DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Tätigkeitsbericht 2015

Datenschutzstelle des Fürstentums Liechtenstein

INHALTSVERZEICHNIS

1. EINLEITUNG

Dies ist unser 14. Tätigkeitsbericht.

Die Anzahl der **Anfragen**, die wir letztes Jahr beantworteten, nahm insgesamt etwas ab. Dabei ging es um Fragen aus den unterschiedlichsten Sachgebieten. Ein Auszug dieser Fragen und deren Beantwortung wird wie üblich im ersten Teil des Berichtes dargestellt. Dabei ging es um Fragen rund um das Auskunftsrecht, Fragen im Rahmen des Finanzbereichs, zur Videoüberwachung und Drohnen, zum Arbeitsbereich oder technische Fragen wie zum Einsatz von IT-Lösungen aus den USA. Bei diesen letztgenannten Anfragen wiesen wir darauf hin, dass es aus Sicht des Datenschutzes besser ist, wenn europäische oder sogar liechtensteinische Produkte amerikanischen Lösungen vorgezogen werden (siehe Kapitel 2.1).

Der **automatische Informationsaustauch in Steuerfragen (AIA)** war letztes Jahr in aller Munde und stellte einen Schwerpunkt unserer Tätigkeiten dar und zwar auf europäischer Ebene wie auch im Inland. Auf europäischer Ebene arbeiteten wir im Rahmen der Artikel-29-Datenschutzgruppe und des Europarates aktiv mit (siehe Kapitel 6.1 und 6.2). Im Inland waren wir Mitglied der Konsultationsgruppe, welche die Regierung eingesetzt hatte und waren bereits im Vorfeld der Ausarbeitung eines Gesetzes über den automatischen Informationsaustausch (AIAG) beteiligt (siehe Kapitel 2.2 und 2.5). Schliesslich veröffentlichten wir auch einen Aufsatz zur Frage «Ist der Datenschutz beim automatischen Informationsaustausch über Finanzkonten (AIA) gewährleistet» (siehe Kapitel 4.2)?

Der AIA stand somit thematisch im Mittelpunkt unserer Tätigkeiten. Zu nennen sind aber auch folgende Tätigkeiten:

Die Arbeit im Zusammenhang mit der **Gesetzesvorbereitung** ist uns nach wie vor sehr wichtig, da dies ermöglicht, dass Gesetze den Datenschutz entsprechend berücksichtigen. Es versteht sich von selbst, dass die Praxis im Rahmen dieser Gesetze den Datenschutz dann auch einhalten muss. Unsere Stellungnahmen werden kurz dargestellt (siehe Kapitel 2.2). Nicht nur die Rechtsetzung, auch die **Rechtsprechung** ist essenziell. Im vergangenen Jahr gab es Entscheidungen des Staatsgerichtshofes und des Verwaltungsgerichts, welche wichtige Aspekte des Datenschutzes betreffen (siehe Kapitel 2.1 und 2.3).

Wir waren in mehreren **Projekten** beteiligt, wo wir aktiv mitarbeiten konnten: So beim Projekt *Datenstandort* oder in der *ZPR Kommission* (siehe Kapitel 2.5).

Im Berichtsjahr hatten wir einzelne **Aufsichtsfälle**. Dabei ist vor allem der Vorschlag der *Concordia* zur Durchführung einer freiwilligen Kontrolle hervorzuheben. Wir begrüssen diesen proaktiven Ansatz ausdrücklich (siehe Kapitel 3).

Im Rahmen der **Sensibilisierung der Öffentlichkeit** für den Schutz der Privatsphäre nimmt der *Europäische Datenschutztag* nach wie vor eine zentrale Rolle ein. Thema war das «Internet der Dinge». Daneben organisierten wir eine weitere Veranstaltung zum Thema *«Microsoft 10: Windows als neue Datenkrake?»* (siehe Kapitel 4.1). In den **Medien** informierten wir zum Beispiel über das *Safe Harbor Urteil* des Europäischen Gerichtshofs (EuGH), das grosse Wellen schlug (siehe Kapitel 4.2).

Bei der **internationalen Zusammenarbeit** stand der *AIA* im Vordergrund. Wichtig für das Land selbst ist aber auch die *Schengen Evaluation*, die letztes Jahr erneut anstand. Dabei wurden wir darauf geprüft, ob unsere Gesetzgebung, Ressourcen und Praxis den Anforderungen aus Brüssel genügen (siehe Kapitel 6.3).

Im letzten Tätigkeitsbericht hatten wir festgehalten, dass wir mehr versuchen werden, in die Tiefe ausgewählter Themen zu gehen, was eine **Straffung unserer Ressourcen** erfordert. Wir trafen einige Ent-

scheidungen, verschiedenen Tätigkeiten nicht mehr (oder zumindest nicht mehr im bisherigen Ausmass) nachzugehen. Dies betrifft vor allem den Schengen-Bereich. Aber auch im Rahmen der Stellungnahme zu Gesetzesvorhaben sind Einschränkungen nötig (siehe Kapitel 7).

Inhaltlich wollen wir an den **Schwerpunktthemen Gesundheit und Soziales, Finanzen, Datensicherheit und Jugendliche** festhalten. Absätze zu den Schwerpunktthemen haben wir in diesem Bericht entsprechend gekennzeichnet.

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 beitrugen, dass die Belange des Schutzes der Privatsphäre berücksichtigt und oft auch verbessert werden können, gilt mein aufrichtiger Dank.

Vaduz, im März 2016

Dr. Philipp Mittelberger
Datenschutzbeauftragter

2. ALLGEMEINE ORIENTIERUNG UND INDIVIDUELLE BERATUNG

2.1. Anfragen

Im letzten Tätigkeitsbericht hatten wir betont, dass wir den zukünftigen Fokus auf «weniger ist mehr» legen wollen. Dieser Anspruch bezieht sich auf alle unsere Tätigkeiten. Bei den Anfragen kann dies nur bedingt beeinflusst werden. Im Rahmen des Möglichen setzten wir einzelne Schritte: So werden Anfragen von anderen Datenschutzbehörden, die nicht nur an uns gehen und die ein Gebiet betreffen, auf dem wir keine spezielle Expertise aufweisen nicht mehr beantwortet. Zudem wurde für «Stellungnahmen und Gutachten» eine Gebührenpflicht eingeführt. Dies führte dazu, dass einzelne Anfragen zurückgezogen wurden. So gesehen setzten die insgesamt 637 Anfragen im vergangenen Jahr den Trend der zunehmenden Arbeitsbelastung fort. Soviel zum Stichwort «weniger ist mehr», auf das noch an anderen Stellen einzugehen sein wird.

Die Anzahl der Anfragen ist zwar leicht rückläufig, bewegt sich aber insgesamt seit Jahren auf einem hohen Niveau.[1] Weiterhin gingen viele Anfragen telefonisch ein und konnten ohne grossen Aufwand beantwortet werden. Bei anderen war dies nicht der Fall. Wie üblich stellen wir in Folge einen Auszug von Fragen und deren Beantwortung dar, von denen wir denken, dass sie für die Öffentlichkeit von Interesse sind.

Diese Anfragen kommen aus verschiedenen Bereichen. Bei der Darstellung dieser Anfragen folgen wir der Gliederung in früheren Tätigkeitsberichten. Zuerst werden die Anfragen dargestellt, bei denen es um die Wahrnehmung gesetzlicher Rechte ging.

Wahrnehmung gesetzlicher Rechte

Im Rahmen eines **Auskunftsbegehrens an das Landesarchiv** stellten sich zwei Fragen: Erstens müssen Daten laut Datenschutzgesetz (DSG) «erschliessbar» sein, damit ein Auskunftsbegehren zu beantworten ist. Wie ist in einem Fall zu verfahren, in dem solche Personenangaben nicht direkt auffindbar sind, sondern nur mittelbar? Die zweite Frage lautet, wie entgegengesetzte Interessen Dritter zu gewichten sind, die ebenfalls vom Auskunftsbegehren betroffen sind?

