Jahr speichert, ohne diese Speicherdauer begründen zu können. Im Bericht finden sich auch Empfehlungen im Zusammenhang mit den Statusmeldungen, die von sämtlichen Nutzern gelesen werden können, welche die entsprechende Telefonnummer im Adressbuch gespeichert haben.

In Folge des NSA-Skandals entstand die Forderung, den **Datenschutz auf internationalem Niveau zu verankern**. Dies vor dem Hintergrund, dass es zwar in Europa Regelungen zum Datenschutz gibt, diese jedoch auf internationaler Ebene, also bei den Vereinten Nationen, fehlen. Diese Forderung der Internationalen Datenschutzkonferenz unterstützten wir in einem *Schreiben an die Regierung*.

Aus Anlass des NSA-Abhörskandals haben wir **Tipps für den Selbstdatenschutz** zusammengestellt. Durch die technologische Entwicklung können heute Informationen aus verschiedensten Quellen miteinander verknüpft und so ein umfangreiches Persönlichkeitsprofil über eine Person erstellt werden. Genau diese Verknüpfung von Informationen ist beispielsweise das Geschäftsmodell von Google.[57] Doch jeder Einzelne hat es grösstenteils selbst in der Hand, wie viele Spuren er im – zweifelsohne nützlichen – Internet hinterlässt. Unsere Tipps zeigen auf, wie man das Internet nutzen und trotzdem sparsam mit der Preisgabe von persönlichen Informationen sein kann. Beispiele sind: *Multiple Identity*, also das Verwenden von verschiedenen Browsern, Suchmaschinen und E-Mail-Adressen. Eine einfache und wirkungsvolle Massnahme ist auch, *Suchmaschinen* zu verwenden, welche die eingegebenen Suchbegriffe nicht sammeln und ein Profil daraus erstellen. Ganz generell empfehlen wir, *zurückhaltend und sorgsam* mit den eigenen (und fremden) persönlichen Daten umzugehen. Auf unserer Internetseite stehen auch Hilfsmittel wie z. B. ein Passwortcheck zur Verfügung.[58]

Im Zuge der Migration vom alten **Schengener Informationssystem** zum neuen **SIS II** startete eine schengenweite Informationskampagne. Wir aktualisierten auf unserer Internetseite die Informationen und stellten von der EU-Kommission bereitgestelltes Informationsmaterial zur Verfügung. Auch die Landespolizei schaltete Informationen zum neuen SIS II auf ihrer Internetseite auf. Zudem wurde über eine Pressemitteilung der Regierung, bei der wir mit beteiligt waren, auf die Inbetriebnahme des SIS II aufmerksam gemacht.

3. Mitarbeit bei der Gesetzgebung

Die Mitarbeit bei der Gesetzgebung ist eine weitere unserer Kernaufgaben. Dabei ist unser Hauptanliegen, dass im Gesetzgebungsprozess die Privatsphäre der Bürger beim Erlass neuer Vorschriften beachtet wird. Im Zuge des Vernehmlassungsverfahrens haben wir vier Stellungnahmen zu Gesetzesvorhaben abgegeben. Sie betrafen das *Heilmittelgesetz*, das *Polizeigesetz und das Strafgesetzbuch*, das *Steuerabkommen zwischen Liechtenstein und Österreich* sowie das *Steueramtshilfegesetz*.

Bei der **Abänderung des Gesetzes über die Durchführung der internationalen Amtshilfe in Steuersachen (SteAHG)** sowie die **Abänderung des Gesetzes über die Amtshilfe in Steuersachen mit den Vereinigten Staaten** ging es um die Einführung einer Informationssperre in den Fällen eines Amtshilfeverfahrens, in denen die Benachrichtigung der betroffenen Person den Erfolg des ausländischen Ermittlungsverfahrens vereiteln würde. Anlass hierfür ist eine entsprechende Empfehlung des Global Forums mit dem Ziel, dass das Amtshilfeverfahren nicht unangemessen beeinträchtigt oder übermässig verzögert wird, nachdem in der jetzigen Fassung des SteAHG keine Ausnahmen von der Pflicht zur vorherigen Benachrichtigung der betroffenen Person vorgesehen sind. Wir unterstützen das Vorhaben der Regierung im Rahmen dieser Revision. Unter bestimmten Umständen kann es durchaus angezeigt sein, dass ein Betroffener nicht über staatliche Handlungen informiert wird. Dies ist bereits im geltenden Recht so.[59] Dem Grundrecht auf rechtliches Gehör wird in diesen Ausnahmefällen dennoch Genüge getan, indem sie unter dem richterlichen Vorbehalt stehen und unverzüglich nach Wegfall der Gründe, spätestens nach 2 Jahren, nachzuholen ist. Auch das DSG selbst kennt eine vergleichbare Ausnahme vom Grundsatz der Informationspflicht u. a. in den Fällen, in denen ansonsten eine Strafuntersuchung oder andere Untersuchungen in Frage gestellt wären.[60]

57 Siehe hierzu unter 1.2, Stichwort Webanalyse.
58 http://www.llv.li/#/1299/selbstdatenschutz.

59 Indirektes Auskunftsrecht im Rahmen des Polizeigesetzes und Überwachung der elektronischen Kommunikation.
60 Vgl. Art. 5 Abs. 5 in Verbindung mit Art. 12 Abs. 1 und 2 DSG.

Weiters waren wir unabhängig von öffentlichen Vernehmlassungsverfahren oder im Vorfeld davon bei diversen Gesetzesprojekten intern beteiligt, wie beispielsweise beim DRG (Diagnosis Related Groups) in Zusammenarbeit mit dem Amt für Gesundheit. Wir schätzen es sehr, wenn uns die verantwortlichen Stellen bereits *in einem frühen Stadium* beiziehen und wir so die Möglichkeit haben, bereits von Anfang an die datenschutzrechtlichen Anforderungen mit einzubringen.

