DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN


# Tätigkeitsbericht 2014

## Datenschutzstelle des Fürstentums Liechtenstein

# INHALTSVERZEICHNIS

# 1. EINLEITUNG

Dies ist unser 13. Tätigkeitsbericht.

Dem aufmerksamen Leser wird auffallen, dass wir die **Struktur (wieder) nach der Erfüllung von Gesetzesaufgaben gegliedert** haben. In den letzten Jahren orientierte sich der Aufbau mehr nach spezifischen Themen. Durch die neue inhaltliche Gliederung kehren wir zu unserem ursprünglichen Ansatz zurück. Nun ist besser ersichtlich, wie das Datenschutzgesetz (DSG) gelebt wird und vor allem, wie wir unseren gesetzlichen Aufgaben nachkamen. Weiterhin ist auch der Rechenschaftsbericht beizuziehen, in dem wir ebenfalls über unsere Aktivitäten informieren, jedoch weniger inhaltlich. Insgesamt geht es uns darum, den «Puls» des Datenschutzgesetzes zu fühlen.

Der Anwendungsbereich des DSG ist enorm. Vor diesem Hintergrund müssen Prioritäten festgelegt werden, was wir 2012 mit inhaltlichen **Schwerpunktthemen taten: Gesundheit und Soziales, Finanzen, Datensicherheit und Jugendliche.** An diesen Schwerpunkten wollen wir weiter festhalten. Absätze zu den Schwerpunktthemen haben wir in diesem Bericht entsprechend gekennzeichnet.

Wir konnten wieder **zahlreiche Anfragen von Behörden, Unternehmen und Bürgern** beantworten – nach dem vergangenen Jahr wieder ein neuer Rekord. Dies kann gewiss auf ein gestiegenes Bewusstsein für den Schutz der Privatsphäre zurückgeführt werden. Einige Anfragen, vor allem aus dem Bereich der genannten Schwerpunktthemen, werden dargestellt (siehe Kapitel 2.1).

Die Arbeit im Zusammenhang mit der **Gesetzesvorbereitung** intensivierten wir, und auch zu einzelnen Fällen im Rahmen der **Rechtsprechung** nahmen wir Stellung (siehe Kapitel 2.2 und 2.3). Damit achten wir darauf, dass die Anliegen des Datenschutzes bei anderen sehr wichtigen Institutionen berücksichtigt werden. Verschiedene **Projekte** konnten wir aktiv begleiten und beratend unterstützen. Beispielsweise wiesen wir bei mehreren Treffen mit dem Landesspital auf Möglichkeiten für eine datenschutzkonforme Ausgestaltung eines *Klinikinformationssystems (KIS)* hin. Weiter suchte die Steuerverwaltung im Zusammenhang mit einem *Steuerabkommen* bereits in einem sehr frühen Projektstadium das Gespräch mit uns. Dadurch konnten wir bereits sehr früh im Sinne einer die Privatsphäre der Betroffenen schützenden Weise mitarbeiten (siehe Kapitel 2).

Diese präventive Arbeit sollte die Bedeutung der **Aufsicht** verringern. Nichtsdestotrotz gibt es Fälle, in denen wir auch unsere Aufsichtsaufgaben wahrnehmen müssen. Insbesondere die *Schengen-Mitgliedschaft* verlangt regelmässige Kontrollen. So stellten wir beispielsweise bei einer Überprüfung der Protokollierung im Schengener Informationssystems (SIS II) Nachbesserungsbedarf fest (siehe Kapitel 3).

*Nach wie vor ist für uns die* **Sensibilisierung der Öffentlichkeit** für den Schutz der Privatsphäre zentral. Neben eigenen Veranstaltungen wie am *Europäischen Datenschutztag* oder der jährliche *Gedankenaustausch mit den Datenschutzverantwortlichen* werden wir auch eingeladen, Vorträge zu halten. Im vergangenen Jahr waren wir auch mit einem Stand an der *LIHGA* präsent (siehe Kapitel 4).

Seit dem 1. Februar 2014 besteht die Möglichkeit der Einführung eines **Datenschutzgütesiegels**. Eine solche Zertifizierung generiert in vielerlei Hinsicht Mehrwert und kann einen Wettbewerbsvorteil schaffen, wenn Vertrauen ein wichtiges Element in einem Geschäftsmodell darstellt. Wir waren in Kontakt mit mehreren interessierten Unternehmen, bis Ende 2014 wurde jedoch noch kein Datenschutzgütesiegel vergeben (siehe Kapitel 5).

Die **europäische Zusammenarbeit** ist bei unseren Tätigkeiten sehr wichtig. Der *automatische Austausch von Steuerinformationen* und dessen Umsetzung in Europa wurde ein Thema, das an Wichtigkeit gewann. Auch die Umsetzung des *EuGH-Urteils zu GoogleSpain* löste bei uns einzelne Anfragen aus, da Google sich weigerte, einen Link zu löschen (siehe Kapitel 6).

Die neue Struktur des Tätigkeitsberichts zeigt einige Schwächen des geltenden Gesetzes auf. Nach unserer Meinung wäre es an der Zeit, eine ähnliche **Evaluation des Datenschutzgesetzes** durchzuführen, wie sie in der Schweiz bereits vor einigen Jahren stattfand (siehe Kapitel 7). Das wäre auch sinnvoll, um die kommende *Datenschutzreform in Brüssel* vorzubereiten.

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, den Regierungsmitgliedern und Regierungsmitarbeitern sowie den Kollegen in der Landesverwaltung, und last but not least dem Team,

meinen Dank für die gute Zusammenarbeit aussprechen. Aber auch all jenen, 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 März 2015

Dr. Philipp Mittelberger
Datenschutzbeauftragter

# 2. ALLGEMEINE ORIENTIERUNG UND INDIVIDUELLE BERATUNG

## 2.1. Anfragen

Die Entwicklungen der letzten Jahre bestätigten sich auch im vergangenen: Die Anzahl der Anfragen, die an uns gerichtet wurden, erreichten erneut einen Höchststand.[1] Davon gingen viele per Telefon ein und konnten ohne grossen Aufwand beantwortet werden. Bei anderen war dies nicht der Fall. Es würde den Rahmen dieses Berichts sprengen, alle Anfragen darzustellen. Jedoch sollen einige Fragen und deren Beantwortung dargestellt werden, die für die Öffentlichkeit interessant sein dürften.

In zwei Fällen, in denen sich **Google weigerte, Personendaten aus der Suchtrefferliste der Suchmaschine zu entfernen**,[2] wurden wir um Hilfe gebeten. Dies, weil Google darauf hingewiesen hatte, dass man sich an die nationale Datenschutzbehörde wenden kann, falls man mit der Entscheidung von Google nicht einverstanden ist. Das war in unserem Fall nicht so einfach, da es *in Liechtenstein keine Niederlassung von Google* im Sinne der Datenschutzrichtlinie gibt. Somit stellte sich die Frage, ob wir eine solche Beschwerde entgegennehmen und an eine Datenschutzbehörde in einem Land zur Entscheidung weiterleiten können oder sollen, in dem Google eine Niederlassung hat. Bis Ende des Jahres war nicht geklärt, an welche Datenschutzbehörde wir eine solche Beschwerde weiterleiten sollen.

Eine andere Beschwerde ging im Rahmen des **Betrieblichen Mobilitätsmanagements** der Landesverwaltung ein. Hier wurde die Frage gestellt, ob für die Erfassung der Nummernschilder der Mitarbeiter eine genügende gesetzliche Grundlage besteht. Wir stellten fest, dass für die Abfrage bei der Motorfahrzeugkontrolle sowie die Erfassung der Nummernschilder der Mitarbeiter der Landesverwaltung zwar eine Kompetenz im Gesetz vorgesehen ist, jedoch keine Kompetenz zur Führung einer eigenen Datenbank besteht. Wir regten die *Schaffung einer ausreichenden gesetzlichen Grundlage* an und brachten auf Anfrage einen Vorschlag zur Formulierung einer entsprechenden Bestimmung ein.

Das Schulamt erwägt die **Einführung eines Cloud-Dienstes, konkret den Einsatz von Microsoft Office 365 an heimischen Schulen**. Wir wurden gebeten, die datenschutzrechtlichen Fragen zu prüfen. Die Vorteile von Office 365 liegen auf der Hand: Über den Abschluss eines Volumenlizenzvertrags haben die Schulen die Möglichkeit, ihren Schülern und Lehrpersonen das volle Office-Programm kostenlos zum Download anzubieten. Durch die Nutzung von Cloud-Diensten entstehen jedoch nicht zu unterschätzende Risiken, da von den Cloud-Anwendern Computerressourcen genutzt werden, auf die sie selbst keinen direkten Zugriff bzw. über die sie keine Kontrolle haben.[3] Durch die Möglichkeit, die Lizenz für Office 365 über den «educa.ch»-Rahmenvertrag zu erwerben, ist eine datenschutzkonforme Nutzung grundsätzlich gewährleistet.[4] Allerdings – auch wenn einer Nutzung von Office 365 im Bildungsbereich somit nichts entgegensteht – muss darauf geachtet werden, welche Daten in der Cloud bearbeitet werden bzw. «Cloud-tauglich» sind. Als

1 Siehe unter 9.1.
2 Vgl. EuGH-Urteil «Google Spain SL, Google Inc.», siehe unter 4.3 und 6.1.
3 Vgl. dazu die Ausführungen zu Microsoft Live@edu im Tätigkeitsbericht 2011, Pkt. 1.8., Cloud Computing im Tätigkeitsbericht 2011, Pkt. 1.6., sowie «Datenschutzrechtliche Chancen und Risiken von Cloud Computing» von Philipp Mittelberger und Gabriele Binder, in «Jus & News» 2011/2, S. 163ff.
4 educa.ch, der schweizerische Bildungsserver ist ein Gemeinschaftsprojekt der Schweizerischen Fachstelle für Informationstechnologien im Bildungswesen (SBFI) und der Schweizerischen Konferenz der kantonalen Erziehungsdirektoren (EDK). educa.ch hat einen Rahmenvertrag mit Microsoft abgeschlossen, der die datenschutzrechtliche Situation beim Einsatz von Office 365 Diensten speziell regelt. Mit dem Rahmenvertrag wird über das Schutzniveau der europäischen Standardvertragsklauseln, die ebenfalls Bestandteil des Rahmenvertrags bilden, hinausgegangen. Beispielsweise dürfen Daten nur innerhalb von Europa gespeichert werden.

Grundsatz muss gelten, dass die *Zurückhaltung der Nutzung des Cloud-Dienstes mit der Sensitivität der bearbeiteten Daten steigt.*

Wir wurden nach bestehenden Vorgaben und Regelungen für die **Veröffentlichung von Fotos von Schülern auf Internetseiten von Schulen** angefragt. Dazu verfasste die Artikel-29-Datenschutzgruppe bereits 2009 eine Stellungnahme.[5] Es sollte demnach stets gründlich geprüft werden, um welche Art von Foto es sich handelt, ob seine Veröffentlichung relevant ist und welcher Zweck damit verfolgt wird. Die Kinder und ihre gesetzlichen Vertreter sind auf die Veröffentlichung hinzuweisen. Beabsichtigt die Schule, einzelne Fotos bestimmter Kinder zu veröffentlichen, ist die vorherige *Einwilligung vor allem der Eltern einzuholen*. Bei Fotos von schulischen Veranstaltungen brauchen Schulen keine vorherige Zustimmung der Eltern, sofern die Fotos nicht die **einfache Identifizierung von Schülern ermöglichen**. Gleichwohl hat die Schule in diesen Fällen die Kinder und Eltern darüber zu informieren, dass Fotos gemacht wurden und wie sie verwendet werden. So erhalten sie Gelegenheit, sich einer Aufnahme zu verweigern. Betroffene Personen (auch die Kinder selbst) dürfen jederzeit einer Veröffentlichung ohne Angabe von Gründen widersprechen. Ein solcher Widerspruch ist zu berücksichtigen. Damit ist von einer Veröffentlichung abzusehen oder ein Foto offline zu nehmen.[6]

Das Kostenwachstum im Gesundheitswesen ist ein bekanntes Phänomen und eine grosse Herausforderung. Möglichkeiten der Eindämmung des Wachstums werden laufend diskutiert und Wege dahin werden gesucht. In diesem Zusammenhang erhielten wir von der Regierung eine Anfrage. Sie wollte von den Krankenkassen Daten, um mögliche neue Wege zur Kostendämmung ausmachen zu können. Es sollten durch Erkennung von Mustern in den Daten Erkenntnisse über kostentreibende Behandlungsmethoden oder Gründe für extrem häufige Arztbesuche gewonnen werden. Dazu werden Behandlungsdaten mit pseudonymisierten Patientendaten benötigt. Vor diesem Hintergrund sahen wir keine grundsätzlichen Hindernisgründe an einer **Datenbekanntgabe der Krankenkassen an die Regierung**. Dies zumindest insofern, als es sich (vorerst) um eine einmalige Datenlieferung an die Regierung handelt. Je nach Ergebnis der Untersuchung kann es zu neuen Datenflüssen kommen, die dann möglicherweise neu beurteilt werden müssen.

In einem anderen Fall wurden wir darauf aufmerksam gemacht, dass ein **Austausch von Gesundheitsdaten** zwischen der LAK, der Familienhilfe und dem Landesspital stattfindet. Ungeachtet der übertragenen Inhalte ergaben sich insbesondere Fragen zur Datensicherheit. Gibt es benutzerfreundliche und «einfache» Möglichkeiten eines sicheren Datentransfers von sensiblen Personendaten im Gesundheitsbereich? Dies haben wir zum Anlass genommen, allgemein auf eine sichere Kommunikation hinzuwirken. Es wurde der persönliche Kontakt mit den genannten Institutionen gesucht, um mögliche Lösungen zu diskutieren.

Nach einer Meldung prüften wir die Umsetzung von **Massnahmen zur Datensicherheit bei einer Internetplattform**. Auf dieser konnten sich registrierte Nutzer mittels Benutzername und Passwort anmelden sowie persönliche Daten erfassen. Die Prüfung ergab, dass sämtlicher Datenverkehr, samt der Übermittlung der Zugangsdaten, unverschlüsselt erfolgte. Wir konnten bei den Verantwortlichen erfolgreich darauf hinwirken, dass zukünftig sämtliche Datenübermittlungen über verschlüsselte Verbindungen stattfinden. Auch in anderen Fällen konnten wir beobachten, dass *Zugangsdaten auf Webseiten häufig unverschlüsselt* übertragen werden, wodurch ein Ausspähen von Passwörtern ohne grossen Aufwand möglich ist. Gerade weil Nutzer in der Praxis ihre Passwörter mehrfach auf verschiedenen Plattformen verwenden, stellt ein ausgespähtes Passwort für einen Nutzer ein besonders hohes Risiko dar.[7] Deshalb wird die Datenübermittlung über unsichere Verbindungen zukünftig einen *Schwerpunkt unserer Sensibilisierungsarbeit* darstellen.

Für Kinder und Jugendliche ist die Vernetzung über das Internet zentral. Nach wie vor gilt: wer nicht angeschlossen ist, ist ausgeschlossen. **Jugendtreffs** bieten häufig kostenlosen Internetzugang über **WLAN** an, um für ihre Zielgruppe attraktiv zu bleiben. Das Kinder- und Jugendgesetz (KJG) schreibt Betreibern solcher WLAN-Hotspots vor, dass sie durch geeignete und zumutbare Massnahmen sicherzustellen haben, dass Kinder und Jugendliche keinen Zugang zu Inhalten bekommen, die für ihre Altersgruppe nicht geeignet sind. So können beispielsweise Webfilter eingesetzt werden. Gerade durch die Verwendung von Filter- und Überwachungssoftware ergeben sich

5 Artikel-29-Datenschutzgruppe, Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen) (WP 160), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_de.pdf.

6 Siehe Tätigkeitsbericht 2008, Pkt. 10.2.1.

7 Zu sicheren Passwörtern, siehe Tätigkeitsbericht 2011, Pkt. 1.2.

zahlreiche Berührungspunkte mit der Privatsphäre der Betroffenen. So sind beispielsweise Informationspflichten einzuhalten und personenbezogene Auswertungen des Surfverhaltens nur eingeschränkt zulässig. Wir regten bei einer Sensibilisierungsveranstaltung an, speziell für Jugendtreffs und für andere vergleichbare Orte eine *einheitliche datenschutzfreundliche Lösung anzuschaffen*. Eine solche Lösung erleichtert den Erfahrungsaustausch zwischen den betreibenden Stellen und reduziert den Aufwand für die Wartung. Zudem können bei einer vorgelagerten Evaluation möglicher Lösungen sowohl die Vorgaben des Kinder- und Jugendschutzes als auch jene des Datenschutzes entsprechend berücksichtigt werden.