- Zur ersten Frage ist festzuhalten, dass das Auskunftsrecht gemäss Rechtsprechung des EuGH das zentrale Recht darstellt.[2] Somit ist darauf zu achten, dass es möglichst oft zum Tragen kommt. Im konkreten Fall war es so, dass das Landesarchiv zwar Daten über die betreffende Person führte, diese jedoch nicht direkt in der entsprechenden Datenbank auffindbar waren, wohl aber über den Namen einer Drittperson. Damit stellte sich die Frage, ob das Kriterium der Erschliessbarkeit erfüllt war. Diese Datenbank fusst auf dem Archivgesetz, das vor Inkrafttreten des DSG geschaffen wurde. Um der Rechtsprechung des EuGH zu entsprechen, hielten wir fest, dass das Element der *«Erschliessbarkeit» weit auszulegen* ist. In Fällen von älteren Datenbanken, wie im vorliegenden Fall, muss speziell darauf geachtet werden, ob Daten einer Person auch, wie von der Antragstellerin behauptet, über eine Drittperson gefunden werden können.

- Bei der zweiten Frage geht es um eine *Gewichtung der Interessen*: Im entsprechenden Akt beim Landesarchiv sind Daten einer Drittperson enthalten, deren Bekanntgabe nicht unproblematisch ist, da es sich um eine heikle Familiengeschichte handelte. Ist Auskunft zu geben oder nicht? Wir hielten fest, dass zunächst zu prüfen ist, ob die Interessen Dritter durch Anonymisierung oder allenfalls Erstellen einer Zusammenfassung geschützt werden können. Ist dies vollumfänglich oder in Teilen nicht möglich, ist eine Interessenabwägung vorzunehmen. Hierbei ist einerseits das Geheimhaltungsinteresse der dritten Person zu berücksichtigen und andererseits der Grund und Zweck des Auskunftsbegehrens. Grundsätzlich ist ein Auskunftsbegehren nicht zu begründen. Eine Interessenabwägung wird aber erleichtert, wenn das Landesarchiv Grund und Zweck bei der anfragenden Person in Erfahrung bringt. Diese ist jedoch dazu nicht zur Auskunft verpflichtet, obwohl dies unter Umständen vorteilhaft sein könnte. Jedoch wäre es auch denkbar, dass ihr die Angabe eines Grundes und Zweckes unter Umständen gar nicht möglich ist, da ihr die angefragten Daten gar nicht bekannt sind. Dies dürfte häufig der Fall sein. In diesen

1 Siehe unter 9.

2 Tätigkeitsbericht 2009, 1.1.2. Der Europäische Gerichtshof (EuGH) hat in einem Urteil die Bedeutung des Auskunftsrechts betont, da es erforderlich ist, um der betroffenen Person die Wahrnehmung weiterer Rechte zu ermöglichen. Vgl. College van burgemeester en wethouders van Rotterdam gegen M. E. E. Rijkeboer, Urteil vom 07. Mai 2009, Erwägung 51: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62007J0553:DE:HTML.

Fällen ist eine Interessengewichtung schwierig. Es ist aber zu beachten, dass das Auskunftsrecht das zentrale Recht darstellt.

Im Zusammenhang mit **Auskunftsbegehren** erhielten wir eine weitere Anfrage. Wird einem solchen Begehren nicht stattgegeben, ist dies nach Art. 12 Abs. 4 DSG zu begründen. Denn nur begründete Antworten können wirksam angefochten werden. *Wie gestaltet sich der Fall, wenn eine Begründung kaum oder nur schwer möglich ist, ohne eine inhaltliche Antwort zu geben?* Diese Frage stellte sich im Rahmen der Tätigkeiten der Stabsstelle Financial Intelligence Unit (SFIU). Der Verwaltungsgerichtshof hielt hierzu im Entscheid VGH 2015/030 vom 10. Juni 2015 fest, dass im Falle eines gegebenen überwiegenden öffentlichen Interesses zwar keine Auskunft zu erteilen sei,[3] allerdings müsse der Inhaber der Daten angeben, aus welchem Grund er die Auskunft verweigert, einschränkt oder aufschiebt. Die SFIU habe im Gegenzug bekanntzugeben, ob sie überhaupt personenbezogene Daten über die Beschwerdeführer bearbeiten würde und falls ja, um welche Art von Daten es sich handelt, welchen Inhalt sie haben und woher sie kommen. Die Auskunft dürfe und müsse nur so weit erteilt werden, als dadurch die überwiegenden öffentlichen Interessen noch genügend gewahrt werden könnten. Der Grund der Geheimhaltung müsse allerdings möglichst genau angegeben werden. All dies könne unter Umständen dazu führen, dass die SFIU nicht genau angeben dürfe, welche Art von Daten sie bearbeite und was der Inhalt dieser Daten sei.

Allgemeines

Das Gerichtsverfahren im Rahmen einer sogenannten Überprüfung der **WZW-Kriterien** über die Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit warf hohe Wellen. Dabei ging es um einen Leistungserbringer, dem unterstellt wurde, Geld zu Unrecht bezogen zu haben. In der Öffentlichkeit wurde spekuliert, welcher Arzt von diesem WZW-Verfahren betroffen wäre. Ebenfalls stellte sich die Frage nach den Kosten dieses Verfahrens. Die Anfrage an die zuständige Behörde *über die Höhe der Kosten* wurde aus *Datenschutzgründen* abgelehnt. Wir überprüften diesen Fall, konnten aber keine Datenschutzgründe erkennen, die gegen die Beantwortung der Anfrage spricht und empfahlen eine nochmalige Anfrage. Generell raten wir genau nachzufragen, wenn etwas pauschal «aus Datenschutzgründen» abgelehnt wird.

3 Erwägung 5 f.

Der Parlamentsdienst fragte uns, ob die **Veröffentlichung der Privatadresse von Richterkandidaten und von Bewerbern um die Einbürgerung nach Liechtenstein** in der Traktandenliste, in der Beratung sowie in den Beschlüssen der Landtagssitzung bzw. im Protokoll der Landtagssitzung datenschutzrechtlich zulässig ist und falls ja, welchen Anforderungen eine solche Bekanntgabe zu genügen hat. Nach Art. 2 Abs. 3 Buchstabe b DSG ist das Datenschutzgesetz auf «Beratungen im Landtag und in Kommissionen des Landtags» nicht anwendbar. Dies ist wohl darauf zurückzuführen, dass der Landtag «in der Regel» öffentlich tagt,[4] was jedoch nicht immer der Fall ist.[5] Nach Art. 73 Abs. 1 sind die Sitzungen der Kommissionen nicht öffentlich.[6] Es ist unklar wieso das DSG, das wichtige Aspekte wie die der Datenrichtigkeit, der Datensicherheit, der Löschung, der Archivierung, etc. enthält, bei Tätigkeiten des Landtags nicht gelten soll. Dies hiesse beispielsweise auch, dass Unterlagen von Landtagskommissionen nicht durch Sicherheitsmassnahmen geschützt werden müssten, was wohl kaum im Sinne des Gesetzgebers war. Unabhängig davon, ob das Datenschutzgesetz Anwendung findet oder nicht, ist die *Verhältnismässigkeit gemäss der Landesverfassung* zu beachten. Daher konnten wir hinsichtlich der Veröffentlichung der Privatadressen die Ansicht des Parlamentsdienstes bestätigen: Insbesondere im Beschluss des Landtags ist es ausreichend, wenn der Name und der Wohnort des Richterkandidaten oder des Einbürgerungsbewerbers genannt werden. Weder die Angabe der Privatadresse noch die des Geburtsdatums sind hierfür erforderlich. Dies gilt im Speziellen für künftige Landrichter, die aufgrund ihrer beruflichen Tätigkeit einem möglichen Gefährdungspotenzial ausgesetzt sind.