4. Kontrollen

Im Tätigkeitsbericht 2010 hatten wir über die Vorbereitung von Kontrollen im Rahmen des Kommunikationsgesetzes (KomG) informiert.[61] Gemäss den im 2010 eingeführten Bestimmungen[62] müssen wir die Einhaltung des Datenschutzes, insbesondere mit Blick auf die Vorratsdatenspeicherung, kontrollieren; dieser Aufgabe kamen wir nach. Die Kontrollen bei drei **Providern** konnten inzwischen abgeschlossen werden. Dabei wurden auch die Ergebnisse des Enforcement-Berichts der Artikel-29-Datenschutzgruppe[63] berücksichtigt.[64] Ergänzend wurde die Umsetzung unseres im Vorfeld ausgearbeiteten *Leitfadens für den Austausch von Personendaten zwischen Telekommunikationsanbietern und Behörden anlässlich von Überwachungsmassnahmen der elektronischen Kommunikation gem. Art. 52 ff. KomG*[65] geprüft. Provider müssen ihre Datenbearbeitungen unabhängig von der technischen und örtlichen Telekommunikationsinfrastruktur nach folgenden Bearbeitungszwecken trennen: 1. Vorratsdatenspeicherung[66], 2. Verrechnung[67] und 3. Erfüllung der Informationspflichten[68]. Nur so ist die Einhaltung des Datenschutzes möglich. Insgesamt kann die Haltung der Provider gegenüber dem Datenschutz als *positiv* bezeichnet werden. Die Provider scheinen sich der Wichtigkeit des Datenschutzes, speziell auch im Zusammenhang mit der Vorratsdatenspeicherung, bewusst zu sein, und sie scheinen bestrebt, Datenschutzmassnahmen in der Praxis umzusetzen und laufend zu verbessern. Nichtsdestotrotz konnten wir in verschiedenen Bereichen Mängel feststellen. Der Fokus der Kontrollen lag auf der rechtmässigen Bearbeitung der Vorratsdaten. Nicht alle Provider hatten Löschprozesse implementiert, um die aufgezeichneten *Vorratsdaten nach sechs Monaten zu löschen*, wie das Gesetz dies verlangt.[69] Wir haben hier konkrete Empfehlungen abgegeben. Insbesondere soll ein automatisierter Prozess für das Löschen der Vorratsdaten gegenüber manuellen Prozessen bevorzugt werden. Diese und ergänzende Empfehlungen[70] wurden von den Providern allesamt angenommen.

Das Amt für Statistik (AS) ist mit dem Anliegen an uns herangetreten, den Datenaustausch mit Institutionen und Personen ausserhalb der Landesverwaltung auf ihre Datenschutzkonformität hin zu überprüfen. Anlässlich der **Kontrolle beim AS** haben wir festgestellt, dass zwar die gesetzlichen Anforderungen an die *Datensicherheit* vonseiten des AS selbst grösstenteils erfüllt werden, dass jedoch beim *Datenaustausch mit verwaltungsexternen Stellen* durchaus Verbesserungsbedarf besteht. Ursache dafür sind vor allem unterschiedliche technische Vorkehrungen und Möglichkeiten und daraus folgend unterschiedliche Sicherheitsniveaus. Da das AS den verwaltungsexternen Datenlieferanten die Erhebung der statistischen Daten nicht unnötigerweise erschweren möchte, wird versucht, in Zusammenarbeit mit dem Amt für Informatik (AI) neue Kommunikationswege zu schaffen. Erklärtes Ziel des AS ist es, den verwaltungsexternen Stellen einen unkomplizierten, aber dennoch datenschutzkonformen Datenaustausch anbieten zu können.

61 Siehe Tätigkeitsbericht 2010, II. 1.3.
62 Vgl. Art. 52b KomG.
63 Bericht 01/2010 über die zweite gemeinsame Durchsetzungsmassnahme: Erfüllung der nach den innerstaatlichen Rechtsvorschriften über die Vorratsspeicherung von Verkehrsdaten aufgrund der Artikel 6 und 9 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der Richtlinie 2006/24/EG bestehenden Pflichten durch die Telekommunikations-Diensteanbieter und die Internet-Diensteanbieter auf nationaler Ebene, angenommen am 13. Juli 2010, WP 172, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_de.pdf.
64 Siehe Tätigkeitsbericht 2010, II. 4.1.
65 Siehe Tätigkeitsbericht 2012, 1.3.
66 Vgl. Art. 49 Abs. 2 Bst. a KomG in Verbindung mit Art. 51 bis 53 KomG.
67 Vgl. Art. 49 Abs. 2 Bst. e KomG.
68 Vgl. Art. 49 Abs. 2 Bst. a KomG in Verbindung mit Art. 44 KomG.
69 Vgl. Art. 52a Abs. 1 S. 2 KomG.
70 Beispielsweise müssen, mit Blick auf eine ordnungsgemässe Trennung der Testsysteme von den Produktivsystemen, auf Notebooks und anderen mobilen Geräten die lokalen Datenträger verschlüsselt werden; bei Fernzugriffen muss eine dem Stand der Technik entsprechende 2-Faktor-Authentifizierung eingeführt werden.

Wir hatten 2012 bei der Freiwilligen Krankenkasse Balzers (FKB) die **Datenflüsse zwischen dem Vertrauensarzt und der Verwaltung** der FKB untersucht.[71] Damals wurde der FKB empfohlen, das durch den vertrauensärztlichen Dienst implementierte System der Hilfspersonen genau zu überprüfen und bestehende mögliche Interessenskonflikte (die auf der Kleinheit des Unternehmens gründeten) aufzulösen. Ausserdem war uns wichtig, dass die FKB auch darauf einwirkt, dass der Vertrauensarzt seine Filterfunktion effektiv ausübt. Bei der **Folgekontrolle** konnte festgestellt werden, dass die FKB alle unsere Empfehlungen umfassend umgesetzt hat. Die Massnahmen, welche die FKB zur Verbesserung und Stärkung des Datenschutzes seit 2012 getroffen hatte, gingen zum Teil über die ausgesprochenen Empfehlungen hinaus. Hierbei ist vor allem die Implementierung des „Reglements Datenschutz und Datensicherheit" hervorzuheben, das die gesetzlichen Vorgaben vorbildhaft umsetzt. Die FKB setzte mit der Umsetzung ein Zeichen dafür, dass sie die Wichtigkeit des Datenschutzes erkannt hat.