Das **Zentrale Personenregister (ZPR)** ist eine zentral geführte Datenbank der Landesverwaltung. Darin gespeichert sind unter anderem sämtliche Einwohner Liechtensteins. Sie dient insbesondere der Erleichterung administrativer Abläufe; zahlreiche Amtsstellen haben Zugriff.[8] Die Rechtsgrundlage der Datenbearbeitung findet sich im ZPRG.[9] Die *unbefugte Datenbearbeitung ist strafbeschwert.*[10] In diesem Zusammenhang wurde von der ZPR-Kommission und von uns angeregt, dass für jene Personen mit ZPR-Zugriffsrechten anstelle einer zwingenden Bestrafung mit Busse die Einführung eines gestuften Sanktionssystems (z. B. Sanktionen nach dem Staatspersonalgesetz) überlegt werden sollte. Aus Sicht der Regierung ist es durchaus gerechtfertigt, dass in den Fällen der unbefugten Bearbeitung, Abfrage oder Bekanntgabe von Daten aus dem ZPR sowie der Verwendung der eindeutigen Personenidentifikationsnummer (PEID)[11] ohne Berechtigung eine Verbüssung erfolgt. Dies sind nach Meinung der Regierung keine Kavaliersdelikte. Allein aus generalpräventiven Gründen sei es angezeigt, die Strafbestimmung des Art. 19 ZPRG nicht zu ändern.

Die technologische Entwicklung ermöglicht es, mit immer kleineren Geräten, die zudem immer günstiger in der Anschaffung werden, Bild- und/oder Tonaufnahmen zu machen. Man denke an **Kleinstkameras in Autos (Dashcams)**, Kameras, die an Skihelmen befestigt werden usw. Auch wenn in den meisten Fällen diese Aufnahmen für den persönlichen Gebrauch gemacht werden, fehlt generell das Bewusstsein, dass mit diesen Aufnahmen meist auch Personendaten erfasst werden[12] und dass dieses Erfassen von Personendaten teilweise sogar strafbeschwert ist.[13] In diesem Zusammenhang wurden wir angefragt, ob es legal ist, *Mobbingverhalten am Arbeitsplatz zu Beweiszwecken zu filmen*. Wir sind der Auffassung, dass die Anwendung der entsprechenden Strafbestimmungen in bestimmten Fällen zu stossenden Ergebnissen führen könnten und haben bei der Regierung angeregt, sie möge prüfen, ob allenfalls gewisse Ausnahmen der Strafbarkeit von Bild- als auch Tonaufnahmen zu Beweiszwecken in Zivil- und Strafverfahren im Gesetz verankert werden sollten.

Die Blossstellung im Internet (**«naming and shaming»**) ist ein trauriges Phänomen. Dazu werden oft Informationen, die man unter Umständen über sich selbst ins Internet gestellt hat, in Kombination mit sonst öffentlich zugänglichen Informationen benutzt. Beispielsweise fanden sich mehr als 73 Millionen Facebook-Profilfotos auf www.jerk.com, wo die betroffenen *Personen öffentlich beschimpft und blossgestellt* wurden. Auch in Liechtenstein waren mehrere Personen betroffen.[14] Die Betroffenen hätten Geld für die Wahrnehmung ihrer Rechte oder Löschung der Inhalte an die Betreiber zahlen sollen. Doch auf die Bezahlung von Geldbeträgen reagieren die Betreiber in den wenigsten Fällen. Ein solcher Webauftritt widerspricht in mehrfacher Hinsicht dem Datenschutzrecht. Die FTC in den USA hat nun Ermittlungen wegen Datenschutzverstössen gegen www.jerk.com eingeleitet.[15] Die Informationen der betroffenen Personen aus Liechtenstein sind mittlerweile auf der genannten Internetseite nicht mehr öffentlich abrufbar. Allgemein gilt in der Informationsgesellschaft, dass immer mehr Wert auf eine entsprechende Online-Reputation gelegt wird, was unseriöse Seitenbetreiber ausnutzen. *Wir raten daher zur Zurückhaltung bei der Veröffentlichung von persönlichen Informationen im Internet*. Dies gilt vor allem für Fotos und Videos.

Weiter gaben wir Hilfestellung im Zusammenhang mit der Löschung eines sogenannten **Fake-Profils**

8 Siehe Tätigkeitsbericht 2011, Pkt. 4, Tätigkeitsbericht 2008, Pkt. 3.1, Tätigkeitsbericht 2003, Pkt. 4.1.2.
9 Siehe Tätigkeitsbericht 2012, Pkt. 1.8.
10 Art. 19 ZPRG.
11 Zur PEID siehe auch Tätigkeitsbericht 2009, Pkt. 1.2. und Tätigkeitsbericht 2008, Pkt. 3.1. sowie Tätigkeitsbericht 2007, Pkt. 5.1.2.

12 Gemäss jüngster Rechtsprechung des EuGH ist die Ausnahme, die in der Datenschutzrichtlinie 95/46/EG für die Datenverarbeitung zur Ausübung ausschliesslich persönlicher oder familiärer Tätigkeiten vorgesehen wird, eng auszulegen. Auch Bilder von Kleinstkameras fallen somit grundsätzlich unter den Geltungsbereich des DSG (Urteil des EuGH vom 11.12.2014 Rechtssache C212/13 František Ryneš gegen Úřad pro ochranu osobních údajů, Randnrn. 29f).
13 Strafbestimmungen finden sich in Art. 118ff Strafgesetzbuch (StGB, LGBl. 1988 Nr. 37) sowie im Gesetz über den strafrechtlichen Schutz des persönlichen Geheimbereichs (LGBl. 1969 Nr. 34).
14 Siehe Tätigkeitsbericht 2012, Pkt. 2.1.
15 http://www.ftc.gov/news-events/press-releases/2014/04/ftc-charges-operators-jerkcom-website-deceiving-consumers.

**auf Facebook**. Auf Facebook war ein Profil samt Foto unter dem Namen der betroffenen Person erstellt worden. Das verwendete Foto war zuvor in einem anderen Zusammenhang im Internet veröffentlicht worden. Offensichtlich wurde durch den Ersteller des Fake-Profils das Foto von dort kopiert und zweckentfremdet. *Facebook stellt zur Meldung von gefälschten Profilen ein Formular zur Verfügung*.[16] Wir unterstützen betroffene Personen, doch müssen diese das Formular schliesslich selbst ausfüllen. Um noch gezielter beraten und Betroffene unterstützen zu können, sind wir an jeglichen Informationen interessiert, die schliesslich zu erfolgreichen Lösungen führten. Feedback von Betroffenen ist sehr willkommen.

## 2.2 Stellungnahmen zu Vorlagen und Erlassen

Die **Mitarbeit bei der Gesetzgebung** ist eine weitere Kernaufgabe. Das DSG sieht vor, dass wir zu Vorlagen und Erlassen, die für den Datenschutz erheblich sind, Stellung nehmen und insbesondere deren Übereinstimmung mit der allgemeinen Datenschutzrichtlinie überprüfen. Wir waren schon immer für möglichst klare Regeln in der Gesetzgebung. Rechtssicherheit dient allen. *Es hat sich sehr bewährt, wenn wir in einem möglichst frühen Verfahrensstadium in den Gesetzgebungsprozess einbezogen werden.* Dementsprechend erhalten wir alle Vernehmlassungsvorlagen der Regierung zur Stellungnahme zugestellt. Natürlich können wir nicht immer Stellung beziehen. Auch hier gilt es, eine entsprechende Auswahl zu treffen.

Insgesamt verstärkten wir unsere Tätigkeiten in diesem Bereich. Wir gaben zu zahlreichen Gesetzesvorhaben in verschiedenen Stadien des Gesetzgebungsverfahrens eine Stellungnahme ab. Exemplarisch soll im Folgenden aufgrund besonderer datenschutzrechtlicher Relevanz auf einige Gesetzesvorhaben näher eingegangen werden.

Das **FATCA-Gesetz** dient der Umsetzung des Abkommens zur Umsetzung des Foreign Account Tax Compliance Act (FATCA). Mit Hilfe dieser Regelwerke soll erreicht werden, dass sämtliche in Liechtenstein gehaltenen Vermögenswerte von Personen, die in den USA der Steuerpflicht unterliegen, in den USA auch tatsächlich besteuert werden. Zu diesem Zweck werden liechtensteinische Finanzinstitute dazu verpflichtet, bestimmte Informationen der Steuerverwaltung zu melden, die ihrerseits diese Informationen automatisch an die US-Steuerbehörde (IRS) weiterleiten wird. Wir wiesen darauf hin, dass die Datensicherheit im Rahmen der OECD-Initiative «Keeping it Safe»[17] generell und insbesondere auch im Rahmen von FATCA eine zentrale Rolle spielt. Wir regten an, eine Bestimmung im FATCA-Gesetz einzufügen, die klarstellt, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen.

Bei zwei Gesetzesvorlagen, konkret bei der **Abänderung des Bankengesetzes** sowie bei der **Abänderung des Staatspersonalgesetzes** ging es unter anderem um die Einführung eines Mechanismus zur Meldung von Verstössen, eines sogenannten *«Whistleblowing-Systems»*[18]. Dabei konnten wir auf ein Papier verweisen, das die europäische Sicht darstellt.[19] Die oberste Maxime bei einem solchen System muss der Schutz der Privatsphäre bzw. die Vertraulichkeit aller Beteiligten sein. Denn oft haben Hinweisgeber ein Naheverhältnis zu den gemeldeten Missständen und fürchten aufgrund dieser Nähe (etwa am Arbeitsplatz) negative Konsequenzen für sich. Dabei sind auch gewisse Berufs- oder Betriebsgeheimisse zu berücksichtigen, die nicht unberechtigt gebrochen werden dürfen. Diese unbedingte Vertraulichkeit kann beispielsweise durch angemessene Massnahmen der Datensicherheit erreicht werden. Bei der Einführung eines konkreten Systems gilt es, die Kleinheit des Landes speziell zu berücksichtigen. Denn die Anonymität einer Person ist hierzulande rasch aufgehoben. Sichergestellt werden muss ferner auch die Einhaltung des Gebots der Verhältnismässigkeit. Demnach dürfen die für das Verfahren notwendigen Informationen nur so lange bearbeitet und gespeichert werden, wie sie zur Erreichung des Zwecks erforderlich sind. Beim Bankengesetz war zudem die Schaffung einer Vorschrift über die Veröffentlichung von Sanktionen nach dem Prinzip des «naming and shaming» vorgesehen. Wir wiesen diesbezüglich auf das *Urteil des Europäischen Gerichtshofs (EuGH) in Sachen Schecke* hin.[20] Danach ist

16 https://www.facebook.com/ unter Hilfe – Inhalte melden. Hier z. B. «Wie melde ich ein gefälschtes Konto, das sich für mich ausgibt, wenn ich kein Facebook-Konto habe?».

17 http://www.oecd.org/ctp/exchange-of-tax-information/keeping-it-safe.htm.

18 Siehe unter 2.2. zum Thema «Whistleblowing».

19 Artikel-29-Datenschutzgruppe, Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmasslicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität (WP 117), siehe auch Tätigkeitsbericht 2006, Pkt. 7.1.

20 EuGH-Urteil vom 9.11.2010, C92/09 und C93/09, http://curia.eu-

eine Veröffentlichung als Ausnahme und Einschränkung in Bezug auf den Schutz der personenbezogenen Daten zwar nicht per se unzulässig, aber mit grosser Zurückhaltung zu betrachten.

Zu folgenden Gesetzesprojekten gaben wir ebenfalls eine Stellungnahme ab:[21]

- Energieeffizienzgesetz
- Gesundheitsgesetz
- Krankenversicherungsgesetz
- Marktmissbrauchsgesetz
- Steueramtshilfegesetz und Steueramtshilfegesetz-USA
- Strafprozessordnung
- Versicherungsaufsichtsgesetz
- Zahlungsdienstegesetz

## 2.3 Stellungnahmen zu Datenschutzfragen in hängigen Verfahren vor Rechtsmittelbehörden – Rechtsprechung zum Datenschutzgesetz

Das DSG sieht auch vor, dass wir in hängigen Verfahren Stellungnahmen abgeben können. Damit soll eine Möglichkeit gegeben sein, dass wir quasi als «Anwalt des Datenschutzes» einbezogen werden. Diese Möglichkeit ist auf Ersuchen von entscheidenden Organen oder Rechtsmittelbehörden gegeben. In den vergangenen Jahren wurde davon kaum Gebrauch gemacht. Wir finden sie jedoch sehr sinnvoll und möchten an dieser Stelle auch darauf eingehen.

Im Zusammenhang mit einer **Datenbekanntgabe im Rahmen eines Zivilverfahrens** wurden wir zur Abgabe einer Stellungnahme aufgefordert. Grundsätzlich findet das DSG keine Anwendung auf hängige Zivilverfahren. Festzustellen ist jedoch, dass mit der Aufnahme von hängigen Zivilverfahren in den Katalog von Ausnahmen vom Geltungsbereich des Datenschutzgesetzes[22] Liechtenstein seiner Verpflichtung, die Bestimmungen der Datenschutzrichtlinie (RL 95/46/EG) in nationales Recht zu übernehmen und umzusetzen, nicht korrekt nachgekommen ist. Daher sahen wir uns befugt, Stellung zu einer Datenbekanntgabe zwischen Behörden zu nehmen. Wir führten dabei aus, dass *im Rahmen der Amtshilfe das Verhältnismässigkeitsprinzip zu berücksichtigen ist:* es sind jeweils nur jene Daten zu übermitteln, die zur Erfüllung einer vom Gesetz umschriebenen Aufgabe notwendig und erforderlich sind.

In einem anderen Verfahren wurden wir gebeten, eine Stellungnahme zur Frage abzugeben, **ob das Auskunftsrecht nach Art. 11 DSG auch die Abgabe einer Negativmeldung umfasst**. Das Auskunftsrecht – und dazu gehört auch die Abgabe einer Negativmeldung – ist ein Eckpfeiler des Datenschutzes. Nur wer feststellen kann, ob und wer welche Personendaten einer betroffenen Person bearbeitet, kann überhaupt Rechte, gestützt auf das DSG, wahrnehmen. Sofern kein Gesetz die Auskunftserteilung verbietet, oder wenn eigene oder die Interessen eines Dritten überwiegen und die Daten nicht an Dritte bekanntgegeben werden, muss ein Inhaber einer Datensammlung einer betroffenen Person auch darüber Auskunft geben, ob er über sie Daten bearbeitet.

## 2.4 Auslandsdatentransfer und Empfehlungen bei Auslandsdatentransfer

Auch im vergangenen Jahr standen im Zusammenhang mit grenzüberschreitendem Datentransfer vor allem Fragen zu **Standardvertragsklauseln**, zu unternehmensinternen verbindlichen Datenschutzregelungen (**Binding Corporate Rules, BCR**) sowie zum **Outsourcing** im Vordergrund.[23] Insbesondere die Entwicklung, Datenbearbeitungen oder IT-Serviceleistungen aus Kosten- oder Effizienzgründen in Drittstaaten, wie z. B. Indien, vornehmen zu lassen, bedingt die *vorherige Klärung diverser datenschutzrechtlicher Erfordernisse*. Festzustellen ist, dass sich die Verwendung von Standardvertragsklauseln, obwohl sinnvoll und einfach in der Verwendung, nach wie vor nicht durchsetzt. Bei uns ging nur eine einzige diesbezügliche Meldung ein.

## 2.5 Projektbegleitung

Das Landesspital modernisiert derzeit die vorhandene IT-Infrastruktur und wird zukünftig für die Bearbeitung von Patientendaten vermehrt elektronische Systeme nutzen, z. B. das **Klinik-Informationssystem** (KIS), das Radiologie-Informationssystem (RIS) oder das Labor-Informationssystem (LIS). Es sollen insbesondere die interne Verwaltung verein-

ropa.eu/juris/document/document.jsf?docid=79001&doclang=DE.

21 Die Stellungnahmen sind zum Teil abrufbar unter http://www.llv.li/ unter Stabsstelle Regierungskanzlei (SRK), Externe Stellungnahmen zu Berichten und Anträgen und zu Vernehmlassungsberichten.