Technologischer Datenschutz

In regelmässigen Abständen werden wir zur Zulässigkeit der **Verwendung der PEID angefragt. Die** PEID ist eine «persönliche Identifikationsnummer» zur Sicherung der Unverwechselbarkeit von Personen (natürliche und juristische Personen), die im Zentralen Personenregister (ZPR) der Landesver-

4 Art. 26 Abs. 1 der Geschäftsordnung des Landtags.
5 Art. 27 und 28 der Geschäftsordnung des Landtags.
6 Diese Ausnahmebestimmung im DSG wird bereits im Bericht und Antrag 2001/33 auf Seite 14 erwähnt, wo jedoch keine spezifischen Gründe angeführt werden, ausser dass die Ausnahmen «restriktiv handzuhaben sind». Somit geht aus den Materialien zum DSG nicht hervor, wie diese Ausnahmebestimmung auszulegen ist. Jedenfalls fällt die Gleichbehandlung von Landtag und den Kommissionen auf, macht jedoch auf Grund der Geschäftsordnung des Landtags nur wenig Sinn. Zudem ist zu erwähnen, dass die Datenschutzrichtlinie, die mit dem DSG umgesetzt wurde, keine solche Ausnahmen vorsieht.

waltung registriert sind.[7] Ihre Verwendung ist im Gesetz über das Zentrale Personenregister (ZPRG) geregelt. Sowohl Behörden als auch private Dateninhaber (Privatpersonen und Unternehmen) dürfen die PEID *ausschliesslich im Behördenverkehr* zur eindeutigen Identifizierung von Personen verwenden. Eine anderweitige Nutzung ist nicht zulässig und strafbeschwert.[8] Die Landesverwaltung hat vor, die PEID auf deren Dokumenten prominenter als bisher abzudrucken. Bereits in der Vergangenheit wiesen wir darauf hin, dass dabei Bedürfnisse geweckt werden könnten, diese Nummer auch im Privat- und Unternehmensumfeld zu verwenden.[9] Dies würde eine firmenübergreifende Identifizierung sowie einen automatisierten Abgleich von Informationen über die Grenzen von Datenbeständen hinweg ohne grossen Aufwand ermöglichen, was aus Sicht des Datenschutzes eine der grössten Gefahren im Zusammenhang mit der Verwendung der PEID darstellt.[10] Aus diesem Grund raten wir zu einem verantwortungsbewussten Umgang mit der PEID und, wo zweckmässig und sinnvoll, die Verwendung einer bereichsspezifischen ID.

Eine **Arztpraxis** fragte an, ob es mit dem Datenschutz vereinbar wäre, wenn **Terminabsprachen mit Patienten** über einen durch sämtliche Mitarbeiter gemeinsam genutzten Kalender (konkret in der **iCloud** von Apple Inc.) bearbeitet würden. Gerade im Zusammenhang mit der Nutzung von Cloud-Diensten kann die Prüfung der Datenbearbeitung sowie der organisatorischen und technischen Sicherheitsmassnahmen und somit die Wahrnehmung der Verantwortung durch den Cloud-Nutzer aufgrund der fehlenden Transparenz schwierig sein (z. B. aufgrund des fehlenden Zugangs zu den Protokollen). Zudem besteht unter Umständen das Risiko eines unbefugten Zugriffs auf die Datenbearbeitung sowie das einer widerrechtlichen Veröffentlichung.[11] Da das Bekanntwerden von Praxisbesuchen bei einem Facharzt einen Eingriff in die Privatsphäre der Betroffenen darstellt, erfordert dies entsprechend hohe Sicherheitsmassnahmen. Im konkreten Fall ergab eine erste Beurteilung der iCloud von Apple, dass die Speicherung und Bearbeitung von Patientennamen aufgrund des erhöhten Schutzbedarfs *ohne zusätzliche Sicherheitsmassnahmen* mit dem Datenschutz *nicht vereinbar ist*. Seit der Entscheidung des EuGH zum Safe-Harbor-Abkommen ergeben sich zusätzliche Hürden bei der Nutzung von Cloud-Diensten in den USA.[12] Dieses Problem könnte mit dem Einsatz einer europäischen oder gar einer liechtensteinischen Cloud umgangen werden. Letzteres wäre auch für den «Datenstandort Liechtenstein» von Vorteil.

In eine ähnliche Richtung gingen mehrere Anfragen betreffend den **Einsatz von Google Analytics**, einem kostenlosen Analysedienst von Google Inc., mit dem Daten zum Nutzungsverhalten von Besuchern auf Internetseiten gesammelt und ausgewertet werden können.[13] So wird unter anderem gespeichert, woher die Besucher kommen, welche Inhalte auf einer Internetseite aufgerufen und wie oft bzw. wie lange welche Unterseiten und Kategorien betrachtet werden. Seitenbetreiber müssen diese Daten löschen oder anonymisieren, sobald sie ihren Zweck der Erstellung von Statistiken erfüllt haben. Die Auswertung und Aufbereitung der Statistiken findet bei Google Analytics in der Standardkonfiguration in erster Linie in den USA statt. Aus diesem Grund ist auch hier die Safe-Harbor-Entscheidung des EuGH anwendbar. *Dies bedeutet, dass die Übermittlung von personenbezogenen Daten in die USA illegal ist*. Deshalb raten wir Betreibern von Webseiten zum Einsatz einer alternativen Lösung für die Erstellung von Webstatistiken. Auch in diesem Falle empfehlen wir den Einsatz einer europäischen, im Optimalfall einer liechtensteinischen Lösung. Auf unserer Internetseite veröffentlichten wir diesbezüglich allgemeine Informationen.[14]

Ein Unternehmen fragte uns zu einem **Zeiterfassungssystem mit Handscannern** an. Zur Erfassung der Arbeitszeiten sollte jeweils die Handfläche des Angestellten gescannt werden. Bei Handflächenabdrücken geht es um biometrische Merkmale, die im konkreten Fall ausschliesslich zur Zeiterfassung genutzt werden sollten. Die Verwendung als Schutzmassnahme vor unberechtigtem Zutritt zu den Räumlichkeiten stellte sich nicht. Biometrische Merkmale sind höchstpersönlich und unveränderbar, wodurch deren Bearbeitung grundsätzlich ein schwerer Eingriff in die Privatsphäre der Betroffenen darstellt.[15]

7 Zur PEID siehe auch Tätigkeitsbericht 2009, 1.2. und Tätigkeitsbericht 2008, 3.1. sowie Tätigkeitsbericht 2007, 5.1.2.
8 Art. 6 Abs. 3 und Art. 19 ZPRG.
9 Tätigkeitsbericht 2009, 1.2.
10 Vgl. Rechtsgutachten von Giovanni Biaggini, Professor für Staats- und Verwaltungsrecht an der Universität Zürich, Ein Personenidentifikator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes (Art. 13 BV), Dezember 2002), abzurufen unter: http://www.edoeb.admin.ch/datenschutz/00786/00946/00949/index.html?lang=de.
11 Vgl. Thema «Cloud Computing» unter 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.
12 Siehe unter 4.2.
13 Tätigkeitsbericht 2011, 1.2.
14 http://www.llv.li/#/188/auswertungstools-fur-internetseiten.
15 http://www.llv.li/#/11197/biometrische-daten.