5. Internationale Zusammenarbeit

5.1. Artikel-29-Datenschutzgruppe

Ein Schwerpunkt der Arbeit der Datenschutzgruppe bestand im **NSA-Abhörskandal**, da dieser grundlegende Fragen zum Datenschutz aufwarf. Dabei ist zwischen den Überwachungsaktivitäten der NSA und denjenigen ihrer europäischen Partner zu unterscheiden. Bezüglich der NSA-Aktivitäten stand an erster Stelle die *Klärung des Sachverhaltes*, was bei Geheimdienstaktivitäten naturgemäss schwierig ist. Eine weitere Aufgabe war die *Beurteilung der Rechtskonformität*. Aufgrund der Komplexität des Themas konnte diese Arbeit noch nicht abgeschlossen werden.

In zwei Schreiben an das Europäische Parlament äusserte die Gruppe Kritik an verschiedenen Punkten des Vorschlages einer **neuen Geldwäscherei-Richtlinie**.[72] In diesem Vorschlag wird das Schutzniveau gegenüber der bestehenden Richtlinie gesenkt. Eine ähnliche Kritik äussert der Europäische Datenschutzbeauftragte (EDPS), der diese drohende Verschlechterung darauf zurückführt, dass Forderungen der FATF umgesetzt werden sollen, in Europa jedoch der Datenschutz einen anderen Stellenwert hat als in anderen Teilen der Welt. Der EDPS besteht darauf, dass bei einem europäischen Gesetzesvorhaben der *europäische Rahmen* beachtet wird und nicht einfach Forderungen der FATF übernommen werden.[73] Neben weiteren Kritikpunkten äussern sowohl die Datenschutzgruppe als auch der EDPS starke Zweifel daran, dass künftig Steuerdelikte als Vorstrafen für die Geldwäscherei und die Verhinderung des Terrorismus gelten sollen. Hier gehe es um zwei verschiedene Themen, die nicht vermischt werden dürfen. Danach würden die Zweckbindung und die Verhältnismässigkeit durchbrochen.

Die Datenschutzgruppe beschäftigte sich auch mit **Apps**, welche zahlreiche Risiken bei der Wahrung der Privatsphäre bergen. Smartphone-Besitzer haben durchschnittlich 37 Apps auf ihr Gerät geladen. Apps sind Software-Programme, welche meist mit einer zentralen Datenbank beim Anbieter der App verknüpft sind und regelmässig Daten austauschen. Oft fehlt es dabei an der nötigen Transparenz, damit ein Nutzer im Voraus den Umfang der Datenbearbeitung von einzelnen Apps erkennen kann. Datenschutzrisiken ergeben sich bei Smartphones sowohl bei der Installation der App als auch während der Nutzung. Verschiedene Apps greifen auf Daten zu, die auf dem Gerät gespeichert sind, wie beispielsweise Standortdaten, Kontaktdaten, Fotos, Videos, Kreditkartenangaben, Telefonbuchprotokolle, SMS und Instant-Messaging, Surfhistorie, E-Mail und auch biometrische Informationen (Gesichtserkennung und Fingerabdrücke).[74] Dieses Thema wird zusammen mit den spezifischen Bestimmungen des europäischen Datenschutzrechts, welche für App-Entwickler gelten, in einem *Papier zu mobilen Apps* behandelt.[75] Apps, die sich an *Kinder* richten, finden dabei spezielle Beachtung. Zum Thema Datensicherheit im Zusammenhang mit der Entwicklung von Smartphones verweist die Stellungnahme auf ein Papier der European Union Agency for Network and Information Security (ENISA).[76]

71 Siehe Tätigkeitsbericht 2012, 4.

72 Das letzte Schreiben vom 8. November 2013 ist zu finden unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131108_2nd_letter_aml_cft_directive_regulation_en.pdf.

73 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-04_Money_laundering_EN.pdf.

74 Siehe Ausführungen zu WhatsApp unter 2.3.

75 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf.

76 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines.

Um den Grundsatz der **Zweckbindung** bei der Datenbearbeitung ging es in einer weiteren Stellungnahme der Datenschutzgruppe: Daten sollten jeweils nur für einen bestimmten Zweck gesammelt werden. Oft entsteht dabei die Frage, ob dieselben Daten für einen anderen Zweck weiterverwendet werden dürfen. Bei der Klärung dieser Frage ist jeder Fall einzeln zu prüfen. Zentral ist der ursprünglich angegebene Zweck, welcher *möglichst genau umschrieben* werden sollte, damit die betroffenen Personen wissen, was beabsichtigt ist. So wird z. B. beim Ausfüllen von amtlichen Formularen immer ein bestimmter Zweck verfolgt: sei es bei einem Gewerbegesuch, einem IV-Antrag, einer Aufenthaltsgenehmigung usw. Eine Zweckänderung kann erlaubt sein, wenn der ursprüngliche Zweck nicht weit vom neuen (zusätzlichen) Zweck entfernt ist. Dabei ist auch die Erwartungshaltung der betroffenen Person zu berücksichtigen: Je weiter eine Bearbeitung vom ursprünglichen Zweck entfernt ist, desto eher ist diese nicht erlaubt.[77] Zudem ist die Art und Sensibilität der Daten zu berücksichtigen: Je sensibler die Angaben sind, desto eher ist eine Weiterbearbeitung unzulässig.[78] Schliesslich können zusätzliche Schutzmassnahmen wie eine Pseudonymisierung oder eine zusätzliche Einwilligung eine sonst nicht erlaubte Zweckänderung ermöglichen.[79] Die genannte Stellungnahme stützt sich auf die Zweckbindungsbestimmung der allgemeinen Datenschutzrichtlinie, welche in Liechtenstein nicht wörtlich übernommen wurde, sodass Unterschiede bestehen. Auf Druck der ESA wurde die entsprechende Bestimmung geändert und strenger als in der allgemeinen Datenschutzrichtlinie formuliert.[80] Damit können die erwähnten Kriterien in Liechtenstein nur beschränkt zur Anwendung kommen. Die Weiterbearbeitung von Personendaten muss hierzulande in jedem Fall mit dem Zweck vereinbar sein, der bei der Beschaffung angegeben wurde.