22 Art. 2 Abs. 3 DSG.

23 Siehe Tätigkeitsbericht 2008, Pkt. 2.3 zu Binding Corporate Rules, Tätigkeitsbericht 2010, Pkt. 1.10 zu Standardvertragsklauseln, Tätigkeitsbericht 2011, Pkt. 1.10 zu Mustervorlagen von Geheimhaltungsvereinbarungen oder Tätigkeitsbericht 2012, Pkt. 1.9.

facht und die Datenflüsse vereinheitlicht und klar geregelt werden. Die in einem Spital bearbeiteten Patienten- und Gesundheitsdaten sind besonders sensibel. Durch eine automatisierte Datenbearbeitung eröffnen sich spezifische Risiken, denen mit angemessenen technischen und organisatorischen Massnahmen begegnet werden muss. Bei mehreren Treffen konnten wir entsprechende Anregungen geben und Möglichkeiten für eine datenschutzkonforme Ausgestaltung aufzeigen. Dabei verwiesen wir unter anderem auf ein Dokument von privatim:[24] «Datenschutztechnische Anforderungen an ein Klinikinformationssystem (KIS)».[25] In diesem Dokument werden insbesondere die Rechte der Betroffenen, die Einführung eines Berechtigungskonzepts, die Anforderungen an Schnittstellen nach aussen und innen sowie die Protokollierung zur Prüfung der datenschutzkonformen Nutzung adressiert.

Zwischen Österreich und Liechtenstein wurde ein **Abkommen über die Zusammenarbeit im Bereich Steuern** geschlossen. Damit werden unter anderem in Liechtenstein ansässige sogenannte Zahlstellen (z. B. Banken und Wertpapierhändler sowie andere, die im Rahmen ihrer Geschäftstätigkeit regelmässig Vermögenswerte von Dritten entgegennehmen, halten, anlegen usw.) unter bestimmten Voraussetzungen verpflichtet, Kundendaten mit entsprechenden Vermögenswerten nach Österreich zu melden.[26] Die Steuerverwaltung (STV) wurde mit der Umsetzung betraut und gibt hier das Verfahren vor.[27] Sie suchte bereits in einem sehr frühen Projektstadium das Gespräch mit uns. Dadurch konnten wir positiv im Sinne einer die Privatsphäre der Betroffenen schützenden Weise mitarbeiten. Wichtig für uns war unter anderem, dass jegliche Datenübermittlung gesichert erfolgt und die Datensicherheit eingehalten wird. Zahlstellen verwenden für deren Meldung an die STV bestehende eGovernment-Strukturen und elektronische Formulare, was die Datensicherheit gewährleistet. Die STV ihrerseits überträgt die im Abkommen festgelegten Daten nach Österreich, wobei neben einer verschlüsselten Übertragung zusätzlich eine Verschlüsselung der zu übertragenden Daten selbst erfolgt. Wir begrüssen die frühe Kontaktaufnahme der STV und die konstruktive Zusammenarbeit. Mit der frühzeitigen Berücksichtigung des Datenschutzes kann kostspieligen Korrekturmassnahmen vorgebeugt werden.

Im **Zentralen Personenregister (ZPR)**, der zentral geführten Datenbank der Landesverwaltung, werden unter anderem sämtliche Adressen der Einwohner Liechtensteins gespeichert.[28] Zusätzlich pflegen sämtliche Gemeinden (Einwohnerkontrollen) ihre eigenen unabhängigen Systeme mit Meldedaten. Bei Wohnsitzwechsel werden laufend Adressdaten zwischen den Gemeinden untereinander und zwischen den Gemeinden und der Landesverwaltung ausgetauscht; dies meist per E-Mail. Beim Empfänger müssen die Daten in weiterer Folge wieder manuell in die dortigen Systeme übernommen werden. Gemeinsam arbeiten derzeit das Land und die Gemeinden an einer technischen Lösung für den *Austausch* unter anderem von *Meldedaten zwischen* den einzelnen elektronischen *Einwohnerregistern* in den *Gemeinden und* dem *ZPR*. Im Sinne der Datensicherheit ist das Projekt zu begrüssen. Gegenüber dem Amt für Statistik (AS) hatten wir 2013 angeregt, insbesondere beim Datenaustausch mit verwaltungsexternen Stellen, wie beispielsweise Gemeinden, im Hinblick auf die Datensicherheit Alternativen zum E-Mail zu prüfen.[29] Gegenüber den Projektverantwortlichen wiesen wir insbesondere darauf hin, dass beim Datenaustausch die Verhältnismässigkeit zu beachten ist. Offen sind hier vor allem noch Fragen zu den synchronisierten Datenfeldern und zur Rechtsgrundlage.

24 Vereinigung der schweizerischen Datenschutzbeauftragten.
25 http://www.privatim.ch/de/privatim-Nachrichten/anforderungen-an-klinikinformationssysteme.html.
26 Siehe http://www.llv.li/, Steuerverwaltung, Internationales Steuerrecht, Abgeltungssteuerabkommen Österreich.
27 Vgl. Art. 24 im Gesetz zum Abkommen zwischen Liechtenstein und Österreich über die Zusammenarbeit im Bereich der Steuern.
28 Siehe Tätigkeitsbericht 2012, Pkt. 1.8, Tätigkeitsbericht 2011, Pkt. 4, Tätigkeitsbericht 2008, Pkt. 3.1, Tätigkeitsbericht 2003, Pkt. 4.1.2.
29 Siehe Tätigkeitsbericht 2013, Pkt. 4.

# 3. AUFSICHT

Mit der Einführung des Vergütungsmodells vom Typus DRG *(«Diagnosis Related Group»)* per 1. Januar 2014 werden zwischen stationären Einrichtungen im Gesundheitswesen (vor allem Spitäler) und Krankenkassen nicht mehr einzelne Leistungen oder Tagessätze, sondern Fallpauschalen abgerechnet. Jeder Spitalaufenthalt wird anhand von bestimmten Kriterien, wie Hauptdiagnose, Nebendiagnose, Behandlungen und weiteren Faktoren wie Alter, Geschlecht, Schweregrad usw., einer Fallgruppe (DRG) zugeordnet und pauschal vergütet. Für die Entgegennahme von **DRG-Rechnungen** benötigen **Krankenkassen** eine **Datenannahmestelle**. Diese muss nach Art. 14a DSG oder bei einer vom Amt für Gesundheit als gleichwertig anerkannten Stelle zertifiziert sein. Eine Übergangsbestimmung gibt den Krankenversicherern bis zum 31. Dezember 2015 Zeit, eine Datenannahmestelle einzurichten. Solange eine solche nicht eingeführt ist, dürfen Rechnungen vom Typus DRG lediglich an den vertrauensärztlichen Dienst der Krankenkasse gelangen. Wir veröffentlichten aufgrund unserer gesetzlichen Verpflichtung eine Liste der zertifizierten Datenannahmestellen der Krankenkassen auf unserer Internetseite.[30] Die beiden Krankenkassen Concordia und Swica liessen ihre Datenannahmestellen bereits zertifizieren und meldeten sie bei uns an. Um während der Übergangszeit den Schutz der Privatsphäre der Betroffenen zu gewährleisten, hatten wir einige Fragen zur Praxis während der Übergangsfrist an die FKB gerichtet. Aus den Antworten ergab sich für uns kein unmittelbarer Handlungsbedarf. Nach Ablauf der Übergangsfrist werden wir das Thema weiter verfolgen und unter Umständen wieder auf die Krankenkassen zugehen. Im Bereich der DRG-Abrechnungen gibt es zwei Seiten: einerseits die Krankenkassen als Empfänger der Rechnungen und andererseits das Landesspital. Dieses versendet derzeit ihre Rechnungen zwar nach dem Typus DRG, diese enthalten jedoch nur sehr eingeschränkt medizinische Daten, jedenfalls keine Diagnosen und Prozeduren. Auf allfällige Rückfragen hin versendet das Landesspital die gewünschten Informationen an den vertrauensärztlichen Dienst der Krankenkasse.

Im Vorjahr hatten wir **bei drei Telekom-Providern Kontrollen zur Bearbeitung von Vorratsdaten** durchgeführt. Hier waren Nachkontrollen zu gewissen Teilaspekten erforderlich. Insbesondere hatten nicht alle Provider rechtskonforme Löschprozesse implementiert.[31] Bei den Nachkontrollen stellten wir fest, dass die notwendigen Prozesse zur Umsetzung der Löschempfehlungen mittlerweile in die Wege geleitet, jedoch nicht in allen Fällen vollständig umgesetzt sind. Organisatorisch wird zwischenzeitlich sichergestellt, dass *Vorratsdaten, welche älter als sechs Monate sind, unverzüglich einem Löschprozess zugeführt werden*. Die betreffenden Provider haben uns unaufgefordert zu informieren, sobald den noch offenen Empfehlungen nachgekommen wurde.

Beim **Amt für Statistik (AS)** hatten wir 2013 den Datenaustausch mit Institutionen und Personen ausserhalb der Landesverwaltung auf ihre Datenschutzkonformität hin überprüft.[32] Verbesserungsbedarf ergab sich insbesondere aufgrund der unterschiedlichen technischen Systeme und Möglichkeiten der Kommunikationspartner. Zwischenzeitlich wurde auf der Internetseite des AS ein Formular online gestellt, mit welchem Daten ohne grossen Aufwand für die Datenlieferanten sicher übermittelt werden können.[33] Das AS weist sämtliche Datenlieferanten auf diese Möglichkeit der sicheren Datenübermittlung hin. Weitere Projekte zur Optimierung der Datenflüsse bei externen Stellen mit regelmässigem Datenaustausch laufen.[34] Erklärtes Ziel des AS ist es, den verwaltungsexternen Stellen auch weiterhin einen unkomplizierten, aber dennoch datenschutzkonformen Datenaustausch anbieten zu können. Mit der Einführung der genannten Formulare und der verschlüsselten Datenübermittlung konnte ohne wesentliche Einschränkungen für das Tagesgeschäft die Datensicherheit verbessert werden.

Beim **Ausländer- und Passamt (APA)** überprüften wir die Praxis in Bezug auf die Datenbearbeitung im *Schengener Informationssystem (SIS)*. Das APA ist unter anderem für die Ausschreibung von Drittstaatsangehörigen zur Einreiseverweigerung zuständig. Zur Erfüllung dieser Aufgabe hat das APA Zugriff auf Daten im SIS. Sämtliche Abfragen sind dabei vollständig und revisionsgerecht zu protokollieren.[35] Mit der gegenständlichen Kontrolle wurde die *inhaltliche Ausgestaltung der Protokollierung*

30 Internetseite der Datenschutzstelle (www.dss.llv.li) unter DRG Datenannahmestellen.

31 Siehe Tätigkeitsbericht 2013, Pkt. 4.
32 Siehe Tätigkeitsbericht 2013, Pkt. 4.
33 https://formulare.llv.li/formserver_AS/start.do?generalid=AS_SUE.
34 Siehe unter 2.5.
35 Art. 51 N-SIS-V iVm Art. 11 DSV.

und stichprobenartig der jeweilige *Grund sowie die Rechtmässigkeit einzelner Abfragen* durch die APA-Mitarbeiter geprüft. Bei der Kontrolle konnte in einigen Punkten Verbesserungspotenzial herausgearbeitet werden. Eine Empfehlung betraf beispielsweise die Aktualisierung vorhandener Leitfäden und Reglemente, da mit dem SIS II im Jahr 2013 neue Rechtsvorschriften in Kraft getreten sind.[36] Auch ergab sich Nachbesserungsbedarf bei der Protokollierung selbst.

# 4. INFORMATION UND SENSIBILISIERUNG DER ÖFFENTLICHKEIT

Nach wie vor ist für uns die Sensibilisierung der Öffentlichkeit für den Schutz der Privatsphäre eine zentrale Aufgabe. Dies insbesondere, weil die im Jahr 2012 durchgeführte repräsentative Umfrage zum Datenschutz in Liechtenstein gezeigt hatte, dass die Befragten nur wenig über das Thema wissen.[37]

Die Privatsphäre ist in der von digitalen Medien bestimmten Informationsgesellschaft besonders gefährdet. Dies gilt in besonderem Ausmass für **Kinder und Jugendliche.** Die Artikel-29-Datenschutzgruppe betont in einer Stellungnahme, dass Aufklärung und Verantwortung wichtige Instrumente für den Schutz der Daten von Kindern (und Jugendlichen) darstellen.[38] Diese Überzeugung teilen wir und deshalb haben wir die Sensibilisierung der Jugendlichen als Schwerpunktthema definiert. Dies umso mehr, als dass es Soziale Medien und moderne technische Spielereien gerade darauf abgesehen haben, die Nutzer zur – teilweise kompromittierenden – Selbstdarstellung anzuregen. Vor diesem Hintergrund nahmen wir an verschiedenen Veranstaltungen zum Thema teil und hatten entweder bei Multiplikatoren oder auch bei den betroffenen Jugendlichen selbst die Möglichkeit, *auf Gefahren für die Privatsphäre hinzuweisen*. So hielten wir im Zuge eines Elternabends einen Vortrag. Inhaltlich orientierten wir uns an folgenden Fragen: 1. Wer sammelt Daten? 2. Warum werden Daten gesammelt? 3. Worin besteht eigentlich das Problem? Weiter gestalteten wird unter der Leitung der Schulsozialarbeit einen Nachmittag beim freiwilligen 10. Schuljahr zum Thema Medienkompetenz. In der Projektwoche am Liechtensteinischen Gymnasium hielten wir einen Vortrag zum selben Thema. Wie schon vergangenes Jahr wurden wir wieder von einer Bank eingeladen, um deren Lernende des 1. und 2. Lehrjahrs für das Thema Privatsphäre zu sensibilisieren. Gemeinsam mit dem Amt für Soziale Dienste (Kinder- und Jugendschutz) gestalteten wir bei der Erwachsenenbildung Stein Egerta Ende des Jahres einen Kurs mit dem Titel «Erziehung: Internet, Smartphone & Co. Wie begleite ich mein Kind auf dem Weg ins Internet?». Auffallend war die grosse Nachfrage von Eltern nach konkreten Werkzeugen und Hilfsmitteln für deren Kinder.

Die **Kernaussagen dieser Veranstaltungen** auf den Punkt gebracht: 1. Technik und moderne Kommunikationsmedien nicht verteufeln; vielmehr die Gefahren aber auch Chancen (er)kennen lernen. 2. Sei zurückhaltend in der Bekanntgabe von Personendaten; im Zweifel nein. 3. Erst lesen/denken, dann schreiben/klicken. 4. Respektiere die Privatsphäre der anderen. 5. Trenne Beruf und Freizeit. Die private Nutzung – sowohl die Auswahl der Dienste als auch die Art der Nutzung – ist nicht in allen Fällen mit dem beruflichen Umfeld vereinbar. 6. Das Internet ist nicht kostenlos. Personendaten sind der Rohstoff der Informationsgesellschaft.

## 4.1 Veranstaltungen

Anlässlich des **8. Europäischen Datenschutztages** am 28. Januar organisierten wir wieder eine Veranstaltung an der Universität Liechtenstein. Der Vortragsabend fand unter dem Motto **«Wie gesund ist Big Data? – Chancen und Risiken von Datensammlungen im Gesundheitswesen»** statt. In diesem Zusammenhang stellten wir auch unsere Richtlinie zu Big Data vor.[39]

**Big Data** steht für einen neuen Trend. Im Grunde genommen geht es um eine Fortentwicklung von Data Mining, Data Warehousing und Ähnlichem.

36 Siehe Tätigkeitsbericht 2013, Pkt. 5.2.
37 Siehe Tätigkeitsbericht 2012, Pkt. 2.1.
38 Artikel-29-Datenschutzgruppe, Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen), angenommen am 11.02.2009 (WP 160).
39 http://www.llv.li/files/dss/pdf-llv-dss-richtlinie-big-data.pdf.