Jeder Eingriff benötigt einen Rechtfertigungsgrund und muss so gering wie möglich gehalten werden. Der Dateninhaber darf nur diejenigen Daten bearbeiten, die für die Erfüllung des Zwecks unbedingt notwendig und geeignet sind (Verhältnismässigkeitsprinzip).[16] Jedenfalls sind andere, weniger einschneidende Lösungen zu prüfen und anzuwenden. Wir sehen die Bearbeitung von biometrischen Merkmalen zur Zeiterfassung *grundsätzlich kritisch*. Jedenfalls sind alternative, weniger in die Privatsphäre der Betroffenen eingreifende Massnahmen zu prüfen und anzuwenden. Aus diesem Grund teilten wir dem Unternehmen mit, dass das Zeiterfassungssystem mit Handscannern einer datenschutzrechtlichen Prüfung schwer standhalten würde und deshalb unzulässig sei.[17]

Eine Anfrage betraf die Anforderungen an ein **Flottenmanagement.** Grundsätzlich ist der Einsatz von GPS in Fahrzeugen zum Zwecke der Organisation und Steuerung einer Flotte zulässig. In der Ausgestaltung sind jedoch eine Reihe von Restriktionen zu berücksichtigen.[18] Jedenfalls besteht ein *Verbot der Verhaltensüberwachung*. Ebenfalls ist eine Nutzung der erfassten Daten ausserhalb des klar bestimmten Zwecks nicht zulässig. Dieser ist in einem Überwachungsreglement klar und unmissverständlich festzuhalten und den Betroffenen mitzuteilen. Je nach Zweck ist festzulegen, welche Personen Zugriff auf die Lokalisierungsdaten benötigen. Der Kreis der zugriffsberechtigten Personen ist entsprechend klein zu halten. Im Zusammenhang mit den Zugriffsrechten ist zwischen Live-Sichtung und der Bearbeitung von Vergangenheitsdaten zu unterscheiden. Insbesondere der Zugriff auf Vergangenheitsdaten ist entsprechend streng zu regeln. Die GPS-Daten sind nach Zweckerreichung zu löschen oder (z. B. für statistische Zwecke) zu anonymisieren. Es ist wichtig, dass die Datenbearbeitung streng *zweckgebunden* und *transparent* für die betroffenen Mitarbeiter *erfolgt*. Dies schützt deren Privatsphäre und schafft Akzeptanz.

Wir wurden angefragt, welche **Sicherheitsanforderungen an eine physische Ablage** (Aktenschränke) zu stellen sind. Allgemein gilt, dass die Sicherheitsmassnahmen angemessen sein müssen. Die Angemessenheit einer Massnahme zum Schutz von Personendaten hängt unter anderem vom konkreten Schutzbedarf der Daten ab. Art. 9 Abs. 1 DSV verlangt nicht, dass in jedem Fall das Höchstmass an Schutzmassnahmen notwendig ist. Die Massnahmen müssen vor allem Risiken, wie den Schutz vor unbefugter oder zufälliger Vernichtung, zufälligem Verlust sowie unbefugtem Bearbeiten berücksichtigen. Dies gilt sowohl für die physische Ablage als auch für die elektronische Datenbearbeitung. Vor der Festlegung angemessener Schutzmassnahmen ist daher eine entsprechende *Risikobewertung* (engl. Risk Assessment) durchzuführen.[19] Im Zuge der Datenschutzreform in Brüssel wird vor allem darauf abgestellt, das Risiko einer Persönlichkeitsverletzung zu minimieren (Risk Based Approach). Im konkreten Fall waren die uns gegenüber erklärten baulichen sowie organisatorischen Massnahmen, wie z. B. restriktive Vergabe von Schlüsseln für den Zugang zu den betroffenen Räumlichkeiten, ausreichend, um die physische Ablage vor unbefugtem Zugriff angemessen zu schützen. Die Beschaffung von Aktenschränken mit einer erhöhten Schutzklasse war nicht notwendig.

Eine Amtsstelle fragte an, ob im Zusammenhang mit dem **Austausch eines Druckers** spezifische Datensicherheitsmassnahmen zu beachten sind. Moderne Drucker, Kopierer oder andere Multifunktionsgeräte haben häufig Datenträger verbaut. Diese dienen den Geräten als Zwischenspeicher, in denen Druckaufträge sowie in vielen Fällen die vollständigen Dokumente über einen längeren Zeitraum gespeichert bleiben. Dieser Umstand muss bei der Entsorgung von Altgeräten entsprechend berücksichtigt werden. Abhängig vom Schutzbedarf der ausgedruckten Dokumente ergeben sich hier unterschiedliche Anforderungen und Möglichkeiten.[20] Im gegenständlichen Fall bot der Servicetechniker bereits von sich aus an, den Datenträger auszubauen und der Amtsstelle zu übergeben. Wir rieten der Amtsstelle den Datenträger entgegenzunehmen und einer ordnungsgemässen Vernichtung zuzuführen.

Polizei, Sicherheit und Justiz

Zwei Anfragen betrafen die Installation von **Videokameras oder auch Webcams** zur **Dokumentation von**

16 Art. 4 Abs. 2 DSG.
17 Tätigkeitsbericht 2011, 1.7.
18 http://www.llv.li/#/1527/geolokalisierungortung-von-personen.

19 Gerade bei komplexeren Datenbearbeitungen wird es notwendig sein, bereits vor der Inbetriebnahme einer Datensammlung eine entsprechende Risikobewertung durchzuführen. Dabei sind insbesondere der betroffene Personenkreis (Anzahl der Personen, Grund der Aufnahme in die Datensammlung, wie z. B. Vereinsmitglied, Kunden, Krebsregister), die Komplexität des Systems als auch die bearbeiteten Personendaten selbst zu berücksichtigen. Zur Durchführung einer Risikoanalyse, vgl. BSI-Standard 100-3, «Risikoanalyse auf der Basis von IT-Grundschutz» und ISO 31000.
20 Siehe «M 2.400 Sichere Außerbetriebnahme von Druckern, Kopierern und Multifunktionsgeräten» im BSI-Grundschutzkatalog, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02400.html.

Baufortschritten. In einem Fall waren die Aufnahmen in Echtzeit im Internet abrufbar. Wir wiesen die Betreiber jeweils darauf hin, dass die Videokameras so zu konfigurieren sind, dass die aufgenommenen Personen, insbesondere jene, die auf der Baustelle arbeiten, nicht identifiziert werden können. Zudem ist der Kamerafokus so einzustellen, dass andere im Umfeld befindliche Personen nicht aufgenommen werden. Ferner muss die Kamera so angebracht werden, dass der Eindruck der Überwachung vermieden wird. In der Praxis wird empfohlen, sämtliche betroffenen Personen wie auch Nachbarn über die Baustellendokumentation zu informieren. Zusätzlich sind Einwilligungen einzuholen, sollten beispielsweise benachbarte Grundstücke von der Aufzeichnung betroffen sein.

Auch im vergangenen Jahr erhielten wir Anfragen zu Aufnahmen durch an **Drohnen** befestigter Kameras. Bei diesem Thema stellen sich nach wie vor eine Reihe von offenen Fragen, insbesondere diejenigen nach dem Betreiber der Drohne. Dies ist Voraussetzung, um überhaupt zu wissen, an wen man sich wenden kann, wenn man gefilmt wird. Aus diesem Grund konnten wir lediglich allgemeine und grundsätzliche Antworten geben.[21]

Wirtschaft und Finanzen

Das Gesetz zum automatischen Informationsaustausch **(AIA-Gesetz)** sieht vor, dass liechtensteinische Finanzinstitute Kundendaten erheben und an die Steuerverwaltung weiterleiten müssen, welche sie dann in den jeweiligen Heimatstaat übermittelt. Die Kunden sind hiervon vorgängig zu unterrichten und haben diesbezüglich ein Widerspruchsrecht. Artikel 12 des AIA-Gesetzes verweist hier, nach dem Vorbild der entsprechenden Richtlinie 2014/107, explizit auf das DSG. Unter dem Stichwort der Verhältnismässigkeit wird argumentiert, dass im Zuge des Informationsaustauschs auch Daten übermittelt würden, die für den Heimatstaat gar nicht nötig seien. So wurden wir darauf aufmerksam gemacht, dass beispielsweise bei rückkaufsfähigen Lebens- und Rentenversicherungen jährlich der Rückkaufswert zu melden sei. Dieser sei jedoch für Staaten, in denen es keine Vermögenssteuer gibt, steuerrechtlich nicht relevant. Somit könnte man den Austausch diesbezüglicher Daten als unverhältnismässig erachten. Wir wurden nach unserer Ansicht und den Erfolgsaussichten eines solchen Falles vor Gericht gefragt. Wir mussten darauf verweisen, dass der Grundsatz der Verhältnismässigkeit nicht nur von der Landesverfassung, sondern auch von der Europäischen Menschenrechtskonvention vorgegeben ist. Anderseits beruht das System auf internationalen Standards, welche die OECD-Staaten beschlossen haben und die von 78 Staaten (alle EU-Mitgliedstaaten eingeschlossen) unterstützt werden. Daher sind wir der Meinung, dass es hier nicht um die Frage einer konkreten Gesetzesbestimmung in Liechtenstein geht, sondern vielmehr um einen möglichen Widerspruch internationaler Rechtsinstrumente wie dem Common Reporting Standard (CRS) und der Europäischen Menschenrechtskonvention.