Die Anfang 2012 lancierte **Reform des Datenschutzes im EWR** war weiterhin ein beherrschendes Thema der Datenschutzgruppe.[81] Das Reformpaket wurde vom Europäischen Parlament gutgeheissen. Am Schluss fehlte jedoch eine Entscheidung des Europäischen Rates, welche für direkte Verhandlungen zwischen der Kommission, dem Parlament und dem Rat nötig ist. Ziel war ein Abschluss der Arbeit bis im Frühling 2014, wenn das Parlament neu gewählt und die Kommission neu besetzt werden. In Anbetracht dieser Blockade durch den Rat muss davon ausgegangen werden, dass diese wichtige Reform, mit der auch für die Unternehmen Rechtssicherheit geschaffen werden sollte, vorerst verschoben ist.

Die Datenschutzgruppe legt Wert auf eine verbesserte Zusammenarbeit in der Alltagspraxis der Datenschutzbehörden. Deshalb lancierte sie eine interne **Umfrage** zu zwei Bereichen. Der erste Teil betraf die rechtlichen Möglichkeiten der nationalen Datenschutzaufsichtsbehörden bezüglich Tätigwerden, Aufsicht und Durchsetzungsmassnahmen **(Enforcement)**. Beim zweiten Teil ging es um die Zusammenarbeit mit anderen Behörden/Unternehmen auf nationaler Ebene **(national cooperation)**. Gemäss einer ersten Zusammenfassung der Auswertung gehören wir zu drei der insgesamt 30 teilnehmenden Aufsichtsbehörden, die keine rechtsverbindlichen Entscheidungen erlassen oder Sanktionen aussprechen können.[82] Unsere Durchsetzungsmöglichkeiten sind im europäischen Vergleich tatsächlich sehr begrenzt: wir können einzig Bewilligungen von Videoüberwachungsanlagen erteilen.

77 Dementsprechend wird ein Kassaangestellter informiert, dass die Videoüberwachung zur Überwachung der Zahlung stattfindet. Er muss jedoch nicht damit rechnen, dass auch sein Verhalten am Arbeitsplatz überwacht wird und wird dementsprechend überrascht reagieren.

78 Bsp.: In einem Anstellungsverfahren von zwei verschiedenen Organisationen wird jeweils ein Medizintest durchgeführt. Ein Bewerber erhält eine Stelle aufgrund eines negativen Medizintests nicht. Derselbe Bewerber bewirbt sich zwei Jahre später bei einer anderen Einheit und wird ebenfalls nicht angestellt, da der Medizintest vor zwei Jahren negativ ausgefallen war. Hier geht es um Gesundheitsdaten. Dazu kommt, dass der Bewerber nicht damit rechnen muss, dass die zwei Jahre alten Daten erneut und von jemand anderem in Betracht gezogen werden.

79 So benutzt ein Verkehrsamt Lokalisierungsdaten von Verkehrsteilnehmern, um den Verkehr in den Griff zu bekommen. Dies wäre grundsätzlich durch die Kommunikationsgesetzgebung nicht erlaubt. Die Daten werden jedoch anonymisiert, sodass keine Rückschlüsse auf die betroffenen Personen möglich sind. Ja, durch die Anonymisierung ist sogar das Datenschutzgesetz gar nicht anwendbar. Zusätzlich werden die Personen möglicherweise über diese Massnahme informiert, sodass hier eine Bearbeitung durch das Verkehrsamt zulässig ist.

80 Siehe LGBl. 2009 Nr. 46.

81 Siehe Tätigkeitsbericht 2012, 3., 5.1., 5.5 und 7.

82 Liechtenstein, Belgien und Deutschland.

5.2. Gemeinsame Kontrollinstanz Schengen (GKI Schengen)

Das bisher genutzte Schengen Informationssystem (SIS1forALL) wurde durch die zweite Generation (SIS II) abgelöst, welche mehr technische Möglichkeiten bietet. Neu können z. B. in Bezug auf Personenfahndungen Fotos und Fingerabdrücke erfasst werden. Im Bereich der Sachfahndungen wurden insbesondere die Kategorien erweitert. Mit der Einführung des **SIS II** wurde auch eine gesetzliche Grundlage für eine neue Kontrollinstanz, die *SIS Supervision Coordination Group*, geschaffen. Diese Kontrollinstanz nahm ihre Arbeit auf.

Die Schengen-Staaten wurden am 6. Juni 2013 von der dänischen Polizei über einen **Datendiebstahl** informiert, der im Sommer 2012 stattgefunden hat. Hacker hatten sich Zugang zur dänischen SIS-Datenbank verschafft und 1,2 Millionen Datensätze (Personenfahndungen) auf ihren Rechner kopiert. Hier sind Personendaten aller Mitgliedstaaten betroffen, darunter auch 177 Datensätze von Liechtenstein. Der Vorfall wurde untersucht und es wurden Massnahmen eingeleitet. Bis heute liegen keine Anzeichen vor, dass Daten im SIS geändert, gelöscht oder hinzugefügt wurden. Auch gibt es keine Hinweise darauf, dass die Hacker die Daten weitergegeben haben oder dass diese an die Öffentlichkeit gelangt sein könnten. Da Liechtenstein seit der Migration auf SIS II über keinen nationalen SIS-Server mehr verfügt und alle Abfragen direkt beim Zentralserver in Strassburg tätigt, kann das Risiko eines vergleichbaren Vorfalls in Liechtenstein ausgeschlossen werden.