Der Grundtenor ist: Aus allen möglichen Quellen werden Daten gesammelt. In vielen Fällen wird erst im Nachhinein festgelegt, zu welchem Zweck dies geschieht. Durch die gezielte Analyse und Auswertung eines Datenbestands ergeben sich neue Möglichkeiten, die Chancen wie auch Risiken beinhalten. Ein spezielles Risiko besteht darin, dass anonymisierte Daten durch Verknüpfungen mit Daten aus anderweitigen Datenquellen *de-anonymisiert* werden. Dies stellt speziell für (amtliche) Statistiken eine Gefahr dar. Dieses Phänomen ist auch stark mit der Verhaltensforschung im Rahmen von Werbung verbunden. Basierend auf Algorithmen werden Personen in Kategorien eingeteilt und das System erwartet, dass man sich dementsprechend verhält. So soll z. B. Amazon ein Patent dafür bekommen haben, das vorausschauend für den Kunden denkt und vor ihm wissen soll, was er bestellen wird. Damit soll sich Amazon Zeit sparen und Waren können schneller dem Kunden zugestellt werden. An unserer Veranstaltung wurde das Phänomen Big Data vorgestellt und im Rahmen von Entwicklungen im Gesundheitswesen diskutiert.

Neben dem Datenschutztag waren wir dieses Jahr wieder an der **LIHGA** präsent. Als eine kleine Amtsstelle suchten wir auch dieses Mal wieder die Zusammenarbeit mit Kooperationspartnern und konnten unter dem Dach des *Vereins Sicheres Liechtenstein* zusammen mit dem *IT Crowd Club Liechtenstein* und dem Verein *aha – Jugendinformation Liechtenstein* sehr gute Partner gewinnen. Hauptthema war die *Sicherheit im Internet*. Dabei sollten alle Altersgruppen angesprochen werden. Die Entwicklungen sind nach wie vor rasant: Während Smartphones vor wenigen Jahren noch gar kein grosses Thema waren, sind sie heute weit verbreitet und kaum mehr wegzudenken. Deshalb informierten wir speziell über die Themen Smartphones, Apps und die Benützung von WLAN-Netzen. Gerade bei Reisen ins Ausland benützt man oft fremde WLAN-Netze. Wir zeigten auf, dass auch ein geschlossenes WLAN-Netz nicht sicher ist, wenn z. B. alle Hotelgäste dasselbe Passwort benützen. Anhand eines einfachen Versuchsaufbaus demonstrierten wir – mit dem Einverständnis der Nutzer – wie leicht Datenflüsse zwischen einem Smartphone und dem Internet in einem offenen WLAN-Netz eingesehen werden können. Die gesurften Bilder stellten wir dazu auf einem Monitor dar. Weiter informierten wir zu Themen betreffend den Selbstdatenschutz und, wie schon das letzte Mal, sichere Passwörter. Wie bereits an der letzten LIHGA zeigte sich auch diesmal, dass das Gespräch mit Betroffenen wichtig ist. Es konnten viele Eindrücke gesammelt und Erfahrungen ausgetauscht werden. Die Informationen stellten wir in einem Faltblatt zusammen, das von unserer Internetseite heruntergeladen werden kann.[40]

In der Computeria des Seniorenbunds Liechtenstein sensibilisierten wir interessierte **Seniorinnen und Senioren zum Thema Soziale Netzwerke**. Wir unterstützen solche Anfragen gerne. Denn neben der oft zitierten Notwendigkeit der Sensibilisierung Jugendlicher sollten auch andere Altersgruppen berücksichtigt werden.

Dieses Jahr fand bereits zum vierten Mal ein Treffen im Sinne eines **Erfahrungsaustauschs mit den Datenschutzverantwortlichen** von Behörden einerseits und von Unternehmen anderseits statt. Der Datenschutzverantwortliche als Garant für die Einhaltung des Datenschutzgesetzes innerhalb eines Betriebs oder einer Behörde ist die *erste Anlaufstelle bei datenschutzrechtlichen Fragen*. Der jährlich stattfindende Austausch mit den Datenschutzverantwortlichen ist daher sehr wichtig und dient unter anderem dazu, Synergien zu schaffen und den persönlichen Kontakt zu pflegen. Dieses Jahr wurde in einem Gastvortrag aufgezeigt, wie der Datenschutz in einem grossen Industrieunternehmen gelebt wird. Auf Anfrage führten wir ferner eine Einführungsveranstaltung für Datenschutzverantwortliche durch.

## 4.2 Veröffentlichungen in den Medien

Facebook kaufte im vergangenen Jahr den Instant Messenger WhatsApp. Die Datenbearbeitung von Facebook ist in der Vergangenheit mehrfach stark kritisiert worden.[41] Dass sich durch den Kauf für die Nutzer von WhatsApp nichts ändern wird, ist wohl illusorisch. Der Kaufpreis von 19 Milliarden Dollar verdeutlicht einmal mehr den monetären Wert von Personendaten. Diese gelten als *das neue Öl, das neue Gold der Informationsgesellschaft.* Alternativen sind gefragt. Warum keine Lösung aus Liechtenstein mit der Datenbearbeitung im Land? Es wäre ein Zeichen für den **Datenstandort Liechtenstein** und ein Zeichen des Vertrauens für mögliche Nutzer. Dadurch könnte ein wirtschaftlicher Mehrwert geschaffen und die Privatsphäre der Betroffenen geschützt werden.[42]

In einem Magazin veröffentlichten wir einen Beitrag zu **Datensicherungen**. Datensicherungen sind eine

40 http://www.llv.li/files/dss/pdf-llv-dss-merkblatt_lihga_DSS.pdf.
41 Siehe Tätigkeitsbericht 2011, Pkt. 1.2, sowie Tätigkeitsbericht 2012, Pkt. 1.8 und Pkt. 5.1.
42 «Datenschutzbeauftragter schlägt heimische WhatsApp-Alternative vor», Liechtensteiner Volksblatt, 27.02.2014, S. 7.

Massnahme zur Vorbeugung von Datenverlust und zentraler Bestandteil jeder Datenbearbeitung. Dazu gehört auch die örtlich getrennte Aufbewahrung. Doch gerade eine solche örtliche Trennung, beispielsweise bei einem Hoster im Internet, verlangt angemessene Sicherheitsmassnahmen. Es gibt bereits zahlreiche Anbieter im Internet, die entsprechende Dienstleistungen günstig oder gar gratis anbieten, wobei sich speziell bei amerikanischen Anbietern Datenschutzfragen stellen, die nicht in allen Fällen einfach zu beantworten sind.[43] Wir setzen uns für den Datenstandort Liechtenstein ein. Damit ansässige Hoster und datenbearbeitende Unternehmen nach aussen klar sichtbar machen können, dass das Thema Datenschutz innerhalb ihrer Organisation und im Umgang mit den Kunden einen hohen Stellenwert geniesst, besteht die Möglichkeit des Erwerbs einer *Datenschutzzertifizierung*.[44] Gerade im Zusammenhang mit der Wettbewerbsfähigkeit ist für Dienstleister und Hoster im Internet die Berücksichtigung der Privatsphäre der betroffenen Personen ein kritischer Erfolgsfaktor und gegenüber Kunden und Geschäftspartnern stellt das landesspezifische Gütesiegel ein wichtiges, Vertrauen schaffendes Argument dar.

In einem weiteren Beitrag beschäftigten wir uns mit der Frage: **«Wie sieht die digitale Zukunft aus?»** Geht der Trend wirklich in Richtung «Ich habe doch nichts zu verbergen?» oder gibt es Gegenbewegungen? Die Entwicklungen der Technologie der letzten Jahre sind so rasant, dass eine Beurteilung der Zukunft schwerfällt. Die Grundsatzrichtung scheint aber klar zu sein: Es wird immer mehr vernetzt und elektronisch bearbeitet, *Richtung mobile Kommunikation,* vom e-Commerce zum m-Commerce. Daten fallen nicht nur immer öfter an; viele Geräte beginnen, miteinander zu kommunizieren: Das *«Internet der Dinge»* steht vor der Tür. Zur zunehmenden Vernetzung kommt, dass jeder Nutzer selbst zum «Small Brother» wird, Stichwort Mikro-Drohnen und Dashcams. Diese Entwicklungen gefährden das Recht auf das eigene Bild, wie es zum Beispiel das Schweizerische Bundesgericht im Fall «Google Street View» definiert hat. Nicht alles, was möglich ist, wird erlaubt sein. Gewisse Grenzen sind zu ziehen. Hier ist der Gesetzgeber gefordert; es müssen internationale oder zumindest europäische Antworten auf diese Entwicklungen gefunden werden. Oder lösen sich einige Fragen selbst? Der Trend zu mehr Vernetzung scheint dem Höhepunkt zuzustreben. Bring Your Own Device und Konsorten können zu einer zunehmenden Belastung von Mitarbeitern führen, wenn erwartet wird, dass man ständig erreichbar ist, auch an Wochenenden. Wann soll man sich in einer solchen Situation noch erholen? Es ist wenig verwunderlich, dass Burnout auch in den letzten Jahren immer aktueller wurde. In diesem Sinn äusserte sich ein Zukunftsforscher dahingehend, dass es infolge der Erwartung der ständigen Erreichbarkeit bereits Hotels gebe, bei denen man komplett von Internet und Mobiltelefonempfang verschont werde. «Offline» sei der neue Luxus.

## 4.3 Internetseite

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

Die Kontrollen im KomG-Bereich[45] nahmen wir zum Anlass, eine neue **Rubrik «Telekommunikation»** auf unsere Internetseite zu stellen.[46] Die Rubrik zeigt in Form von häufig gestellten Fragen (FAQs) die *Grundsätze und wichtigsten Fallkonstellationen* der Datenbearbeitung im Bereich der Telekommunikation auf, definiert Begrifflichkeiten und geht auf viele praxisrelevante Fragen ein, die sich zum Teil auch aus unserer Beratungspraxis ergeben haben. Datenschutzrechtliche Aspekte im Zusammenhang mit der Marktanalyse werden ebenfalls dargestellt.[47]

Anlässlich des Europäischen Datenschutztages erstellten wir eine **Richtlinie zu Big Data**.[48] Die Richtlinie führt in die Begrifflichkeiten ein, zeigt Chancen sowie Risiken von Big Data auf und diskutiert die Vereinbarkeit mit dem Schutz der Privatsphäre. Im Zentrum steht dabei die Frage, ob und, falls ja, wie Big Data mit dem Datenschutz in Einklang gebracht werden kann. Die Privatsphäre wird durch Big Data massiv bedroht: Massgebliches Gefahrenpotenzial entsteht durch den Umstand, dass viele der im Rahmen von Big Data bearbeiteten Daten personenbezogen sind. Dies, weil sie entweder gar nicht oder nur ungenügend anonymisiert wurden. Erschwerend kommt hinzu, dass die betroffenen Personen

43 Vgl. http://www.llv.li/#/1584/cloud-computing, die Ausführungen zu Cloud Computing im Tätigkeitsbericht 2011, Pkt. 1.6, sowie Aufsatz mit dem Titel «Datenschutzrechtliche Chancen und Risiken von Cloud Computing» von Philipp Mittelberger und Gabriele Binder, in «Jus & News» 2011/2, S. 163ff.

44 Siehe unter 5.

45 Siehe Tätigkeitsbericht 2013, Pkt. 1.3.

46 http://www.llv.li/#/189/telekommunikation.

47 Siehe Internetseite des Amtes für Kommunikation unter http://www.llv.li/#/11710.

48 http://www.llv.li/files/dss/pdf-llv-dss-richtlinie-big-data.pdf.

in vielen Fällen noch nicht einmal wissen, dass ihre Daten für verschiedenste Zwecke weiter bearbeitet werden. Es wurden daher konkrete Empfehlungen erarbeitet, wie auf der einen Seite die Betreiber von Big Data eine *datenschutzkonforme Bearbeitung von Personendaten* sicherstellen können. Auf der anderen Seite finden sich auch Empfehlungen für die von Big Data betroffenen Personen, wie sie ihr *Recht auf Privatsphäre* schützen und wahren können.[49]

In einem wegweisenden **Urteil** entschied der **Europäische Gerichtshof,** dass die **Richtlinie zur Speicherung von Vorratsdaten**, die auch in Liechtenstein umgesetzt wurde, ungültig ist. Der Gerichtshof hält fest, dass aus der Gesamtheit der zu speichernden Daten sehr genaue Schlüsse auf das Privatleben der betroffenen Personen gezogen werden können, etwa *«auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren».* Bei der Prüfung, ob diese Massnahmen auf das absolut Notwendige beschränkt sind, weist der Gerichtshof darauf hin, *«dass alle Verkehrsdaten betreffend Telefonfestnetz, Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie auf Vorrat zu speichern sind»*. Damit gilt die Richtlinie für alle elektronischen und stark verbreiteten Kommunikationsmittel, die im täglichen Leben jedes Einzelnen von wachsender Bedeutung sind. Betroffen ist somit *«fast die gesamte europäische Bevölkerung»; dies «ohne irgendeine Differenzierung, Einschränkung oder Ausnahme»*. Diese Massnahmen seien von einer besonderen Schwere. Deshalb kommt der Gerichtshof zum Schluss, dass der Grundsatz der Verhältnismässigkeit missachtet wurde. Dieses Urteil ist speziell in Zeiten des NSA-Abhörskandals ein wichtiges Zeichen. Der Gerichtshof setzt damit neue Leitlinien für den Datenschutz und bestätigt seine Rolle als Hüter der Grundrechte.

Der **Europäische Gerichtshof** fällte ein weiteres **Urteil**, das wie nur wenige andere das Interesse der Öffentlichkeit weckte. Im Fall **«Google Spain SL, Google Inc.»** ging es um das Recht auf Vergessen. Ein Spanier hatte von Google Spanien die Löschung zweier Links verlangt, die bei der Suche nach seinem Namen angezeigt worden waren. Auf den angegebenen Seiten wurde auf eine Versteigerung eines Grundstücks verwiesen, die im Zusammenhang mit einer Pfändung wegen Schulden stand. Diese Informationen stammten aus dem Jahr 1998. Der EuGH beurteilte diese Information als nicht mehr relevant. Nach diesem Urteil hat jede Person in Europa das Recht, dass Google gewisse Informationen, die auf der Suchmaschine über sie aufscheinen, gelöscht werden. Google hatte auf Informationen einer Zeitung verlinkt. Die Zeitung selbst musste die Daten nicht löschen, da dies im Rahmen der Meinungs- und Pressefreiheit geschehen war. Es entstand eine breite Diskussion über die Folgen des Urteils. Dabei wurden Behauptungen aufgestellt, dies sei das Ende der Informationsfreiheit, es erleichtere Zensur, bewirke nichts für die Betroffenen usw. Die Europäische Kommission nahm hierzu Stellung und entkräftete diese Argumente eindrucksvoll.[50] Es geht – entgegen verschiedener Berichte in der Presse – nicht um eine Einschränkung der Informationsfreiheit, sondern einzig um die Frage, ob Personendaten, die über eine Suchmaschine gefunden werden können, noch relevant sind. Die Reaktionen bei betroffenen Personen liessen nicht lange auf sich warten. Google reagierte rasch und schuf ein Formular, mit dem man eine Löschung beantragen kann.[51] Damit steht den Einwohnern Europas grundsätzlich das *Recht* zu, *Verknüpfungen, die sich bei einer Suchmaschine auf sie beziehen, löschen zu lassen*. Darauf gingen Tausende von Anträgen ein. Die Beurteilung, ob eine Information für die Öffentlichkeit weiterhin wichtig ist oder eben nicht, hat der Betreiber der Suchmaschine zu beurteilen.

Die Europäische Grundrechtsagentur veröffentlichte in Zusammenarbeit mit dem Europarat zwei Untersuchungen. Das **Handbuch zum europäischen Datenschutzrecht** thematisiert die Grundsätze unter Berücksichtigung der Rechtsprechung des Europäischen Menschenrechtsgerichtshofes (EGMR) und des Europäischen Gerichtshofes (EuGH).[52] Daneben wird der Datenschutz im Polizeibereich und im Rahmen der Strafjustiz speziell behandelt und im Rahmen der Medizin oder der Statistik gestreift. In einer weiteren Untersuchung beschäftigte sich die Grundrechtsagentur mit dem **Zugang zu Rechtsbehelfen im Datenschutz**[53] und kommt unter anderem zum Schluss, dass mehr Sensibilisierung bei den Betroffenen, Anwälten und Gerichten wichtig wäre, damit die bestehenden Rechtsbehelfe wirksam sein können.

49 Siehe unter 4.1.

50 http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_rtbf_mythbusting_de.pdf.

51 Löschanträge können hier gestellt werden: https://support.google.com/legal/contact/lr_eudpa?product=websearch.

52 http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law_en.pdf.

53 http://fra.europa.eu/de/publication/2014/zugang-zu-datenschutz-rechtsbehelfen-eu-mitgliedstaaten-zusammenfassung.