Die **vierte europäische Geldwäscherichtlinie** 2015/849/EG sieht in Artikel 30 ein zentrales **Register mit Angaben zu den wirtschaftlich Berechtigten** vor. Künftig sind alle juristischen Personen verpflichtet, präzise und aktuelle Angaben zu ihren wirtschaftlich Berechtigten einzuholen und aufzubewahren. Die Richtlinie sieht vor, dass «der Zugang zu den Angaben zu den wirtschaftlich Berechtigten im Einklang mit den nationalen Datenschutzvorschriften» zu erfolgen hat. Wir wurden verschiedentlich nach unserer *Meinung* gefragt, wie das in Liechtenstein umzusetzen sei, konnten hierzu aber *noch keine* abgeben. Immerhin werden wir in die entsprechende Arbeitsgruppe einbezogen, in der das Thema behandelt wird. Derzeit sind verschiedene Szenarien denkbar.

Arbeitsbereich

Ein Amt beschäftigt die Frage, ob es zulässig sei, **Betriebsinspektionen** mittels Tonbandaufnahme **aufzuzeichnen**. Es wäre auch vorgesehen, von den betroffenen Personen, also sowohl vom Amtsmitarbeiter als auch des betroffenen Betriebs, eine Einwilligung einzuholen. Das Amt fragte bei uns nach, ob es aus datenschutzrechtlicher Sicht Vorbehalte gegen ein solches Vorgehen gäbe. Wir vertreten den Standpunkt, dass Tonbandaufnahmen nach erfolgter *Einwilligung der betroffenen Personen in der Regel zulässig* sind. Es besteht jedoch *Unklarheit* darüber, ob und in welchen Fällen ein *Mitarbeiter* eine gültige Einwilligung zur Bearbeitung von Personendaten durch den Arbeitgeber erteilen kann. Ferner hat sich staatliches Handeln auf eine *gesetzliche Grundlage* zu stützen. Das Amt prüft das weitere Vorgehen.

Wir wurden über einen Fall informiert, bei der sich ein Vorgesetzter alle **E-Mails** eines Mitarbeiters **automatisch weiterleiten** liess. Wir haben zu diesem Thema zwei ausführliche Richtlinien erarbeitet, die auch auf unserer Internetseite abrufbar

21 Weitere Informationen zur Drohnenthematik siehe unter 4.3 und 6.1.

sind.[22] Zur Beantwortung der Anfrage verwiesen wir auf diese Richtlinien. Grundsätzlich ist eine automatisierte Überwachung des E-Mail-Verkehrs eines Mitarbeiters durch den Vorgesetzten nicht zulässig, da sie nicht verhältnismässig ist. Unter gewissen Umständen und unter Einhaltung bestimmter Voraussetzungen gibt es jedoch Ausnahmen von diesem Grundsatz. Dies ist im Einzelfall zu prüfen und dem Mitarbeiter im Vorfeld mitzuteilen.

Wir wurden angefragt, ob es mit einer unternehmensinternen Weisung zulässig sei, **den E-Mail-Verkehr** von Mitarbeitern während **Ferienabwesenheiten** auf das E-Mail-Konto eines Stellvertreters/einer Stellvertreterin **weiterleiten** zu lassen. Bei der Abklärung ergaben sich arbeitsrechtliche Probleme, die auf relativ zwingende Bestimmungen im Arbeitsrecht zurückzuführen sind. Denn auch mit erfolgter Einwilligung des Mitarbeiters stösst man an rechtliche Grenzen, da diese nur die eigenen Daten, nicht die der Absender umfasst. Deshalb empfehlen wir die Verwendung einer Abwesenheitsnotiz mit der Angabe einer Stellvertreteradresse.

Bildung

Aufgrund diverser Anfragen aus dem Schulbereich im Zusammenhang mit der zulässigen Datenbearbeitung und Datenbekanntgabe erarbeiteten wir zusammen mit dem **Schulamt** ein **Merkblatt** zur Frage, wie mit Personendaten in öffentlichen und in von der Regierung bewilligten privaten Schulen umzugehen ist. In der Fassung, welche anlässlich der Schulleiterkonferenz vorgestellt wurde, skizzierten wir die Pflichten der Schule als Dateninhaber, die Rechte der Schüler und Eltern (betroffene Personen) sowie grundlegende Datenbearbeitungen im Schulbereich wie die Weitergabe von Daten, die Auskunft an Erziehungsberechtigte und den Informationsaustausch unter Lehrern. Im Anhang des Merkblatts finden sich Praxisbeispiele, die eine nützliche Hilfe im Schulalltag bieten sollen, wie bspw. der zulässige Inhalt sowie der richtige Umgang mit Schülerbeurteilungen, dem Klassenbuch, Klassenverzeichnissen für unterrichtende Lehrpersonen, Telefonlisten, Ranglisten und Schulwebsites.

22 Richtlinie über Internet- und E-Mail-Überwachung am Arbeitsplatz für öffentliche Verwaltungen und Privatwirtschaft; Richtlinie für die Bearbeitung von Personendaten im Arbeitsbereich, http://www.llv.li/#/12550/richtlinien.

Datenbekanntgabe im Inland

Im Rahmen eines Amtshilfebegehrens wurden wir von einer Amtsstelle angefragt, ob sie der anfragenden Behörde Personendaten von ca. 1600 Personen bekanntgeben dürfen. Diese vertrat den Standpunkt, dass die Daten zur Erfüllung ihrer Aufgabe erforderlich wären und ihr diese Daten aus diesem Grunde zu übermitteln seien. Auf Basis der uns vorliegenden Aktenlage kamen wir zum Schluss, dass die anfragende Amtsstelle im Hinblick auf die in Frage stehende Aufgabe nicht zuständig war und die Datenbekanntgabe daher nicht von den bestehenden Bestimmungen abgedeckt wurde. Zum Zeitpunkt der Anfrage hätte die Datenbekanntgabe ausserdem den verfassungsmässigen Grundsatz der Verhältnismässigkeit nicht gewahrt: Einerseits wurden andere, mildere Mittel zur Aufgabenerfüllung nicht ausgeschöpft, welche die Anzahl der angefragten Personendaten wahrscheinlich reduziert hätten. Andererseits war uns nicht klar, wie die anfragende Amtsstelle die bekanntzugebenden Daten in der Folge so reduzieren hätte können, dass sie die Aufgabe auch tatsächlich erfüllen könnte. Aufgrund der besonderen Umstände des zu beurteilenden Sachverhaltes war ausserdem unklar, ob die bekanntzugebenden Personendaten überhaupt zur Erfüllung der Aufgaben beitragen hätten können.

2.2 Stellungnahmen zu Vorlagen und Erlassen

Der Grundsatz «weniger ist mehr» gilt fortan auch für die Bearbeitung von Vernehmlassungsberichten. Unsere Rechtsordnung hat zum Ziel, das Zusammenleben der Gesellschaft zu regeln. Daher betrifft sie in vielen Fällen Personendaten. Aus diesem Grund erhalten wir alle Vernehmlassungsvorlagen zur Prüfung zugeschickt. Es gibt Vorlagen, deren Bearbeitung sehr zeitintensiv ist. Auch hier müssen wir uns auf das Wichtigste beschränken. Die Entscheidung, ob wir Stellung nehmen, treffen wir anhand unserer definierten Schwerpunkte und auch dort von Fall zu Fall.

In der Folge zählen wir unsere Stellungnahmen in der Reihenfolge ihrer Wichtigkeit auf:

Nachdem wir eine Abschaffung der Datenschutzkommission (DSK) vorgeschlagen hatten, beschloss die Regierung, hierzu ein Vernehmlassungsverfahren durchzuführen. Wir nahmen zu dieser **Revision des Datenschutzgesetzes Stellung**. Dabei begrüssten wir die Abschaffung der DSK. Laut Rechenschaftsbericht 2014 sind bei der DSK 2014 keine

Beschwerden eingegangen.[23] Dies dürfte 2015 nicht anders gewesen sein – jedenfalls wurden wir über keinen Fall informiert oder um eine Stellungnahme gebeten.