Weiters wurde u. a. das folgende Problem aufgegriffen: In bestimmten Fällen gelangen die einzelnen Staaten in Bezug auf ausgeschriebene (Sach-) **Fahndungen** zu **unterschiedlichen Ergebnissen**. Während im einen Staat ein in gutem Glauben gekauftes Auto einen rechtmässigen Besitzer hat, kann nach demselben Auto durch einen anderen Staat, in dem es gestohlen wurde, gefahndet werden. Das Problem ist, dass einerseits der neue Besitzer das Auto aufgrund der Fahndung nur innerhalb der Staatsgrenzen benutzen kann und andererseits der Bestohlene im anderen Staat sein Auto nicht zurückerhält. Ähnliche Fälle liegen offensichtlich in mehreren Schengen-Staaten vor, so auch in Liechtenstein. Dieses Thema soll weiterverfolgt werden.

5.3. Eurodac Supervision Coordination Group

2013 wurde unter anderem die **Asylverfahrens-Richtlinie**[83] und die **Eurodac-Verordnung**[84] angenommen. Die neue Verordnung ist ab Juli 2015 anwendbar. Hervorzuheben ist insbesondere der neu geregelte Zugriff von Strafverfolgungsbehörden auf die Eurodac-Datenbank.[85] Die Gruppe möchte diesbezüglich die weitere Entwicklung genauer beobachten. Bis zum Inkrafttreten der neuen Eurodac-Verordnung möchte die Gruppe Herausforderungen und den Handlungsbedarf definieren.

Im Tätigkeitsbericht 2012 haben wir über das Problem mit **unlesbaren Fingerabdrücken** im Asylverfahren informiert. Da die Eurodac-Verordnung keine entsprechende Regelung enthält, war ein Fragebogen erarbeitet worden, dessen Resultate vorgestellt wurden. Etwa die Hälfte der Staaten hat keine formellen Regeln, wie in Fällen von unlesbaren Fingerabdrücken vorgegangen werden soll. Sie verweisen lediglich auf „Best Practice" Guidelines oder unverbindliche Dokumente. Was die Praxis in Liechtenstein angeht, nimmt das Ausländer- und Passamt (APA) die Fingerabdrücke nach zwei Wochen nochmals ab. Sollten die Abdrücke permanent unlesbar sein, wird das normale Asylverfahren eingeleitet. Bei Unlesbarkeit aufgrund von Manipulation der Fingerabdrücke tritt das APA nicht auf den Antrag ein.

83 Richtlinie 2013/32/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 zu gemeinsamen Verfahren für die Zuerkennung und Aberkennung des internationalen Schutzes (Neufassung).

84 Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Grosssystemen im Raum der Freiheit, der Sicherheit und des Rechts (Neufassung).

85 Für genauere Informationen siehe Tätigkeitsbericht 2012, 5.3.

5.4. VIS Supervision Coordination Group

Mit der VIS-Verordnung wurde die **VIS Supervision Coordination Group (VIS SCG)** ins Leben gerufen.[86] Mitglieder sind die nationalen Kontrollstellen und der EDPS.[87] Ihre Aufgabe besteht in der Zusammenarbeit, dem Austausch von relevanten Informationen, der gegenseitigen Unterstützung sowie der koordinierten Überwachung des zentralen Visa-Informationssystems und der nationalen VIS-Systeme. Zweck des Visa-Informationssystems ist die Verbesserung der Durchführung der gemeinsamen Visumpolitik, der konsularischen Zusammenarbeit und der Konsultation zwischen zentralen Visumsbehörden durch die Erleichterung des Datenaustauschs zwischen Mitgliedstaaten über Visumanträge. Die Datenschutzbehörden sind angehalten, regelmässig eine Kontrolle der nationalen Datenverarbeitung im VIS[88] in Bezug auf ein relevantes Thema einerseits und ein Audit des nationalen Teils des VIS anderseits durchzuführen. Alle zwei Jahre soll die Gruppe einen Tätigkeitsbericht abgeben, der pro Mitgliedstaat ein Kapitel enthalten soll. Ein gemeinsamer Punkt, der angegangen wurde, ist die *Auslagerung der Datenbeschaffung für Visa-Anträge*. Einzelne Länder haben die Vorbereitung der Dossiers (Erhebung der Fingerabdrücke, Aufnahme der Daten etc.) an externe Dienstleister ausgelagert bzw. werden sie in Zukunft auslagern. Hierbei haben sich insbesondere Zuständigkeitsfragen in Bezug auf Kontrollen in Drittländern gestellt. Das Thema wird wohl noch weiter behandelt und verfolgt werden. Was die Praxis in Liechtenstein angeht, werden Visaanträge, die im Ausland gestellt werden, von den Schweizer Aussenstellen entgegengenommen und ans APA weitergeleitet, wo sie geprüft werden. Es gibt drei mögliche Resultate: Entweder wird das Schengen-Visum (höchstens 90 Tage) vergeben oder dem Visumantrag wird nicht stattgegeben oder es wird ein Visum mit einer „Limited Territorial Validity" vergeben.

Somit ist die Schweiz für einen wesentlichen Teil der Datenbearbeitung bei Visaanträgen, die in Drittstaaten gestellt werden, verantwortlich. Eine Zusammenarbeit mit dem in der Schweiz zuständigen EDÖB[89] wurde noch nicht geprüft. Die Wichtigkeit dieser neu geschaffenen Arbeitsgruppe konnten wir noch nicht beurteilen.

5.5. Europarat

Nachdem der **Konventionsausschuss** die Arbeit an der *Revision des Datenschutzabkommens* abgeschlossen hatte, war noch der Textentwurf des *Erläuternden Berichtes* zu behandeln. Ausserdem war die Arbeit bezüglich der *Empfehlung (87) 15 zur Bearbeitung von Personendaten im Polizeibereich* noch nicht abgeschlossen.[90] Auch als Folge des NSA-Überwachungsskandals wurde vom Experten empfohlen, eine Konvention zum Polizei- (einschliesslich Geheimdienst-) Bereich auszuarbeiten. Die Schaffung einer Konvention ist oft der nächste Schritt nach der Schaffung einer nicht verbindlichen Empfehlung. Ausserdem ist die Überarbeitung der *Empfehlung (89) 2 zum Datenschutz am Arbeitsplatz* zu erwähnen.