# 5. WEITERE AUFGABEN

Seit 1. Juli 2009 müssen **Videoüberwachungen** im öffentlichen Bereich von uns bewilligt werden.[54] Obwohl anzunehmen ist, dass zahlreiche Videoüberwachungen im Land betrieben werden, erreichen uns nur sehr wenige Anträge. Dies hat wohl mit den mangelhaften Durchsetzungsbestimmungen im DSG zu tun. Eine Bewilligung kann für maximal fünf Jahre erteilt werden,[55] wodurch wir 2014 erstmals *Verlängerungen bestehender Videoüberwachungen* verfügt haben. Somit wird uns zukünftig die Überprüfung bestehender Videoüberwachungsanlagen regelmässig beschäftigen. Für Betreiber gilt es zu beachten, dass bei wesentlichen Änderungen unverzüglich, d. h. schon vor Ablauf der Gültigkeitsdauer, eine neue Bewilligung zu beantragen ist.

In einem Fall wurde ein Neuantrag auf Bewilligung einer schwenkbaren Videokamera im Kassenbereich eines Geschäftslokals gestellt. Da von der gegenständlichen **Videoüberwachung** auch die **Arbeitnehmer an deren Arbeitsplätzen** betroffen sind, wurde eine Ortsbesichtigung beim Betreiber gemeinsam mit dem Amt für Volkswirtschaft (Arbeitsbedingungen) durchgeführt.[56] Die ursprüngliche Ausgestaltung war weder mit dem Datenschutz noch mit den Arbeitnehmerschutzvorschriften vereinbar, wodurch sie in mehreren Punkten entsprechend angepasst werden musste. So war beispielsweise die zusätzliche Speicherung von Tonaufnahmen mit den Videobildern im gegenständlichen Fall mit dem Datenschutz unvereinbar und musste abgeschaltet werden. Weiters war die Speicherdauer auf das notwendige Mass zu reduzieren und der Aufnahmebereich war einzuschränken.[57] Zum Nachweis der Notwendigkeit wurde die *Auflage* erteilt, nach jedem Zugriff auf aufgezeichnete Videobilder den Zeitpunkt, die Bezeichnung des Ereignisses und den Grund (Zweck/Anlass) des Zugriffs sowie eine Beschreibung der betroffenen Personen (Angestellte, Kunden usw.) zu protokollieren.

Nicht nur Unternehmen, sondern auch **private Personen** haben bei **Videoüberwachungen** die **Datenschutzbestimmungen**, wie insbesondere die Geeignetheit und Notwendigkeit der Überwachung, **zu beachten** und eine mögliche Bewilligungspflicht zu prüfen. In einem Fall wurde durch einen Hausbesitzer mit einer Kamera nicht nur die eigene Grundstücksfläche, sondern auch die angrenzende öffentliche Strasse überwacht. Wir tauschten uns mit dem Betreiber mehrmals betreffend der Ausrichtung der Kamera aus. Die Kameraeinstellung wurde schliesslich derart verändert, dass der *Fokus nun auf das Privatgrundstück* sowie eine davor liegende Hecke gerichtet ist. Zudem wurde auf die Möglichkeit der *Festlegung eines Erkennungsbereichs für die Bewegungserkennung* hingewiesen. Dadurch werden Videobilder nur dann gespeichert, wenn eine Bewegung an bestimmten Bereichen auf dem Privatgrundstück erfolgt.

Am 1. Februar 2014 trat die Verordnung über die **Datenschutzzertifizierungen** in Kraft.[58] Hersteller von Datenbearbeitungssystemen oder -programmen sowie private Personen oder Behörden, die Personendaten bearbeiten, können nun ihre Produkte, Systeme, Verfahren sowie ihre Organisation einer Bewertung durch anerkannte, unabhängige Zertifizierungsstellen unterziehen und ein Datenschutzgütesiegel erwerben. Eine solche Zertifizierung generiert in vielerlei Hinsicht Mehrwert. Ein Gütesiegel zeigt, dass das Thema Datenschutz innerhalb einer Organisation und im Umgang mit deren Kunden einen hohen Stellenwert geniesst. Es gibt Rechtssicherheit in «kritischen» Bereichen der Datenbearbeitung, wie beispielsweise im Zusammenhang mit Cloud-Computing oder im Gesundheits- und Krankenversicherungsbereich. Durch das Zertifizierungsverfahren werden bestehende Datenbearbeitungsprozesse analysiert, wobei in den meisten Fällen Optimierungspotenzial entdeckt wird. Neben den genannten Aspekten schafft ein Gütesiegel Vertrauen, was die Grundlage jeder Geschäftsbeziehung ist.[59] Wir waren in Kontakt mit mehreren interessierten Unternehmen, bis Ende 2014 wurde jedoch noch kein Datenschutzgütesiegel vergeben. Hier müssen weitere Anreize geschaffen werden. Im Zusammenhang mit der Zertifizierung erarbeiteten und veröffentlichten wir auch einen **Kriterienkatalog**.[60] Dieser ist Grundlage für eine Datenschutzzertifizierung und gliedert sich in sechs Abschnitte.[61] Er

54 Siehe Tätigkeitsbericht 2009, Pkt. 1.5.
55 Art. 27 Abs. 3 DSV.
56 Siehe Tätigkeitsbericht 2010, Pkt. 1.7, sowie Merkblatt «Überwachung der Arbeitnehmer am Arbeitsplatz» unter http://www.llv.li/#/1792.
57 Vgl. dazu die Ausführungen zur Verhältnismässigkeit der Datenschutzkommission vom 7.04.2008, Az. DSK 2007/01.
58 https://www.gesetze.li/Seite1.jsp?LGBlm=2013403.
59 Details zum Verfahren sowie Fragen und Antworten auf unserer Internetseite und www.dssl.llv.li.
60 http://www.llv.li/files/dss/pdf-llv-dss-vdsz_kriterienkatalog_v1.0.pdf.
61 1. Grundsätze der Datenbearbeitung, 2. Anforderungen an die Datensicherheit, 3. Zulässigkeit der Datenbearbeitung, 4. Pflichten des Inhabers einer Datensammlung, 5. Rechte der betroffe-

ist zudem so gegliedert, dass er unabhängig von einer Datenschutzzertifizierung als Nachschlagewerk und zur Beurteilung jeglicher Datenbearbeitung verwendet werden kann.

Das **Register der Datensammlungen** nach Art. 15 DSG bezweckt die Schaffung von Transparenz, damit die Öffentlichkeit in Erfahrung bringen kann, wo Datensammlungen bestehen und wer sie bearbeitet. In das Register werden keine Einzeldaten über die Betroffenen, sondern nur summarische Angaben aufgenommen, welche einen Überblick über die gesamte Datenbearbeitung erlauben. Nähere Angaben können die Betroffenen aufgrund des gesetzlichen Auskunftsrechts beim Inhaber der Datensammlung selbst bekommen. Die *Pflicht zur Meldung der Datensammlungen* trifft die Dateninhaber.[62] Der Gesetzgeber hat die Wichtigkeit dieser Bestimmung dadurch unterstrichen, dass private Personen (das sind auch Unternehmen) die vorsätzlich ihre Datensammlungen nicht melden oder bei der Meldung falsche Angaben machen, sich strafbar machen.[63] Anmeldungen zum Register können elektronisch eingereicht werden;[64] wir können sie ohne Medienbruch direkt in das Register zur Prüfung übernehmen. Zusätzlich zur Wegleitung veröffentlichten wir Antworten zu den häufigsten Fragen auf unserer Internetseite.[65] Trotz allem kommen die Dateninhaber dieser Verpflichtung nur eingeschränkt nach.[66] Diese Praxis wurde vom Landtag bereits kritisiert.[67]

Das Gesetz über das zentrale Personenregister (ZPRG) sieht eine **ZPR-Kommission** vor, in der wir vertreten sind.[68] In der Kommission wurde weiter an der *Umsetzung der Bestimmungen im ZPRG* gearbeitet. In den Übergangsbestimmungen ist unter anderem vorgesehen, dass die Kommission zu prüfen hat, ob Behörden, die zum Zeitpunkt des Inkrafttretens dieses Gesetzes Daten bearbeiten oder abfragen dürfen, die gesetzlichen Voraussetzungen dafür erfüllen. Ist dies nicht der Fall, so hat die ZPR-Kommission der betroffenen Behörde die Datenbearbeitung oder Datenabfrage zu untersagen.[69] Dieser Punkt wurde zwar angegangen, konnte jedoch trotz der gesetzlichen Übergangsbestimmung nicht abgeschlossen werden. Immerhin wurde die Leseprotokollierung aktiviert. Hier muss in der ZPR-Kommission jedoch noch darüber beraten und entschieden werden, in welcher Form die Protokollierung zur Überprüfung der rechtmässigen Nutzung des ZPR unterstützen kann. Dies insbesondere, da die Regierung sich klar dafür ausgesprochen hat, dass eine widerrechtliche Nutzung strafbeschwert sein soll.[70] Seit dem Inkrafttreten des ZPRG konnten weitere Fortschritte in der Umsetzung der oben genannten Forderungen erzielt werden. Doch sind zahlreiche Punkte nach wie vor offen.

Die heutige Informationsgesellschaft ist stark von Medien beeinflusst. In diesem Zusammenhang taucht häufig der Begriff Medienkompetenz auf. Das Verstehen der modernen Medien ist Voraussetzung für die Fähigkeit sie anzuwenden, zu gestalten, sich auszudrücken oder auch nur zu experimentieren. Medienkompetenz ist ein Schlüsselfaktor. Bereits Ende 2012 installierte die Regierung eine Arbeitsgruppe zur Ausarbeitung eines Konzepts «Umgang mit neuen Medien», bei welcher wir aktiv mitwirkten. Die Regierung folgte dem Vorschlag der Arbeitsgruppe und schuf eine **Fachgruppe Medienkompetenz**.[71] Die Fachgruppe soll das im Land bereits bestehende, jedoch verteilte Know-how bündeln und koordinieren, um Medienkompetenz gesamtgesellschaftlich zu stärken. Wir sitzen als ständiges Mitglied in dieser Fachgruppe, wodurch wir eine weitere Möglichkeit für unsere Sensibilisierungsarbeit, gerade bei unseren Themenschwerpunkten Datensicherheit und Jugendliche, eröffnen konnten. Hier wirkten wir vor allem bei der Jahresplanung 2014/2015 mit und waren federführend an der Durchführung einer Umfrage und Auswertung der Rückmeldungen zum Thema Medienkompetenz beteiligt.

nen Personen und 6. Anforderungen an das Datenschutzmanagementsystem.

62 Siehe Tätigkeitsbericht 2010, Pkt. 5.

63 Art. 40 Abs. 2 Bst. a DSG.

64 https://formulare.llv.li/formserver_DSS/start.do?generalid=DSS_DSG_DSV.

65 http://www.llv.li/#/12346/fragen-und-antworten.

66 Siehe Tätigkeitsbericht 2012, Pkt. 6.

67 Landtagsprotokoll vom 22.05.2013 zum Tätigkeitsbericht 2012.

68 Art. 16 ZPRG; siehe Tätigkeitsbericht 2012, Pkt. 1.8.

69 Art. 21 Abs. 1 ZPRG.

70 Vgl. Abschnitt 2 zur Strafbestimmung Art. 19 ZPRG.

71 www.medienkompetenz.li.

# 6. INTERNATIONALE ZUSAMMENARBEIT

Wir verfolgten die **Datenschutzreform in Europa** weiter.[72] Das Europäische Parlament verabschiedete seine Stellungnahme im Frühling. Im Europäischen Rat konnte jedoch keine Einigung erzielt werden, sodass das ursprüngliche Ziel der Verabschiedung bis Ende 2014 nicht eingehalten werden konnte. Die Datenschutz-Grundverordnung wird direkt anwendbar sein. Der *nationale Gesetzgeber* ist damit weniger gefordert als die Behörden, die mit der Praxis zu tun haben. So müssen die zuständigen *Datenschutzbehörden Leitlinien für die Praxis ausarbeiten*, was zu einem wesentlichen Teil im künftigen Europäischen Datenschutzausschuss (als Nachfolger der Artikel-29-Datenschutzgruppe) geschehen wird. Es bestehen Tendenzen im Rat, die von der Verordnung hin in Richtung einer Richtlinie gehen. Damit wäre der *nationale Gesetzgeber* doch vermehrt gefordert. Wir werden die Reform weiter verfolgen, damit notwendige Schritte eingeleitet werden können, wenn es soweit ist.

Bekanntermassen finden im Zusammenhang mit der **Schengen-Mitgliedschaft** regelmässig **Evaluationen im Bereich Datenschutz** statt. Wir waren 2011 evaluiert worden und bestanden diese Evaluation. Dabei wurden auch verschiedene Empfehlungen ausgesprochen.[73] Der Evaluation folgte der offizielle Beitritt Liechtensteins in den Schengen-Raum. Die nächste Evaluation Liechtensteins, und damit der Datenschutzstelle, steht 2015 an. Die Evaluationen laufen so ab, dass bei den zu untersuchenden Ländern jeweils einige Datenschutzexperten gesucht werden. So auch bei der *Evaluation der Schweiz*, die im Frühjahr des Berichtsjahres stattfand. Das Datenschutzregime in Liechtenstein hat sehr vieles mit der Schweiz gemein, sowohl was die Rechtsgrundlagen als auch was die Praxis betrifft. Deshalb entschieden wir uns für eine Teilnahme bei der Evaluation der Schweiz. Dabei wurden neben dem Eidgenössischen Datenschutz- und Informationsbeauftragten (EDÖB) auch die Kantone Bern, Jura und Neuenburg jeweils in deren Zuständigkeitsbereich evaluiert. Bei einer solchen Folgeevaluation geht es unter anderem um die Umsetzung von früheren Empfehlungen, die Unabhängigkeit und Tätigkeiten der Datenschutzbehörde(n), die Umsetzung der Datenschutzrechte der betroffenen Personen und der Datensicherheit im Bereich Schengen. Es war auch möglich, sich mit der Arbeits- und der Denkweise der Experten vertraut zu machen, was einer Vorbereitung der Evaluation Liechtensteins dient.

In der Schweiz gibt es eine **Koordinationsgruppe Schengen**, die aus dem EDÖB einerseits und den kantonalen Datenschutzbeauftragten anderseits besteht. Nach Angaben auf der Internetseite des EDÖB ermöglicht diese Gruppe eine aktive Zusammenarbeit dieser Stellen unter Berücksichtigung der jeweiligen Zuständigkeiten für die Beaufsichtigung der Datenbearbeitungen, die in Anwendung der Schengen-Assoziierungsabkommen vorgenommen werden. Sie widmet sich verschiedenen Aufgaben.[74] Die Behördenpraxis in der Schweiz ist oft mit derjenigen in Liechtenstein vergleichbar, werden doch zum Teil dieselben Systeme benützt. Hier gibt es auch Parallelen zur *SIS Supervision Coordination Group (SIS SCG)*,[75] in der wir das Land vertreten. Dort werden die entsprechenden Themen aus der europäischen Sicht angegangen. Um ein vollständigeres Bild zu bekommen, wurde uns auf Anfrage der *Beobachterstatus in der Koordinationsgruppe* gewährt, was wir sehr begrüssen. Damit können Synergien geschaffen werden.