Der automatische Informationsaustausch von Steuerdaten ist ein wichtiges Thema für einen Finanzplatz wie Liechtenstein. In diesem Zusammenhang konnten wir auf verschiedenen Ebenen mitwirken: Neben der Artikel-29-Datenschutzgruppe (WP 29) waren wir auch in Liechtenstein in einer entsprechenden Kooperationsgruppe, die von der Regierung ins Leben gerufen worden war, vertreten.[24] Informationen aus diesen beiden Gremien flossen in den **Vorentwurf eines Gesetzes über den automatischen Austausch von Steuerdaten** (AIAG) ein. Die geänderte Amtshilferichtlinie 2014/107/EG enthält einige zusätzliche Datenschutzbestimmungen, welche in der ursprünglichen Richtlinie 2011/16/EG noch nicht enthalten waren. Obwohl Liechtenstein (noch) nicht formell verpflichtet war, diese Bestimmungen zu übernehmen, befürworteten wir dies, da sie vielfach die Rechte von Personen betreffen. Unsere Anmerkungen wurden fast alle berücksichtigt. Wir begrüssen es, bei einem so wichtigen Gesetzesvorhaben frühzeitig beigezogen worden zu sein.

Zu folgenden Gesetzesprojekten gaben wir ebenfalls eine Stellungnahme ab:[25]

- Gesetz über die Stabsstelle Financial Intelligence Unit (FIUG)
- Strafgesetzbuch (StGB) und Gesetz über den Erwerb und Verlust des Landesbürgerrechtes (BüG) (Terrorismusbekämpfung)
- Gesetz über bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (UCITSG)
- Rechtshilfegesetz (RHG)
- Gesetz über die Durchführung der internationalen Amtshilfe in Steuersachen (Steueramtshilfegesetz; SteAHG) im Bereich Gruppenanfragen
- Gesetz über die Architekten und andere qualifizierte Berufe im Bereich des Bauwesens (Bauwesen-Berufe-Gesetz; BWBG)
- Gesetz über die Finanzmarktaufsicht (FMAG) (Verfahren zur Zusammenarbeit mit ausländischen Behörden im Bereich der Wertpapieraufsicht)
- Gesetz über Investmentunternehmen (IUG)
- Geldspielgesetz
- E-Government-Gesetz
- Gesetz über die Banken und Wertpapierfirmen (MiFID II)

In einer internen Vernehmlassung nahmen wir zudem Stellung zur Verordnung über die Informationssysteme der Landespolizei (PolISV).

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

Im letzten Tätigkeitsbericht hatten wir erwähnt, dass wir die dort genannten Rechtsmittelverfahren mit Interesse weiter verfolgen würden.[26] Der StGH entschied in einem Fall, der die Datenbekanntgabe mittels Einantwortungsbeschluss betraf, dass in Bezug auf die Grundverkehrskommission und das Amt für Justiz (Abteilung Grundbuch) kein Erfordernis bestehe, dem Einantwortungsbeschluss Angaben über die Nachlassaktiven und -passiven entnehmen zu können. Auch für die Steuerverwaltung sei dies nicht erforderlich; zum einen weil Liechtenstein weder eine Erbschafts-, Erbanfalls- noch eine Nachlasssteuer kenne und daher diese Angaben nicht zur Berechnung einer Steuer erforderlich seien; und zum Zweiten weil zur Besteuerung des ruhenden Nachlasses sowie für die Kenntnis des Endes der Steuerpflicht des ruhenden Nachlasses und des Übergangs der Steuerpflicht auf die Rechtsnachfolger alle notwendigen Informationen gemäss Steuergesetz von den Gemeinden der Steuerverwaltung übermittelt würden.[27] Von wesentlicher Bedeutung sind für uns insbesondere folgende Aussagen des StGH-Entscheids 2014/107 vom 9. Februar 2015:

- Der sachliche Schutzbereich des grundrechtlichen Datenschutzes umfasst jeden Umgang mit personenbezogenen Daten, dies ungeachtet der Verfahren der Datenbearbeitung und ungeachtet davon, ob die Datenbearbeitung fallweise erfolgt oder ob die personenbezogenen Daten in einer erschliessbaren Datensammlung bearbeitet werden (Erw. 3.1).
- Der Eingriff in ein spezifisches Grundrecht wie die Geheim- und Privatsphäre ist nur zulässig, wenn die entsprechenden Eingriffskriterien, insbesondere das Verhältnismässigkeitsprinzip bzw. das Übermassverbot eingehalten werden (Erw. 3.2).

23 Rechenschaftsbericht 2014, S. 305.
24 Mehr dazu unter 2.5 und 6.1.
25 Die Stellungnahmen sind zum Teil abrufbar unter http://www.llv.li/#/12458/externe-stellungnahmen-zu-vernehmlassungsberichten.
26 Tätigkeitsbericht 2014, 2.3. und 8.
27 StGH 2014/107 vom 09.02.2015 in: LES 2015, 69 (Heft 2).

- Da es um einen Eingriff in die von Art. 32 Abs. 1 LV und Art. 8 EMRK geschützte Privatsphäre geht, haben die Gerichte ein vom Gesetzgeber eingeräumtes Ermessen immer im Lichte dieses Grundrechts und somit insbesondere auch verhältnismässig auszuüben (Erw. 3.3).

Dieser Entscheid ist für den Datenschutz sehr wichtig, weil es im Kern dieses Falls um Fragen des Datenschutzes geht. Diese höchstgerichtliche Rechtsprechung schafft Klarheit für die Praxis. Bedeutend ist insbesondere die Aussage, dass (auch) die Gerichte bei einer Ermessensausübung im Rahmen der Privatsphäre die Verhältnismässigkeit zu beachten haben.

Diese Rechtsprechung erfordert eine Änderung der bisherigen Vorgehensweise. Wir wurden informiert, dass die neue Praxis den Anforderungen des Urteils nicht mehr genüge. Dies konnten wir noch nicht prüfen und werden dies im kommenden Jahr erledigen.

2.4 Auslandsdatentransfer und Empfehlungen bei Auslandsdatentransfer

Unternehmensinterne verbindliche Datenschutzregelungen (Binding Corporate Rules – BCRs) stellen eine Möglichkeit dar, den Datentransfer ins Ausland zu regeln. Diese Regeln sind umfassend und betreffen insbesondere die Datenbearbeitung allgemein, die Datenbekanntgabe, aber auch Fragen der Datensicherheit und Haftbarkeit. BCRs müssen in Liechtenstein durch die Regierung genehmigt werden. Wir haben zu einem solchen Antrag eine Stellungnahme abzugeben (Art. 8 Abs. 3 DSG). Da BCRs vom jeweiligen Konzern normalerweise gleich in mehreren EWR-Staaten genehmigt werden sollen, wurde ein spezielles vereinfachtes Prüfungsverfahren eingeführt, das Mutual Recognition Procedure.[28] Wir wurden erstmals von einem Konzern angefragt, ob wir als Lead Authority agieren möchten. Verschiedene Gründe innerhalb des Konzerns führten zu einer Verzögerung bei der Antragsstellung. Dennoch setzten wir uns vertieft mit dieser Thematik auseinander und konnten einige Vorfragen klären sowie Kontakte mit anderen Datenschutzbehörden herstellen. Die offizielle Antragsstellung ist offenbar für 2016 geplant. Wir sehen die Möglichkeit, BCRs in Liechtenstein genehmigen zu lassen, als Chance für den «Datenstandort».[29]