Das Ministerkomitee setzte einen **Adhoc-Ausschuss (CAHDATA)** zur Finalisierung der Arbeit an der neuen **Datenschutzkonvention** ein. Dieser Ausschuss sollte primär mit Vertretern von Ministerien besetzt sein. Da es um eine Fortführung der Arbeit des Konventionsausschusses aus den Vorjahren ging, erklärten wir uns bereit, hier mitzuwirken.

86 Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) Artikel 2. Das zentrale Visa-Informationssystem (C-VIS) ist ein System zum Austausch von Daten über Visa für einen kurzfristigen Aufenthalt zwischen den Mitgliedstaaten des Schengenraums. Es soll vor allem der Durchführung der gemeinsamen Visumpolitik und der konsularischen Zusammenarbeit dienen.

87 Der Europäische Datenschutzbeauftragte.

88 Vgl. Visa-Informationssystem-Verordnung.

89 Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte.

90 Siehe Tätigkeitsbericht 2011, 5.4.

5.6. Internationale Datenschutzkonferenz

An der Internationalen Datenschutzkonferenz (an der wir nicht teilnahmen) entstand aufgrund des NSA-Abhörskandals die Forderung, dass der **Datenschutz auf UNO-Ebene** geregelt werden sollte, um der Privatsphäre mehr Achtung zu geben. Wir unterstützen dieses Anliegen und gelangten damit an die Regierung. Auf Initiative Deutschlands und Brasiliens verabschiedete die UN-Vollversammlung eine entsprechende Resolution. Diese ist zwar nicht rechtlich verbindlich. Immerhin wird das Thema nun aber durch die UNO in den Fokus genommen, was das Ziel der Internationalen Konferenz war.

Von der **Berlin Gruppe (IWGDPT)** wurden wieder verschiedene Arbeitspapiere veröffentlicht.[91] Ein Papier richtet sich an Anbieter von Internetseiten sowie an Softwareentwickler und Service Provider, die *Trackingtechnologien* anbieten bzw. nutzen. Es behandelt die Entwicklung von Trackingtechnologien und ihre möglichen Auswirkungen auf die Privatsphäre.[92] Zudem wurde ein Arbeitspapier betreffend den Einsatz von *Drohnen* veröffentlicht.[93] Es enthält eine allgemeine Einführung in die Thematik und Empfehlungen wie beispielsweise zur Zweckbindung und Informationspflicht.

5.7. Privatim – Vereinigung der Schweizer Datenschutzbeauftragten

Die **Arbeitsgruppe Gesundheit (AGX)** von privatim beschäftigt sich mit verschiedenen Themen, die aufgrund der Nähe des liechtensteinischen zum schweizerischen Gesundheitssystem auch für uns relevant sind, wie z. B. Entwicklungen im Bereich *eHealth*, *SwissDRG* und *Klinikinformationssysteme*.

6. In eigener Sache

Bei der **Diskussion unseres Tätigkeitsberichts im Landtag** werden immer wieder Fragen gestellt. Solche Fragen können an uns gerichtet sein. Dann sind wir dazu aufgerufen, sie zu beantworten. Fragen können aber auch der Regierung gestellt werden. Die Erfahrung hat gezeigt, dass diese nicht oder nur teils beantwortet wurden, was aus unserer Sicht unbefriedigend ist. Deshalb wendeten wir uns an die Stabstelle Regierungssekretär mit der Bitte, einen *Prozess zu definieren*, damit solche Fragen durch das zuständige Ministerium an den Landtag beantwortet werden. Bei der Diskussion unseres letztjährigen Tätigkeitsberichts gab es Fragen in Bezug auf eine mögliche Revision des Sorgfaltspflichtgesetzes, der Strafprozessordnung und einer Gebührenerhebung für unsere Tätigkeiten.[94] In einem Schreiben des Regierungssekretärs an den Landtagssekretär wurden die Fragen zur Strafprozessordnung und zu einer möglichen Gebührenerhebung beantwortet. Wir begrüssen die Festlegung dieses Verfahrens.

Der Landtag stimmte dem Abkommen über die **Zusammenarbeit mit Eurojust und Europol** zu. Beide Abkommen beinhalten Regelungen zum Datenschutz. Bei der Landtagsdiskussion gab es auch kritische Stimmen zur Einhaltung des Datenschutzes.[95] Zur Einhaltung der Datenschutzbestimmungen bei den genannten Abkommen gibt es eigene Gremien.[96] Im Landtag geäusserte Bedenken wären theoretisch Sache dieser Kontrollgremien, bei denen nur Datenschutzbehörden der EU-Länder teilnehmen dürfen.

91 http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group.

92 Arbeitspapier Webtracking und Privatsphäre, http://www.datenschutz-berlin.de/attachments/951/675.46.18.pdf.

93 http://www.datenschutz-berlin.de/attachments/1005/675.47.26.pdf?1389364999.

94 Siehe Landtagsprotokoll der Sitzung vom Mai 2013: http://www.landtag.li/protokolle/default.aspx?mode=lp&prim=2013&value=5&id=7464&backurl=?mode=lp%26prim=2013%26value=5.

95 http://www.landtag.li/protokolle/default.aspx?mode=lp&prim=2013&value=10.

96 Für Europol: http://europoljsb.consilium.europa.eu/about.aspx und für Eurojust: http://eurojust.europa.eu/about/structure/jsb/Pages/independent-joint-supervisory-body.aspx.