## 6.1 Artikel-29-Datenschutzgruppe

Die Entwicklung hin zu einem **automatischen Informationsaustausch im Steuerbereich (AIA)** ist vielschichtig, äusserst dynamisch und stellt den Finanzplatz vor grosse Herausforderungen. Mit wem Informationen ausgetauscht werden sollen, hängt zu einem grossen Teil von der Gewährleistung eines ausreichenden Datenschutzes des entsprechenden Partnerlandes ab. Mit dem **Common Reporting Standard** (CRS, gemeinsamer Meldestandard) hat die OECD einen globalen Standard für den automatischen Informationsaustausch über Finanzkonten vorgelegt, der auf den FATCA-Abkommen mit den USA basiert. Pikant ist, dass die FATCA-Abkommen kaum Vorschriften zum Datenschutz beinhalten. Die Artikel-29-Datenschutzgruppe wurde auf schwerwie-

72 Siehe zuletzt Tätigkeitsbericht 2013, Pkt. 5.1 und 7.
73 Tätigkeitsbericht 2011, Pkt. 1.5.
74 Austausch von Informationen, die für die wirksame Beaufsichtigung der Datenbearbeitungen notwendig sind; Prüfung der Schwierigkeiten bei der Auslegung oder Anwendung der Gesetzesbestimmungen; Untersuchung der Probleme, die sich bei den Aufsichtstätigkeiten oder der Ausübung der Rechte der betroffenen Personen ergeben können; Formulierung von harmonisierten Vorschlägen und Stellungnahmen im Hinblick auf gemeinsame Lösungen; Unterstützung und Koordinierung der Aufsichtstätigkeiten der einzelnen Mitglieder, siehe http://www.edoeb.admin.ch/dokumentation/00153/00215/00231/index.html?lang=de.
75 Siehe unter 6.3.

gende datenschutzrelevante Probleme des gemeinsamen Meldestandards, insbesondere im Lichte des EuGH-Entscheids zur Vorratsdatenspeicherung,[76] hingewiesen und hat in einem Schreiben unter anderem die OECD und die Europäische Kommission auf die kritischen Punkte aufmerksam gemacht.[77] Sowohl die OECD als auch die Europäische Kommission antworteten auf dieses Schreiben und betonten dabei die Wichtigkeit des Datenschutzes im Rahmen des automatischen Informationsaustausches (AIA) generell. Die Kommission ersuchte die Artikel-29-Datenschutzgruppe um die Schaffung von nicht-bindenden Richtlinien betreffend notwendige und ausreichende Datenschutzbestimmungen sowohl in Abkommen als auch in nationalen Umsetzungsgesetzen im Zusammenhang mit dem AIA. Wir verfolgen hier die Entwicklungen aktiv, da wir in einer von der Regierung eingesetzten Arbeitsgruppe vertreten sind. Zentrale Bedeutung hat hier das Prinzip der Zweckbindung und der Verhältnismässigkeit der Datenbearbeitung.

Die Artikel-29-Datenschutzgruppe setzte sich wenig überraschend auch mit dem **Urteil des EuGH zu Google Spain** auseinander, in dem das **Löschrecht von Personendaten im Zusammenhang mit Suchmaschinen** bestätigt wurde. Während Google der Ansicht war, dass europäisches Recht nicht anwendbar ist, urteilte der EuGH, europäisches Recht sei sehr wohl anwendbar, wenn das in Frage stehende Unternehmen eine Niederlassung in Europa hat.[78] Die Gruppe hat im Anschluss Leitlinien zur Umsetzung des Urteils erarbeitet.[79] Dabei wird festgehalten, dass das vielzitierte *«Recht auf Vergessen»* im Allgemeinen höher zu gewichten ist als die wirtschaftlichen Interessen einer Suchmaschine. Dennoch muss eine Interessensabwägung stattfinden. Betroffene müssen sich direkt an die Suchmaschinen wenden, die nicht nur Onlineformulare zur Verfügung stellen sollten. Eine wirkungsvolle Umsetzung des Urteils verlangt auch, dass dieses Recht auch bei nicht-europäischen Internetseiten umgesetzt wird (einschliesslich .com). Weigert sich eine Suchmaschine einen Löschantrag umzusetzen, kann man sich an die nationale Datenschutzbehörde wenden. Das Dokument enthält gemeinsame Kriterien für die Behandlung von Beschwerden durch die Datenschutzbehörden.[80]

Ebenso äusserte sich die Gruppe zum **Urteil des EuGH zur Vorratsdatenspeicherung**.[81] Dabei wird vor allem bestätigt, dass eine massenweise Speicherung von Daten ohne Differenzierungen, Beschränkungen oder Ausnahmen problematisch sind. Dies war der Hauptgrund, wieso der EuGH zum Ergebnis kam, dass die *Vorratsdatenspeicherung sich nicht auf das beschränkt, was «unbedingt notwendig»* ist. Ausserdem sollten nationale Gesetze einen wirksamen Schutz für betroffene Personen vorsehen. Dies vor allem, wenn es kein Erfordernis gibt, dass die Daten im EWR gespeichert werden. Auch in diesen Fällen besteht nach dem Urteil das Erfordernis einer unabhängigen Kontrolle. Aufgrund der Masse der Daten sind auch erhöhte Anforderungen an die Datensicherheit zu richten. Dieses Urteil wird wohl auch in anderen Bereichen, wie dem automatischen Austausch von Steuerdaten, zu beachten sein.

Neben grundlegenden Fragen und Beurteilungen, die der **NSA-Abhörskandal** aufgeworfen hatte, erarbeitete die Artikel-29-Datenschutzgruppe eine Stellungnahme. Anlass waren die Enthüllungen von Edward Snowden über die umfassende *Überwachung der elektronischen Kommunikation europäischer Bürger durch ausländische Geheimdienste*. Die Stellungnahme geht der Frage nach, ob und in welchem Umfang nationale Sicherheits- und Geheimdienste die elektronische Kommunikation überwachen dürfen.[82] Die Datenschutzgruppe verurteilt die geheime, massive, vorbehaltlose und willkürliche Überwachung von Telekommunikationsmitteln als *unvereinbar mit unseren Grundrechten auf Schutz der Privatsphäre*, die nicht mit dem Kampf gegen Terrorismus oder anderen nationalen Sicherheitsinteressen gerechtfertigt werden könne. Einschränkungen könnten nur dann gerechtfertigt sein, wenn die (Über-

76 Zum EuGH-Entscheid Vorratsdatenspeicherung siehe unter 4.3.

77 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140918_letter_on_oecd_common_reporting_standard.pdf.pdf. Der Anhang des Schreibens enthält die einzelnen Punkte, die zu berücksichtigen sind: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140918_annex_oecd_common_reporting_standard.pdf.pdf.

78 Siehe unter 4.3.

79 Artikel-29-Datenschutzgruppe, Guidelines on the implementation of the Court of Justice of the European Union judgment on »Google Spain and Inc v. Agencia Española de Protección de datos (AEPD) and Mario Costeja González" C131/12, angenommen am 26.11.2014 (WP 225), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

80 Siehe auch unter 4.3.

81 Artikel-29-Datenschutzgruppe, Statement on the ruling of the Court of Justice of the European Union (CJEU) which invalidates the Data Retention Directive, angenommen am 1.08.2014 (WP 220), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp220_en.pdf.

82 Artikel-29-Datenschutzgruppe, Stellungnahme 04/2014 zur Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken, angenommen am 10.04.2014 (WP 215), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_de.pdf.

wachungs-)Massnahme absolut unentbehrlich und erforderlich sei. Weder das Safe-Harbor-Abkommen noch die Standardvertragsklauseln oder verbindliche unternehmensinterne Datenschutzvereinbarungen stellen geeignete Mittel dar, um derartige, weitreichende Überwachungsmassnahmen rechtfertigen zu können. Folgende Forderungen werden gestellt: 1. Transparenz bezüglich der Überwachungsprogramme, um das Vertrauen der Bürger zu gewinnen. Dies bedingt vor allem eine Information der Bürger, wenn Geheimdiensten der Zugriff auf Personendaten gewährt wird. 2. Aussagekräftige Darstellung und Übersicht über die Aktivitäten der nationalen Geheimdienste. Die Datenschutzgruppe fordert hier die Möglichkeit zur Aufsicht über die Geheimdienste durch die nationalen Datenschutzaufsichtsbehörden. Was unter dem Begriff der Geheimdienste zu verstehen ist, müsse ebenso definiert werden wie der Umfang der derzeit geltenden Ausnahme der Geheimdienste von jeglicher Aufsicht. 3. Stärkung der Pflicht der Staaten, die Grundrechte ihrer Bürger zu schützen und zu verteidigen, insbesondere durch Implementierung von geeigneten Strafmassnahmen und Sanktionsmöglichkeiten durch die nationalen Datenschutzaufsichtsbehörden. 4. Schaffung einer internationalen Vereinbarung zum Schutz der Privatsphäre gegen Überwachungsmassnahmen von Geheimdiensten. Und 5. Forcierung der Anstrengungen, die Datenschutzreform auf europäischer Ebene voranzutreiben und abzuschliessen, wonach u. a. vorgesehen ist, dass Bürger zwingend zu informieren sind, wenn in den letzten zwölf Monaten gegenüber einer Behörde Daten bekannt gegeben wurden.

Speziell im Rahmen der Strafverfolgung heisst es immer wieder, dass gewisse staatliche Massnahmen «notwendig» seien. Dabei werden aber nicht immer einheitliche und klar definierte Kriterien für den Begriff der Notwendigkeit verwendet. Dies wollte die Datenschutzgruppe ändern und beschloss, ein **Dokument zum Begriff der Notwendigkeit im Strafverfolgungsbereich** zu erstellen.[83] Dieses Papier stützt sich im Wesentlichen auf die Rechtsprechung des Europäischen Menschenrechtsgerichtshofs (EGMR) und des Europäischen Gerichtshofs (EuGH). Es kommt dabei zu folgenden Schlussfolgerungen: Im Dokument hebt die Datenschutzgruppe insbesondere die Wichtigkeit der Notwendigkeit und der Verhältnismässigkeit in Zusammenhang mit Massnahmen im Bereich Freiheit, Sicherheit und Justiz hervor. Die Datenschutzgruppe stellt den Prüfungsprozess zu Einschränkungen des Rechts auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) des Europäischen Gerichtshofs für Menschenrechte als *Leitfaden für Gesetzgeber und Behörden* zur Verfügung. Es werden Kriterien erläutert, die bei der (Wieder-)Erwägung neuer oder bestehender Massnahmen im Bereich Freiheit, Sicherheit und Justiz beachtet werden müssen. Massnahmen müssen sich demnach immer auf eine genügende rechtliche Grundlage stützen. Massnahmen können zudem nur als notwendig erachtet werden, wenn sie einen legitimen Zweck verfolgen und für eine demokratische Gesellschaft notwendig sind. Unter dem letzten Punkt wird zudem geprüft, ob eine dringende soziale Notwendigkeit besteht, die Verhältnismässigkeit gewahrt wird und die Gründe stichhaltig und ausreichend sind.

Die Artikel-29-Datenschutzgruppe erarbeitete eine Analyse existierender **Anonymisierungstechniken**.[84] Darin werden die häufig angewendeten Techniken *«generalization»* und *«randomization»* in Bezug auf deren Effektivität und Einschränkungen analysiert. Die Stellungnahme erläutert ausführlich die «Robustheit» der einzelnen Verfahren. Dabei wird jeweils auf folgende drei Kriterien eingegangen: 1. Ist es noch möglich, einzelne Personen zu identifizieren? 2. Ist es noch möglich, verschiedene Datensätze einer Person miteinander zu verbinden? und 3. Können bestimmte Informationen zu einer Person aus anderen Informationen abgeleitet werden? Das Wissen über die Stärken und Schwächen der einzelnen Techniken soll helfen zu entscheiden, wie ein angemessener Anonymisierungsprozess in einem bestimmten Kontext zu entwerfen ist. Eine angemessene Anonymisierungstechnik berücksichtigt jedenfalls das Risiko der Re-Identifizierung und kombiniert abhängig vom Einzelfall und dem Zweck (z. B. für Veröffentlichungen) in der Regel mehrere Anonymisierungstechniken. Unsere *Richtlinie über die Anwendung der Anonymisierung und Pseudonymisierung* haben wir entsprechend angepasst.[85]

Die Artikel-29-Datenschutzgruppe veröffentlichte eine Stellungnahme zum Internet der Dinge.[86] Hin-

83 Artikel-29-Datenschutzgruppe, Stellungnahme 01/2014 zur Anwendung der Begriffe der Notwendigkeit und der Verhältnismässigkeit sowie des Datenschutzes im Bereich der Strafverfolgung, angenommen am 27.02.2014 (WP 211), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_de.pdf.

84 Artikel-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken, angenommen am 10.04.2014 (WP 216), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf.

85 http://www.llv.li/files/dss/pdf-llv-dss-richtlinie-anonymisierung-pseudonymisierung.pdf.

86 Artikel-29-Datenschutzgruppe, Opinion 8/2014 on the on Recent Developments on the Internet of Things, angenommen am 16.09.2014 (WP 223), http://ec.europa.eu/justice/data-protection/

ter dem **Internet der Dinge (IoT)** wird im weitesten Sinn eine Infrastruktur verstanden, in der Milliarden von Sensoren in alltägliche Geräte («Dinge») eingebettet sind. Die Dinge bearbeiten Informationen und kommunizieren miteinander, ohne dass ein Mensch eingreift. Sie sind darauf ausgelegt, völlig autonom und unauffällig zu kommunizieren. So lassen sich bereits Wohnhäuser mit einer Unmenge an Sensoren ausstatten. Diese messen die Temperatur innen und aussen, die Luftfeuchtigkeit und Beleuchtung in den Räumen, die Sonneneinstrahlung und noch vieles mehr. Moderne Geräte machen jedoch sehr viel mehr als nur die Temperatur zu regeln. Sie vernetzen sich mit ihrem Umfeld und tauschen sich mit anderen Dingen aus. Da die Dinge in der Regel autonom und somit ohne Zutun des Nutzers miteinander oder mit ihrem Umfeld kommunizieren, ergeben sich konkrete Fragen, die die Privatsphäre betreffen: Was wird an Daten erzeugt? Welche Daten werden weitergegeben? An wen werden diese weitergegeben? Wann werden sie gelöscht? Wie wird das sichergestellt? Wie kann eine betroffene Person dies kontrollieren? Wo kann eine betroffene Person ihre Rechte wahrnehmen? usw. *Unkontrollierte Datenflüsse* stellen dabei das grösste Risiko für Betroffene dar. Denn aus den durch die Dinge gesammelten Daten lassen sich *Nutzerprofile* erstellen, die speziell Dritte, wie beispielsweise Versicherungen, interessieren werden. Durch das Internet der Dinge entstehen auch zahlreiche neue Angriffsflächen, wobei die «klassischen» Sicherheitsmechanismen nicht einfach anwendbar sind. Es besteht hier dringender Handlungsbedarf seitens der Hersteller und Entwickler, welche die Dinge angemessen sichern müssen. Die Nutzer sind jedenfalls zu informieren (Informationspflichten) und wo notwendig, ist für die Datenbearbeitung eine Einwilligung einzuholen.

## 6.2 Europarat

Der **Konventionsausschuss** beschäftigte sich mit verschiedenen Themen. Dabei schloss er die Revision der Empfehlung (89)2 zum *Datenschutz am Arbeitsplatz* ab. Zudem verabschiedete er eine Stellungnahme zum *automatisierten Austausch von Personendaten im Steuerbereich*.[87] Dabei wurde betont, dass der Standard des Europarates, namentlich die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und die Datenschutzkonvention, auch im Rahmen von Entwicklungen bei der OECD weiterhin gelten und damit durch die Mitgliedsstaaten des Europarates zu beachten sind.

Der **Ad-hoc-Ausschuss (CAHDATA) zur Revision der Datenschutzkonvention** setzte die Arbeit fort und verabschiedete einen Schlusstext. Nun liegt es am Ministerkomitee des Europarates, den Text zu genehmigen. Dann wäre die *Datenschutzreform* im Europarat abgeschlossen. Denn im verabschiedeten Text sind einige Vorbehalte der Europäischen Kommission enthalten. Diese Vorbehalte haben mit der Revision in Brüssel zu tun, wo die Arbeit ja nicht wie beabsichtigt vorankommt. Damit dürfte auch die Revision im Europarat verzögert werden.

Im Internet hinterlässt man Spuren. Hier besteht ein wichtiger Unterschied zur Offline-Welt. So ist z. B. in einem Bücherladen in der Regel nicht einfach feststellbar, wofür sich ein einzelner Kunde interessiert hat. Im Internet ist dies dagegen üblich. Dennoch gelten dieselben Rechte, online wie offline. Zu dieser Schlussfolgerung kommt ein **Leitfaden zu Menschenrechten von Internetnutzern** des Europarates.[88] Dieser Leitfaden richtet sich direkt an den Nutzer und stellt die *Rechte* zusammen, die man bei der Nutzung des Internets hat, und wie man sie am besten nutzt. Dabei steht die Meinungsfreiheit im Vordergrund. Aber auch die Privatsphäre spielt eine Rolle. Auf die Situation von Kindern wird speziell eingegangen. Wichtig ist dabei, dass diese Rechte auch durchgesetzt werden können.