Wir wurden von einer Anwaltskanzlei angefragt, was zu berücksichtigen sei, wenn ein Unternehmen DNA-Proben von Liechtenstein in die USA liefern möchte. Dort soll die DNA nach ethnischer Herkunft aufgeschlüsselt werden. Ohne tiefere, auf den konkreten Fall bezogene Abklärung ist in Bezug auf den Auslandsdatentransfer hinzuweisen, dass die USA grundsätzlich nicht als ein Land gilt, das einen angemessenen Datenschutz aufweist. In solche Drittländer können Daten nur unter bestimmten Voraussetzungen transferiert werden. Dazu gehören unter anderem Standardvertragsklauseln oder das Safe-Harbor-Abkommen.[30] Zusätzlich zu den Voraussetzungen für einen zulässigen Auslandsdatentransfer sind gegebenenfalls diejenigen zur Auftragsdatenbearbeitung[31] zu berücksichtigen, ebenso wie die Grundsätze des Datenschutzes. Insbesondere ist auf eine gültige Einwilligung zu achten.[32]

2.5 Projektbegleitung

In der **Konsultationsgruppe über den automatischen Informationsaustausch von Steuerinformationen konnten** wir über aktuelle Entwicklungen auf der Seite des Datenschutzes informieren. Dabei ging es vor allem um Entwicklungen auf europäischer Ebene.[33]

Dieses Wissen war auch im Rahmen der Arbeiten zum **Abschluss eines Abkommens über den automatischen Informationsaustausch zwischen Liechtenstein und den EU-Mitgliedstaaten** gefragt. Dort konnten wir unsere Kenntnisse in Bezug auf die revidierte Amtshilferichtlinie und insbesondere die Entwicklungen im Rahmen der WP 29 einbringen und der Europäischen Kommission gegenüber vertreten.[34] Wir betonten dabei vor allem, dass relevante europäische Rechtsprechung in jedem Fall zu beachten ist, um allfälligen Haftungsfragen zuvorzukommen.[35]

28 Dabei ist eine Datenschutzbehörde die federführende Behörde (Lead Authority) und prüft die BCRs eingehend. Das Ergebnis, der Bericht, wird den anderen Teilnehmenden Datenschutzbehörden mitgeteilt. Diese können sich dann auf die Befunde der Lead Authority berufen.

29 Siehe unter 2.5.

30 Diese Anfrage wurde noch vor dem Safe Harbor Urteil des EuGH beantwortet. Seither ist Safe Harbor keine gültige Rechtsgrundlage mehr, siehe unter 4.2.

31 Art. 23 DSG, http://www.llv.li/#/11479/outsourcing-datenbearbeitung-im-auftrag.

32 Art. 18 Bst. c DSG.

33 Siehe unter 6.1 und 6.2.

34 Siehe unter 2.2.

35 Siehe unter 6.1.

Im aktuellen Regierungsprogramm ist das Stichwort **«Datenstandort»** enthalten. Unter dem Titel «Liechtenstein als attraktiven Wirtschaftsstandort positionieren» wird als Massnahme erwähnt: «Die Chancen von Liechtenstein als Datenstandort werden geprüft».[36] Im Rahmen des Teilprojektes «Datenschutz» wurden wir eingeladen, mitzuarbeiten. In Sitzungen mit Unternehmensvertretern wurde diskutiert, was der Datenschutz dazu beitragen könnte, damit sich Liechtenstein als attraktiver Wirtschaftsstandort positionieren kann. Unserer Ansicht nach ist Datenschutz oft mit dem Schutz von Vertrauen gleichzustellen. Vertrauen stellt in vielen Bereichen eine unerlässliche Basis für Beziehungen dar, sei es im Zusammenhang mit Unternehmen oder Behörden. Wir wiesen auf die Bedeutung der schon länger laufenden Reform des europäischen Datenschutzes hin, die ja nicht zuletzt durch Unternehmen gefordert wurde, um Rechtssicherheit in Europa zu schaffen. Liechtenstein als EWR-Mitglied sollte – unter Berücksichtigung der Kleinheit des Landes – versuchen, diese Reform als Chance zu verstehen, gerade im Zusammenhang mit dem Schlagwort «Datenstandort». Bei diesem Projekt geht es um weit mehr als um den Aufbau von Datenzentren, sondern auch beispielsweise um die Förderung von Massnahmen im Rahmen von BCR.[37] Die kurzen Wege in Liechtenstein stellen hier einen Vorteil dar, der genutzt werden sollte. Es geht allgemein darum, wie sich Liechtenstein in einem sich ständig ändernden Umfeld möglichst gut vorbereiten kann, um neue Geschäftsfelder zu generieren. Dazu gehören auch Fragen zur Digitalisierung unserer Gesellschaft. Die Wichtigkeit, aber auch die Komplexität dieses Projektes, kann nicht genügend betont werden.

Bekanntermassen erklärte der EuGH die **Richtlinie zur Vorratsdatenspeicherung** für ungültig. Somit fällt in den Ländern die europarechtliche Grundlage dieser Speicherung weg. Liechtenstein hat diese Richtlinie ebenfalls umgesetzt. Es ist unbestritten, dass die Strafverfolgungsbehörden ihren Aufgaben nachkommen müssen, dies auch und gerade in einer zunehmend technisierten Welt. Die Frage ist aber, in welchem Rahmen dies erfolgen soll. Der europäische Gesetzgeber hatte mit der erwähnten Richtlinie über das Ziel geschossen, insbesondere da entsprechende Sicherungsmassnahmen nicht vorgesehen waren. Dieses Urteil sorgte auch in Liechtenstein für Diskussionen. Dementsprechend beauftragte die Regierung eine Arbeitsgruppe mit der Analyse der möglichen Folgen für die Gesetzeslage in Liechtenstein. Wir konnten in dieser Arbeitsgruppe einen aktiven Beitrag leisten. Schliesslich ist das Thema für uns nicht neu. Der EuGH betonte bei der Untersuchung der Verhältnismässigkeit insbesondere die Datensicherheit, die in Liechtenstein noch zu wenig Beachtung gefunden hat. Zudem sollten die Straftaten, die unter die Vorratsdatenspeicherung fallen, eingeschränkt und Sanktionen bei nicht rechtmässiger Datenbearbeitung durch die verpflichteten Unternehmen eingeführt werden.[38] Wichtig ist auch, dass eine effektive Kontrolle in der Praxis möglich ist. Wir hatten in der Vergangenheit eine Kontrolle durchgeführt, die sehr aufwändig war.[39] Der Aufwand lässt sich auch damit begründen, dass nicht wir die eigentlich zuständige Aufsichtsbehörde für das Kommunikationsgesetz sind, sondern das Amt für Kommunikation. Zur Durchführung von effektiven Kontrollen bietet sich in Zukunft eine Zusammenarbeit mit dem Amt oder eine Pflicht zur Datenschutzzertifizierung durch die Unternehmen an.

Das Gesetz über das zentrale Personenregister (ZPRG) sieht eine **ZPR-Kommission** vor, in der wir vertreten sind.[40] In den *Übergangsbestimmungen* ist 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. Dieser Punkt wurde bereits 2014 mehrfach in der ZPR-Kommission behandelt. Es wurden zwar entsprechende Bewilligungen ausgesprochen und – wo notwendig – weitere Abklärungen angeregt. Doch trotz der gesetzlichen Übergangsbestimmung wurde diesen nicht in allen Fällen entsprochen bzw. nicht abschliessend nachgegangen. Wir wiesen darauf hin, dass gesetzliche (Übergangs-)Bestimmungen eingehalten werden sollten. Im ZPR werden seit 31. Dezember 2013 sämtliche Lesezugriffe protokolliert.[41] Die Mechanismen für die Auswertung dieser Protokollierung sind derzeit noch unklar. Hier muss die ZPR-Kommission noch darüber beraten und entscheiden, in welcher Form die Protokollierung zur Überprüfung der rechtmässigen Nutzung des ZPR unterstützen kann. Wir haben hier federführend ent-