7. Ausblick

Der Bericht zeigt, dass der Schutz der Privatsphäre vor neue **Herausforderungen** gestellt wird, die angegangen werden müssen. Aufgrund der Kleinheit der Strukturen sind uns Synergien wichtig. Gute Kontakte können sehr nützlich sein. Dies gilt auch für Kontakte ins Ausland. Datenschutz kann und muss aus einer europäischen und teils globalen Brille gesehen werden. Viele im Bericht erwähnte Punkte sind im Fluss und werden durch uns weiter verfolgt werden.

Seit dem 1. Februar 2014 besteht in Liechtenstein die Möglichkeit, ein **Datenschutz-Gütesiegel** zu erwerben. Damit können Unternehmen und Behörden nach aussen klar sichtbar machen, dass das Thema Datenschutz einen hohen Stellenwert geniesst. Wir sehen in einem solchen Gütesiegel einen möglichen Wettbewerbsvorteil und ein wichtiges, Vertrauen schaffendes Element. Deshalb begrüssen wir die entsprechende *Verordnung über die Datenschutzzertifizierungen*.[97] Damit konnte ein schon länger dauerndes Vorhaben abgeschlossen werden. Wir werden auch hier weiterhin eine aktive Rolle einnehmen.

Im Regierungsprogramm wurde ein Punkt aufgenommen, der uns schon länger wichtig ist: der **Datenstandort Liechtenstein**.[98] Immer wieder hört man, dass nationale oder europäische Lösungen als Folge des NSA-Abhörskandals[99] geschaffen werden sollen. Neben diesem Schutzaspekt gibt es auch wirtschaftliche Gründe, diese Idee zu verfolgen. Wir sind gerne bereit, unseren Beitrag hierzu zu leisten.

Die **Datenschutzreform in Europa** hat eine Pause eingelegt. Wir erinnern daran, dass Aufgaben und Verantwortlichkeiten bei Dateninhabern zunehmen, die Rechte der betroffenen Personen gestärkt werden und auch die Datenschutzbehörden mehr Befugnisse erhalten sollen. Hier sind teils drastische Bussen vorgesehen.[100] Im Rahmen der vorhandenen Ressourcen werden wir das Thema weiterhin verfolgen. Es wird eine direkt anwendbare Verordnung geben, die aber dennoch Teile enthalten wird, die national umzusetzen sind. Dies wird Aufgabe des Gesetzgebers sein. Wir sind gerne bereit, hier mitzuarbeiten.

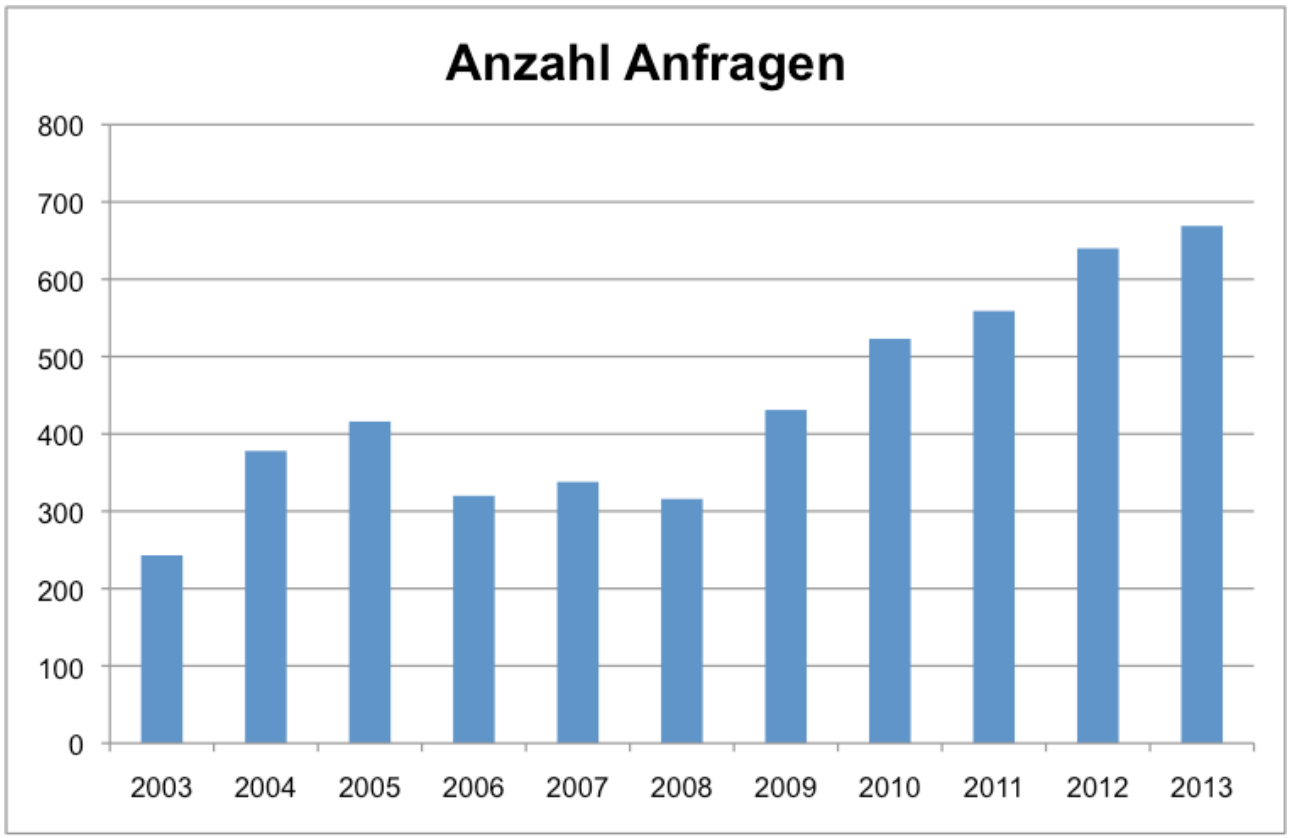
Aufgrund des Umfangs und der Komplexität des Datenschutzes, welcher als Querschnittsmaterie fast alle Bereiche des Lebens tangiert, entschieden wir uns 2012 für folgende **Schwerpunkte**: *Gesundheit und Soziales*, *Finanzplatz* sowie *Datensicherheit*. Diese Bereiche sind, jeder für sich, schon sehr vielschichtig. Dementsprechend braucht es eine gewisse Aufbauarbeit, bis hier konkrete Tätigkeiten angegangen werden können. Vor allem im Bereich Gesundheit haben wir erste Schritte gemacht und Kontakte hergestellt. Liechtenstein ist ein Finanzplatz; dieser Bereich ist dementsprechend wichtig und komplex. Hier wollen wir erste Schritte setzen. Datensicherheit ist in einer automatisierten Welt fast immer ein Thema; in diesem Bereich werden wir konkrete Tätigkeiten definieren.