## 6.3 Weitere internationale Zusammenarbeit

Im Tätigkeitsbericht 2013 informierten wir bereits darüber, dass das SISone4All durch die zweite Generation (SIS II) abgelöst wurde. Hierzu wurde auch eine neue gesetzliche Grundlage geschaffen. Die SIS-II-Verordnung und der SIS-II-Beschluss ersetzen relevante Artikel in der Schengen-Konvention. Die Gemeinsame Kontrollinstanz Schengen hat noch unter der alten Rechtslage eine Stellungnahme zur Zulässigkeit systematischer **Datenabgleiche der Hotelmeldescheine** verfasst. Es stellt sich hier die Frage, ob diese unter den neuen gesetzlichen Bestimmungen noch gilt. Die **SIS Supervision Coordination Group (SIS SCG)** hat dies bejaht. Die Stellungnahme sieht grundsätzlich keine Zulässigkeit eines Abgleichs von Hotelmeldescheinen mit dem SIS II. Sie sieht jedoch einen gewissen Spielraum für

article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

87 http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2014)05_En_Opinion%20tax%20(final).pdf.

88 http://www.coe.int/de/web/portal/-/new-council-of-europe-guide-to-human-rights-for-internet-users.

spezialgesetzliche, nationale Regelungen vor. Solche existieren in Liechtenstein.[89] Die Landespolizei ist in der Vorbereitung, einen Abgleich von Hotelmeldescheinen mit dem SIS II technisch einzurichten. Wir bleiben in Kontakt und werden die Landespolizei bei Bedarf entsprechend beraten.

Im letztjährigen Tätigkeitsbericht berichteten wir auch darüber, dass manche **Fahndungen im SIS II** zu Problemen führen könnten.[90] Es ist zum Teil strittig, wann der Zweck einer Fahndung erfüllt und diese daher aus dem SIS II zu entfernen ist. Die Europäische Kommission versucht dies zunächst auf einer informellen Ebene zu lösen. Die SIS SCG hat zu diesem Thema eine Arbeitsgruppe gebildet, um eine rechtliche Analyse der relevanten Artikel im Zusammenhang mit *Löschungen von Fahndungen* vorzunehmen. Dies betrifft auch Liechtenstein, da momentan ein Fall aktuell ist, bei der Uneinigkeiten über die Löschung einer Fahndung im SIS II mit einer ausländischen Behörde vorliegen.

Wie im Tätigkeitsbericht 2013 ebenfalls erwähnt, tritt im Juli 2015 eine neue Eurodac-Verordnung[91] in Kraft. Aus diesem Grund hat die **EU-LISA** (Europäische Agentur für IT-Grosssysteme), welche für die Verwaltung des Eurodac-Systems verantwortlich ist, im Sommer 2014 begonnen, Anpassungen vorzunehmen. Zudem erarbeitete die **Eurodac Supervision Coordination Group (Eurodac SCG)** einen Fragebogen, der darauf abzielt, die Umsetzung der neuen Regelungen auf nationaler Ebene zu überprüfen. Resultate werden jedoch erst im Jahr 2015 diskutiert. Weitere Informationen zur Eurodac Supervision Coordination Group und EU-LISA veröffentlichten wir auf unserer Internetseite.[92]

Die **VIS Supervision Coordination Group (VIS SCG)** erarbeitete drei kurze Fragebogen und liess diese den nationalen Behörden zur Beantwortung zukommen. Es wurden Informationen zu folgenden Punkten gesammelt: Rechte der Betroffenen, Zugriff der Strafverfolgungsbehörden auf das VIS und Behörden, die Zugriff auf das VIS erhalten. Die vorläufigen Ergebnisse zeigen keine grösseren Probleme auf nationaler Ebene. Es müssen jedoch noch alle Antworten abgewartet werden, um eine umfangreiche Beurteilung vornehmen zu können.[93]

Die **Europäische Datenschutzkonferenz** beschäftigte sich mit der *Zusammenarbeit der Datenschutzbehörden*. Die technischen Entwicklungen kennen keine nationalen Grenzen. Auch die Globalisierung führt zur Notwendigkeit der Zusammenarbeit. Mit anderen Worten stellen sich oft ähnliche Fragen, deren Beantwortung koordiniert werden kann, wenn nicht gar koordiniert werden muss. Hier sind verschiedene Möglichkeiten denkbar. Sei es durch einen Meinungs- und Informationsaustausch (bilateral und multilateral), gemeinsame Kontrollen, wie sie etwa im Rahmen von SIS stattfinden, oder auch die koordinierte Inspektion der Privacy Policy von Google, die Kontrolle von Facebook durch die irische Datenschutzbehörde in Zusammenarbeit mit anderen Datenschutzbehörden. Die Zusammenarbeit ist auch sehr wichtig für die betroffene Person, damit ihre Rechte geltend gemacht werden können. Dies kann aber zu Sprachproblemen führen. Dazu kennt wohl kaum eine betroffene Person das Recht eines anderen Landes, wenn es um ein Unternehmen geht, das seinen Sitz in einem anderen Land hat.[94] Insgesamt geht es dabei auch darum, dass Ressourcen gespart werden können bzw. dass die Notwendigkeit zusätzlicher Ressourcen minimiert werden kann. Dies ist vor allem aus Sicht einer kleinen Datenschutzbehörde, wie wir dies sind, eine gute Sache.[95]

89 Verordnung vom 20.12.2011 über die Melde- und Taxpflicht bei Beherbergungen (BMTV).
90 Siehe Tätigkeitsbericht 2013, Pkt. 5.2.
91 Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26.06.2013 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).
92 http://www.llv.li/#/115433/eurodac-supervision-coordination-group und http://www.llv.li/#/115435/eulisa.
93 Siehe Tätigkeitsbericht 2013, Pkt. 5.4.
94 Zu praktischen Schwierigkeiten österreichischer Studenten vor der irischen Datenschutzbehörde: http://www.europe-v-facebook.org/DE/de.html.
95 Wir haben ja schon früher auf die Notwendigkeit der Schaffung von Synergien, nicht nur im europäischen Umfeld, hingewiesen, siehe Tätigkeitsbericht 2012, Pkt. 7.

# 7. IN EIGENER SACHE

Das Gesetz sieht vor, dass wir als Hauptaufgaben die Sensibilisierung, Beratung und auch die Aufsicht wahrnehmen. Unser Ansatz besteht darin, primär zu sensibilisieren und zu beraten. Was die Aufsicht angeht, haben wir keine Entscheidungsbefugnis. Die **Datenschutzkommission** hat eine Entscheidungsbefugnis, wird aber offenbar nicht angerufen, obwohl es sicher relevante Fälle gäbe. Somit hat die eigentlich wichtige Aufsicht in Datenschutzbelangen ein grosses Manko. Im letzten Tätigkeitsbericht hatten wir auf diese Thematik hingewiesen. Dies war im Landtag ein Thema bei der Behandlung unseres Tätigkeitsberichts.[96] In Folge dieser Diskussion signalisierten wir der Regierung unsere Bereitschaft, bei der Schaffung einer zukünftigen Lösung mitzuwirken. 2014 erhielten wir eine einzige Entscheidung der Datenschutzkommission, die jedoch aus dem Vorjahr stammt. Somit bleibt die Problematik bestehen. Es stellt sich damit auch die Frage, ob hier das Recht auf eine wirksame Beschwerde im Sinne der Europäischen Menschenrechtskonvention verwirklicht ist.

Im vergangenen Jahr hatten wir bei der Stabsstelle Regierungssekretär einen Prozess angeregt, wie Fragen des Landtages an die Regierung zu beantworten sind. Bei der letztjährigen Landtagsdiskussion wurde auch eine **Frage zu unserem Tätigkeitsbericht 2013** gestellt. Dabei ging es um sogenannte *Hilfspersonen bei Krankenkassen*. Offenbar hatten wir unseren Tätigkeitsbericht zu wenig genau formuliert bzw. war diese Thematik in Verbindung mit einer Aussage in unserem Tätigkeitsbericht 2012 zu sehen. Nach demselben Prozess beantworteten wir diese Frage zu Handen des Landtagssekretärs.

Im Rahmen der Diskussion über unseren Tätigkeitsbericht 2012 wurde im Landtag die Frage gestellt, ob es möglich ist, dass gewisse Tätigkeiten bei uns kostenpflichtig werden.[97] In der Folge der Beantwortung dieser Frage äusserten wir uns skeptisch, da es beim Datenschutz um ein wichtiges Recht immaterieller Natur geht. Wir wollten nicht zusätzliche Hürden für den Datenschutz aufbauen, zumindest was Anfragen von Einzelpersonen angeht. In Bezug auf Unternehmen sahen wir dies anders; Die Praxis hat immer wieder den Eindruck erweckt, dass Anfragen zu uns «abgeschoben» wurden. Dies auch in Fällen, in denen ein Unternehmen die Beantwortung der Anfrage berechnen konnte. Vor diesem Hintergrund waren wir für die Einführung von Kosten in gewissen Fällen. Aus dieser Möglichkeit wurde eine Pflicht. Bei der letzten Revision der DSV wurde eine **Gebühr für Stellungnahmen und Gutachten** eingeführt.[98] Wir konnten noch eine andere Einnahmequelle für einzelne **Vorträge und Schulungen** schaffen.

Wie eingangs beschrieben, soll mit dem neuen Aufbau unseres Tätigkeitsberichtes eine Art «Pulsmesser» zur Praxis des DSG geschaffen werden. Die Hauptfrage ist, ob sich das Gesetz in der Praxis bewährt. Dieser Bericht zeigt doch einige Schwachpunkte auf. Wir sind bemüht, das Ganze zu sehen und haben 2012 ja inhaltliche Schwerpunkte definiert, an denen wir festhalten wollen. Nichtsdestotrotz gilt das Gesetz nicht nur für diese Schwerpunkte. Allgemein ist auch ein Rückgang an Beschwerden festzustellen. Dafür kann es verschiedene Gründe geben, die evaluiert werden müssten. Die Anzahl der Anfragen nahm zwar auch im vergangenen Jahr zu, woraus auf ein gesteigertes Bewusstsein geschlossen werden kann. Allerdings muss auch hier gesehen werden, dass die reine Anzahl nicht ausschlaggebend sein kann. Es geht vielmehr um die Frage der Qualität und darum, ob «einfache» Fragen gestellt oder grundsätzliche Themen aufgegriffen werden. Uns fehlen oftmals Informationen zu aktuellen Entwicklungen. Dies ist eine weitere Schwachstelle. Ein weiteres Manko ist die mangelnde Praxis bei der Datenschutzkommission. Wir sind eine kleine Behörde und versuchen praxisnah zu sein. Deshalb veranstalten wir jedes Jahr die Treffen mit den Datenschutzverantwortlichen der Behörden einerseits und der Unternehmen anderseits. Das Gesetz trat 2002 in Kraft. Damals gab es zum Beispiel Facebook noch gar nicht. Die Entwicklungen in der Informationsgesellschaft sind nach wie vor rasant. Nach unserer Ansicht wäre es an der Zeit, eine **Evaluation des Datenschutzgesetzes** durchzuführen. Dabei könnte man sich am Bericht des Bundesrates in der Schweiz vom 9. Dezember 2011 orientieren.[99] Einige Elemente einer solchen Evaluation hatten wir bereits in unserem Tätigkeitsbericht 2009 festgehalten.[100] Eine solche Evaluation wäre auch hinsichtlich der laufenden Reform des Datenschutzes in Europa sinnvoll, da sie den Status quo zur Praxis aufnehmen würde und als Grundlage für die Zukunft herangezogen werden könnte.

96 Landtagsprotokoll vom 8.05.2013, S. 665ff.
97 Landtagsprotokoll vom 22.05.2012, S. 278ff.
98 Art. 33 Abs. 1 DSV.
99 http://www.admin.ch/opc/de/federal-gazette/2012/335.pdf.
100 Siehe Tätigkeitsbericht 2009, Pkt. 1.

# 8. AUSBLICK

Die Anzahl der Anfragen steigt weiterhin. Dies ist eigentlich zu begrüssen, denn damit kann aufgezeigt werden, dass der Datenschutz in Liechtenstein «lebt». Viele Anfragen werden ziemlich oberflächlich, meist telefonisch, an uns gerichtet. Der Aufwand für die Beantwortung dieser Anfragen ist gering. Auch wenn wir den Eingang von Anfragen nur wenig steuern können, werden wir uns dennoch darum bemühen, dass wir mehr in Richtung **Qualität statt Quantität** gehen. Dies gilt auch für unsere Tätigkeiten allgemein. Wir werden versuchen, mehr in die Tiefe zu gehen, und dies vor allem bei unseren Schwerpunktthemen. Einige geschilderte Themen, wie der Austausch von Steuerdaten, sind sehr komplex. Dies erfordert eine *Straffung der vorhandenen Ressourcen*. Dadurch werden andere Tätigkeiten reduziert werden müssen.

Im Rahmen der europäischen Reformarbeiten ist der sogenannte **«risk based approach»** ein wichtiges Element. Hier geht es darum, dass die Schwere des Eingriffs in die Privatsphäre ein entscheidendes Kriterium dafür darstellt, um einen Handlungsbedarf bei Unternehmen oder Behörden festzustellen. Anderseits hilft der «risk based approach» auch uns, vor allem bei der Frage, wo wir unsere *beschränkten Ressourcen noch besser einsetzen* können. Im Rahmen des Möglichen versuchen wir, Elemente der künftigen Verordnung vorwegzunehmen, damit der Umsetzungsaufwand danach geringer wird.

Der **automatische Austausch von Steuerdaten** ist ein Thema, das uns auch weiterhin begleiten wird. Hier wurde ja die Artikel-29-Datenschutzgruppe aktiv. Wir werden diese Tätigkeit aktiv begleiten und versuchen, dieses wichtige Thema voranzubringen.

Den Ausgang der **beschriebenen Rechtsmittelverfahren** werden wir mit Interesse verfolgen.

Ebenso werden wir die nun schon seit drei Jahren laufende **Datenschutzreform in Brüssel** verfolgen. Es bestehen Anzeichen dafür, dass sie bis Ende 2015 abgeschlossen sein wird. Wie erwähnt wird die *Grundverordnung* Spielraum für den nationalen Gesetzgeber enthalten. Die gleichzeitig in Vorbereitung stehende *Richtlinie im Polizeibereich* wird völlig durch den Gesetzgeber umzusetzen sein. Wir werden den Kontakt zur Regierung suchen.

Die **Datenübermittlung über sichere Verbindungen** soll zukünftig ein Schwerpunkt unserer Sensibilisierungsarbeit darstellen. Dabei wollen wir insbesondere auf die *Gefahren im Zusammenhang mit der unverschlüsselten Kommunikation* hinweisen. Dies vor allem im Gesundheitsbereich, wo zahlreiche Datenübermittlungen zwischen den beteiligten Stellen wie Leistungserbringer, Landesspital, Krankenkasse, Patient usw. existieren.

An der Universität Liechtenstein werden wir im Zuge des **Zertifikatlehrgangs «Compliance Officer»** den Teilnehmenden die Begrifflichkeiten und wesentlichen Aspekte des Datenschutzes näher bringen. Neben den rechtlichen Grundlagen werden wir speziell auf die IT-spezifischen Themenfelder eingehen. Der Lehrgang richtet sich an Compliance-Beauftragte aus den verschiedensten Bereichen (Banken, Versicherungen, Instustrie usw.). Durch diese *Kooperation mit der Universität* ergibt sich für uns eine günstige Gelegenheit, eine ausführliche Schulung mit aktuellen Entwicklungen vorzubereiten.

Im kommenden Jahr steht eine erneute **Schengen-Evaluation** bevor. Die letzte im Jahr 2011 bestanden wir erfolgreich; es wurden dennoch einzelne Empfehlungen ausgesprochen. An der kommenden Evaluation geht es erfahrungsgemäss vorwiegend um die *Frage, wie diese Empfehlungen umgesetzt wurden.* Dazu können auch völlig neue Aspekte aufgegriffen werden. Zur Vorbereitung dieser Evaluation gehört, dass wir an einer Evaluation eines anderen Landes, die vorher stattfinden wird, teilnehmen werden.

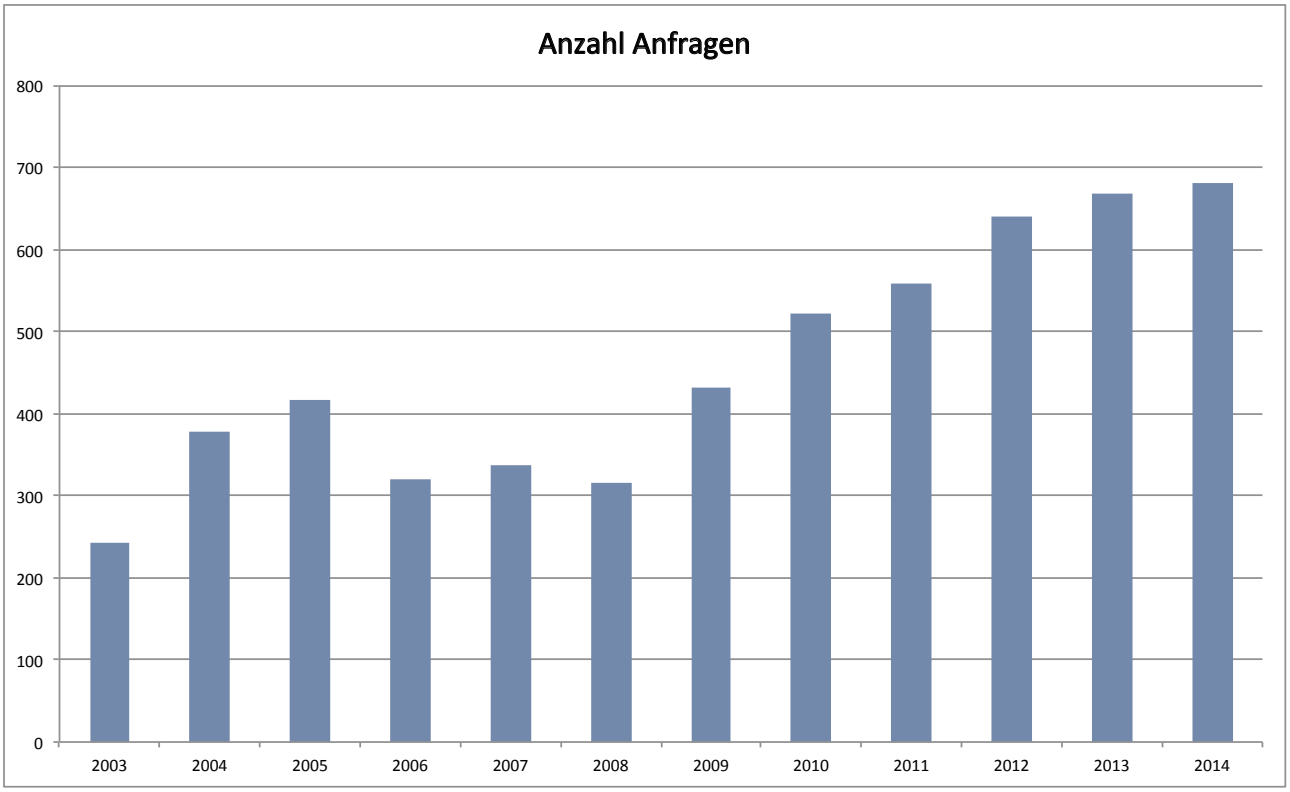
# 9. ANHANG

## 9.1 Anfragestatistik

Die Beratung privater Personen und Behörden ist eine Kernaufgabe. Im Berichtsjahr erhielten wir insgesamt 682 Anfragen. Gegenüber dem Vorjahr bedeutet das eine Zunahme um 13 Anfragen.

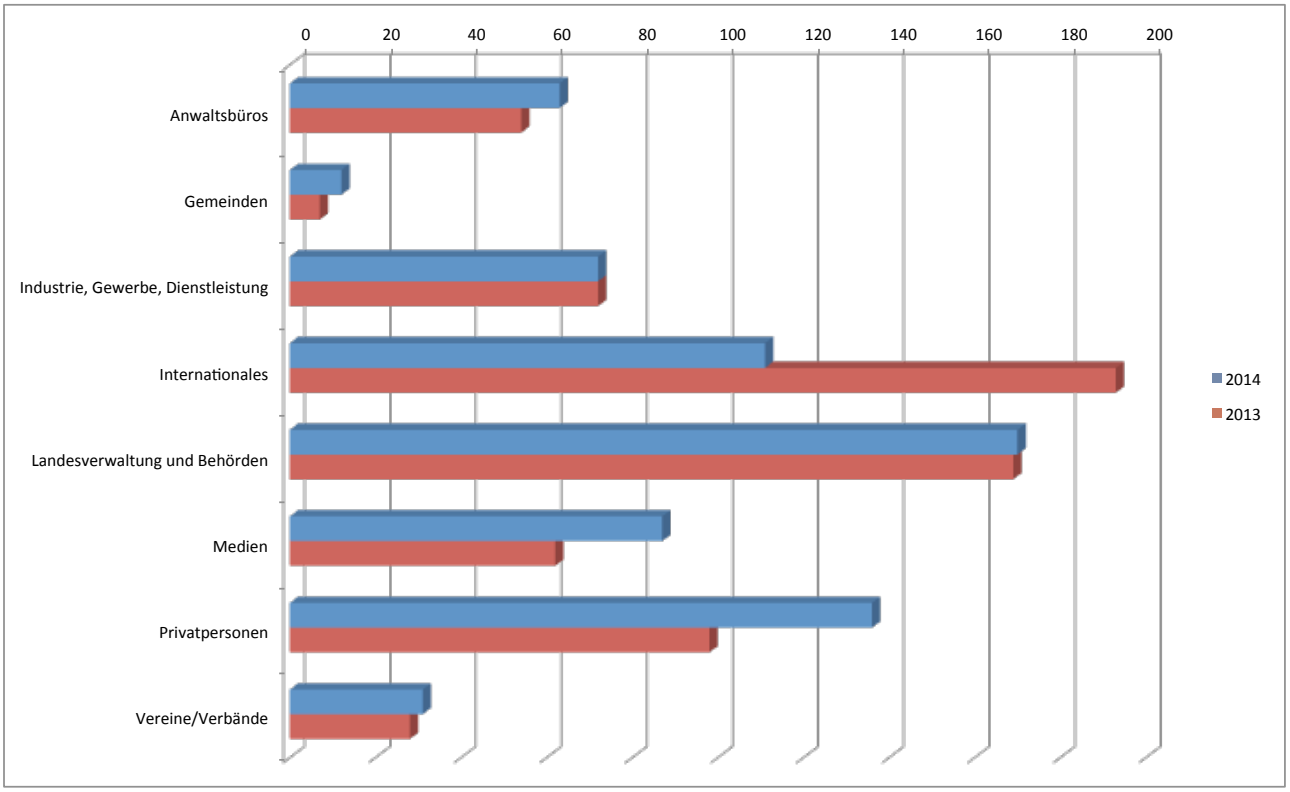
### Anzahl Anfragen im Vergleich zu den Vorjahren

Die nachfolgende Abbildung zeigt die Entwicklung der Anzahl Anfragen über die vergangenen 12 Jahre:



## Anzahl Anfragen pro Personengruppe

In der folgenden Abbildung ist ersichtlich, von welchen Personengruppen bzw. Organisationen die Anfragen eingegangen sind:

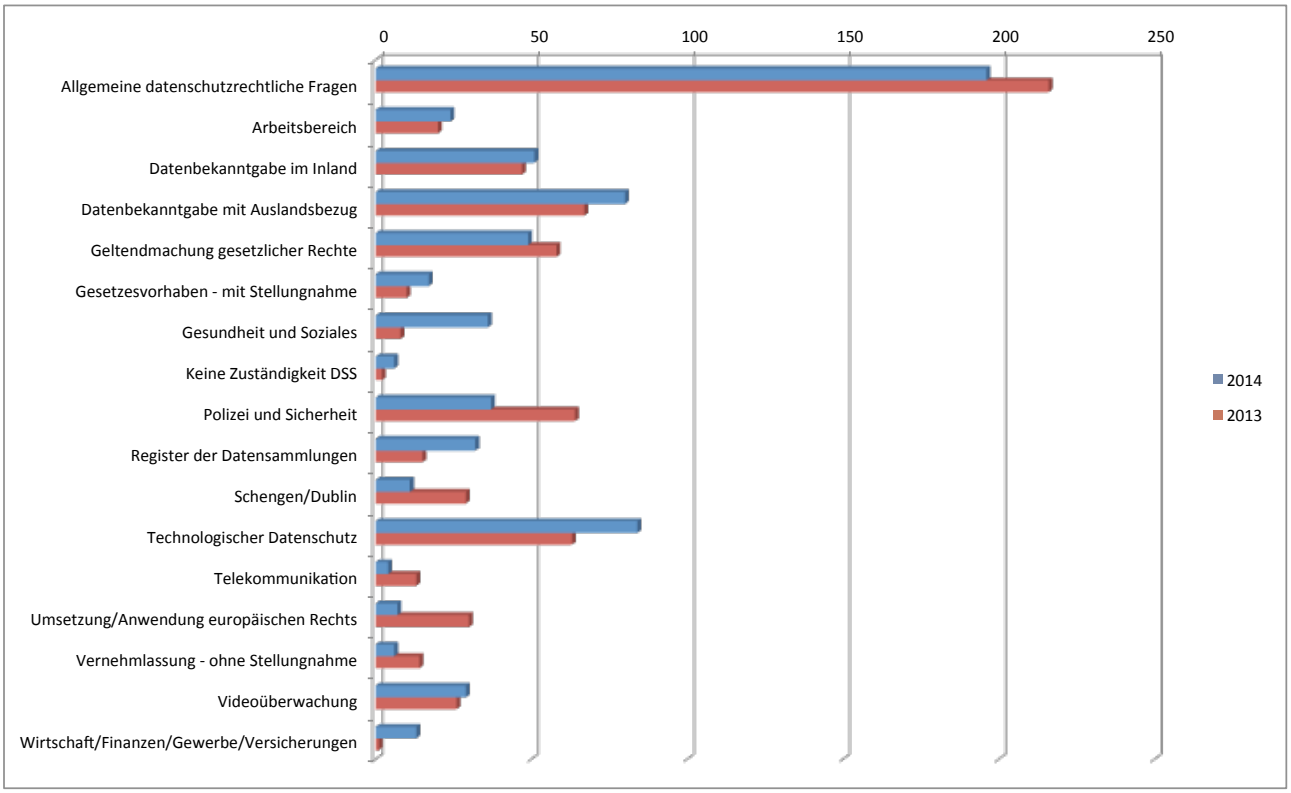



Die meisten Anfragen stammen (abgesehen von einem einmaligen Effekt im 2013) nach wie vor von der Landesverwaltung. Von den Gemeinden gingen fast doppelt so viele Anfragen ein. Diese betrafen vor allem Datenbekanntgaben im Inland, was auf eine verstärkte Sensibilität der Gemeinden bei der Bearbeitung von Personendaten hinweist. Auch bei den Anwaltsbüros spürten wir eine deutliche Zunahme. Besonders deutlich sticht die Zunahme von fast 40 % bei den Privatpersonen hervor. Hier ist zu hoffen, dass das *Bewusstsein für den Schutz der persönlichen Daten* weiter zunimmt. Allerdings steigt auch die Relevanz überproportional, bedingt durch die technische Entwicklung und die starke Zunahme von Anwendungen und Geräten und die damit zusammenhängende Anhäufung von Datenbergen.[101]

101 Siehe unter 4.2, «Wie sieht die digitale Zukunft aus?»

## Anzahl Anfragen pro Sachgebiet

Die nachfolgende Abbildung zeigt auf, um welche Themen es sich bei den Anfragen handelte:




Die meisten Anfragen sind genereller Natur. Spürbar zugenommen haben Fragen im Bereich Wirtschaft/ Finanzen/Versicherung, im Bereich Gesundheit und Soziales, im technologischen Bereich und im Zusammenhang mit Datentransfers ins Ausland.

### Anzahl Anfragen pro Personengruppe und Sachgebiet

Die folgende Tabelle gibt detailliert Auskunft über die Anfragezahlen pro Personengruppe und Sachgebiet:

| | Anwalts-büros | Gemeinden | Industrie, Gewerbe, Dienst-leistung | Inter-nationales | Landes-verwaltung, Behörden | Medien | Privat-personen | Vereine, Verbände |
|---|---|---|---|---|---|---|---|---|
| Datenschutz allgemein | 12 | | 8 | 70 | 33 | 39 | 25 | 9 |
| Arbeitsbereich | 1 | | 3 | 2 | 10 | | 8 | |
| Datenbekanntgabe Inland | 2 | 10 | 6 | | 20 | | 10 | 3 |
| Datenbekanntgabe mit Auslandsbezug | 7 | 1 | 15 | 14 | 20 | | 23 | |
| Geltendmachung gesetzlicher Rechte | 10 | 1 | 7 | | 5 | | 25 | 1 |
| Gesetzesvorhaben | | | | | 17 | | | |
| Gesundheit/Soziales | 12 | | 1 | | 14 | | 1 | 8 |
| Keine Zuständigkeit DSS | | | | | 1 | | 4 | 1 |
| Polizei/Sicherheit | | | | 25 | 3 | | 7 | 2 |
| Register der Datensammlungen | 10 | | 10 | | 6 | | 2 | 4 |
| Schengen/Dublin | 1 | | | | 10 | | | |
| Technologischer Datenschutz | | | 9 | | 13 | 43 | 17 | 2 |
| Telekommunikation | | | 3 | | 1 | | | |
| Umsetzung/ Anwendung europäischen Rechts | | | | | 5 | | 2 | |
| Vernehmlassungen ohne Stellungnahme | | | | | 6 | | | |
| Videoüberwachung | 3 | | 8 | | 1 | 5 | 12 | |
| Wirtschaft/Finanzen Gewerbe/ Versicherungen | 5 | | 2 | | 5 | | | 1 |
| Gesamtergebnis | 63 | 12 | 72 | 111 | 170 | 87 | 136 | 31 |

## 9.2 Internetzugriffsstatistik

Aufgrund der Erneuerung des Internetauftritts der Liechtensteinischen Landesverwaltung kann für das Jahr 2014 keine Internetzugriffsstatistik erstellt werden.

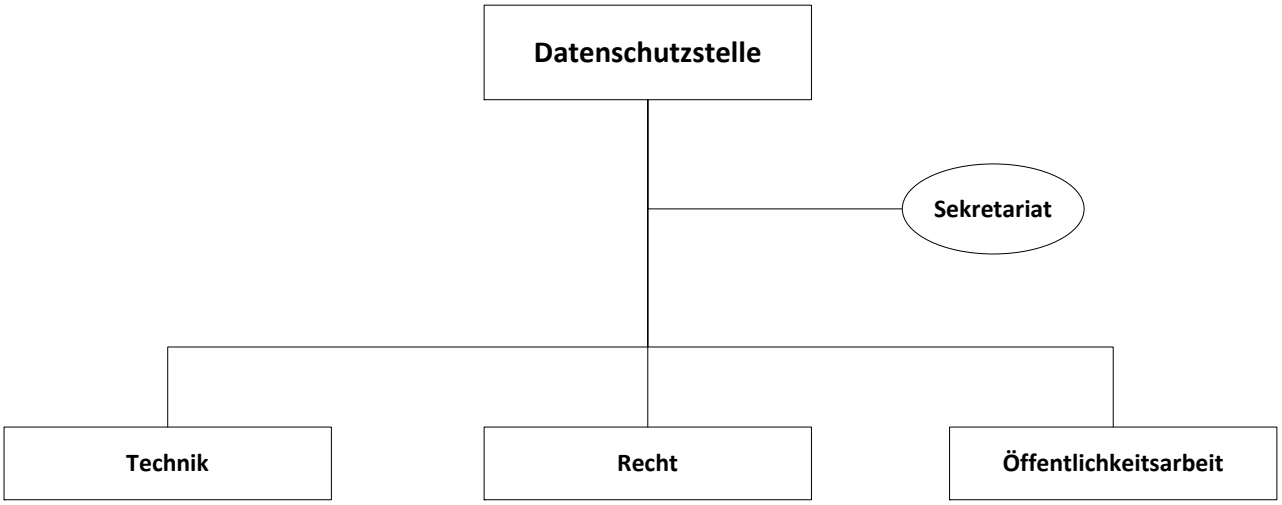
## 9.3 Veröffentlichte Publikationen

Folgende Publikationen wurden erstellt oder überarbeitet:[102]

- Richtlinie Big Data (neu erstellt)
- Richtlinie über die Rechte der betroffenen Personen bei der Bearbeitung von Personendaten (überarbeitet)
- Richtlinie über die Anwendung der Anonymisierung/Pseudonymisierung (überarbeitet)
- Empfehlung zu den technischen und organisatorischen Massnahmen des Datenschutzes (überarbeitet)

102 Auf der Internetseite www.dss.llv.li unter Richtlinien.

## 9.4 Organigramm



DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Kirchstrasse 8
FL-9490 Vaduz

Telefon +423 236 60 90

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