97 Vgl. Art. 14a DSG i. V. m. VDSZ; siehe hierzu auch Tätigkeitsbericht 2012, 7.
98 Siehe Tätigkeitsbericht 2008, 4. und Tätigkeitsbericht 2010, 1.
99 Siehe 2.1 und 2.2.
100 Siehe Tätigkeitsbericht 2012, 3., 5.1. und 7.

8. Anhang

8.1. Statistik der Anfragen

Die Beratung privater Personen und Behörden ist eine Kernaufgabe. Im Berichtsjahr gingen insgesamt 669 Anfragen ein; das ist ein neuer Höchststand. Gegenüber dem Vorjahr bedeutet das eine Zunahme um 29 Anfragen. Die nachfolgende Abbildung zeigt die Entwicklung der Anzahl Anfragen über die vergangenen 11 Jahre.



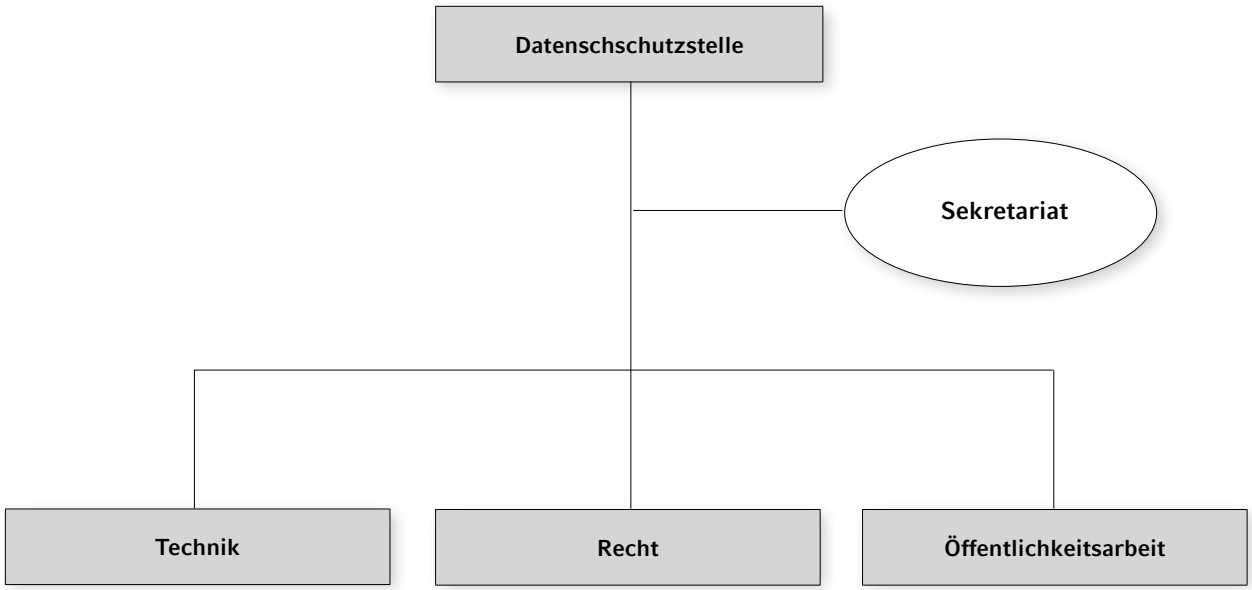
Sachgebiete und Anfragende

Aufgegliedert nach Sachgebieten stehen allgemeine Datenschutzthemen an der Spitze der Anfragen. Auch zu den Themen Datenbekanntgabe im Inland, Polizei/Sicherheit, Technologischer Datenschutz und zur Geltendmachung gesetzlicher Rechte bekamen wir eine grosse Zahl an Anfragen. Die meisten Anfragen stammen (abgesehen von einem einmaligen Effekt in der Gruppe „Internationales“) nach wie vor von der Landesverwaltung.

Die folgende Statistik zeigt auf, zu welcher Gruppe die Anfragenden gehörten und welches Sachgebiet betroffen war.

	Anwaltsbüros	Gemeinden	Industrie, Gewerbe, Dienstleistung	Internationales	Landesverwaltung, Behörden	Medien	Privatpersonen	Vereine, Verbände
Datenschutz allgemein	6		26	57	56	42	21	8
Arbeitsbereich	2	1	5		3	1	2	6
Datenbekanntgabe Inland	3	4	1		24	2	11	2
Datenbekanntgabe mit Auslandbezug	12		13	26	13	2	1	
Geltenmachung gesetzlicher Rechte	4		3		16	3	32	
Gesetzesvorhaben					10			
Gesundheit/Soziales			3		3	1		1
Keine Zuständigkeit DSS			1				1	
Polizei/Sicherheit				52	1	9	1	1
Register der Datensammlungen	6		6		2			1
Schengen/Dublin				29				
Technologischer Datenschutz	14		9	5	9	2	16	8
Telekommunikation	7		2		2		2	
Umsetzung/Anwendung europäischen Rechts				24	6			
Videoüberwachung		2	3		9		11	1
Wirtschaft/Finanzen/ Gewerbe/Versicherungen					1			
Gesamtergebnis	**54**	**7**	**72**	**193**	**155**	**62**	**98**	**28**

8.2. Organigramm



DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Kirchstrasse 8
FL-9490 Vaduz

Telefon +423 236 60 90
Fax +423 236 60 99

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