36 Siehe http://www.regierung.li/files/attachments/Regierungsprogramm_2013-2017.pdf?t=635809566913788421, S. 19.
37 Siehe unter 2.4.
38 Philipp Mittelberger, Verfassungsmässigkeit der Vorratsdatenspeicherung in Liechtenstein?, veröffentlicht in: Liechtensteinische Juristen-Zeitung 1/12, S. 8ff, http://www.llv.li/#/112156/aufsatze, sowie das durch die Datenschutzstelle in Auftrag gegebene Rechtsgutachten von Hilmar Hoch, Die Regelung des staatlichen Zugriffs auf Fernmeldedaten im Kommunikationsgesetz aus grundrechtlicher Sicht, veröffentlicht in Liechtensteinische Juristen-Zeitung 4/2009, S. 99ff, http://www.juristenzeitung.li/papers/showpdf/LJZ_2009_04.pdf.
39 Tätigkeitsbericht 2012, 1.3. und Tätigkeitsbericht 2013, 4.
40 Art. 16 ZPRG; Tätigkeitsbericht 2012, 1.8.
41 Art. 7 Abs. 3 ZPRG.

sprechende Grundlagen ausgearbeitet und in die ZPR-Kommission eingebracht. Die Regierung wurde angefragt und eingebunden. Dies insbesondere, da sie sich klar dafür ausgesprochen hat, dass eine widerrechtliche Nutzung strafbeschwert sein soll.[42] Seit dem Inkrafttreten des ZPRG konnten zwar weitere Fortschritte erzielt werden, doch sind nach wie vor zahlreiche Punkte offen.

Die Regierung bestellte 2014 die **Fachgruppe Medienkompetenz**.[43] Die Fachgruppe soll das im Land bereits bestehende, jedoch an unterschiedlichen Stellen verteilte Know-how bündeln und koordinieren, um Medienkompetenz gesamtgesellschaftlich zu stärken. Wir sitzen als ständiges Mitglied in dieser Fachgruppe, wodurch sich weitere Möglichkeiten für unsere Sensibilisierungsarbeit eröffneten, speziell bei unseren Themenschwerpunkten Datensicherheit und *Jugendliche*.[44] Zum Beispiel konnten wir an verschiedenen Sensibilisierungsveranstaltungen auf den Datenschutz im Umgang mit dem Internet hinweisen.[45] Auf der Internetseite der Fachgruppe werden regelmässig Veranstaltungen zum Thema publiziert.[46] Weiters erörterten wir die Datenschutzaspekte zu aktuellen Entwicklungen im Bereich Medien und Internet.

Diese Arbeitsgruppen sind aus unserer Sicht sehr wichtig. Ihre Tätigkeit war bis Ende des Jahres noch nicht abgeschlossen. Wir werden auch in Zukunft aktiv im Rahmen unserer Möglichkeiten in diesen Arbeitsgruppen mitwirken.

Da Liechtenstein keine eigene Berufsfachschule besitzt, wurden mit diversen Bildungsinstitutionen in der Schweiz Leistungsverträge abgeschlossen. Der frühere Datenaustausch in Papierform wurde immer stärker durch den effizienteren elektronischen Datenaustausch ersetzt. Gemeinsam mit den verbundenen schweizerischen Kantonen wechselt das Amt für Berufsbildung und Berufsberatung 2016 von der aktuellen Softwarelösung Kompass 2 auf **Kompass 3**. Wir wurden in die Projektplanung einbezogen. Es wurden mit dem Amt für Berufsbildung und Berufsberatung vor allem die mit dem Systemwechsel verbundenen technischen Änderungen und dessen Auswirkungen insbesondere hinsichtlich der rechtlichen Qualifikation diskutiert. Man kam zum Schluss, dass sich Kompass 3 – im Gegensatz zu Kompass 2 – durch eine zentrale Datenverwaltung und ein zentrales Personenregister auszeichnet, auf welches mittels Abrufverfahren zugegriffen werden kann. Wir prüften insbesondere, ob die bestehenden gesetzlichen Regelungen für diesen Systemwechsel ausreichend sind. Dabei kamen wir zum Schluss, dass das Abrufverfahren, welches im DSG speziell geregelt ist, weder im BBG noch in der BBV ausdrücklich vorgesehen ist. Somit erwies sich eine Änderung der gesetzlichen Grundlagen sowie eine Anpassung des Lehrvertrages (Aufnahme einer Einwilligungserklärung) als notwendig. Das Amt für Berufsbildung und Berufsberatung leitete umgehend die notwendigen Schritte ein, um die Datenschutzkonformität bis zur Einführung von Kompass 3 sicherzustellen.

42 Art. 19 ZPRG und Tätigkeitsbericht 2014, 2.
43 http://www.medienkompetenz.li.
44 Tätigkeitsbericht 2014, 5.
45 Siehe unter 4.1.
46 http://www.medienkompetenz.li/veranstaltungen.html.

3. AUFSICHT

Im Rahmen der Aufsicht wurden wir erstmals von einem Unternehmen angefragt, das von sich aus eine Datenschutzkontrolle wünschte. Wir begrüssen **freiwillige und präventive Kontrollen**. Dies ist ein Zeichen, dass dem Datenschutz eine entsprechende Bedeutung beigemessen wird. Die Landesvertretung der Concordia schlug im Zusammenhang mit der Datenübermittlung über sichere Verbindungen eine *Fokuskontrolle im Krankentaggeldbereich* vor. Im Zentrum stand der Datenaustausch mit externen Stellen und Kunden. Hierbei wurden die Datenflüsse über Internetformulare, aber auch jene, die telefonisch oder per Brief stattfinden, geprüft. Einige Empfehlungen und Hinweise zur Verbesserung von Datenübermittlungen mit externen Partnern wurden ausgesprochen. Diese wurden von der Concordia unmittelbar umgesetzt. So werden beispielsweise seit der Kontrolle die gesamten Webinhalte der Concordia verschlüsselt übertragen. Ferner wurde von uns angeregt, dass der ausreichenden vorgängigen Information der Kunden mehr als bisher Rechnung getragen werden soll. Auch hier wurden alle empfohlenen Optimierungen rasch umgesetzt. Grundsätzlich ist anzumerken, dass bei der Concordia ein hohes Datenschutzbewusstsein vorherrscht.[47]

Das Kommunikationsgesetz (KomG) regelt die elektronische Kommunikation und dabei unter anderem die **Vorratsdatenspeicherung** sowie die Mitwirkungspflichten der Anbieter bei der Überwachung. Im Rahmen unserer Aufsichtsfunktion schrieben wir gemeldete Unternehmen an, uns *Statistiken* in Bezug auf die aktuelle Praxis bei der *Mitwirkung der Überwachung* zukommen zu lassen.[48] Wir erhielten etwa von der Hälfte der Unternehmen Rückmeldungen, was wir als Indiz werten, dass wir offensichtlich nicht als Aufsichtsbehörde im Zusammenhang mit dem KomG wahrgenommen werden. Ungeachtet dessen konnten wir anhand der Statistiken feststellen, dass die *Mehrzahl* der angeschriebenen Unternehmen entweder *keine Anfragen zur Überwachung von Behörden* erhielten oder von der Mitwirkungspflicht nicht unmittelbar betroffen oder überhaupt operativ sind. Lediglich zwei Unternehmen registrierten Anfragen. Im Zusammenhang mit der Vorratsdatenspeicherung wurden wir von der Presse angefragt, wer denn eigentlich die Rechtmässigkeit der Datenbearbeitung bei den Strafverfolgungsbehörden prüft – nach dem Stichwort «wer überwacht die Überwacher». Grundsätzlich sind wir auch bei den Behörden für die Aufsicht zuständig. Bisher gab es aber keinen zwingenden Grund für eine Aufsichtstätigkeit.

Wir erhielten eine Mitteilung einer Privatperson, dass die **Bergbahnen Malbun AG** bei jedem Passieren eines Drehkreuzes bei der Talstation automatisch ein Foto von jedem Skifahrer machen würde. Die durchgeführte Sachverhaltsabklärung ergab, dass diese Drehsperren mit einer integrierten Fotokamera ausgestattet sind. Dabei wird beim Passieren mit einer Saison- oder Mehrtageskarte (ab 7 Tage) jedes Mal ein Foto von Gesicht und Oberkörper jener Person erstellt, die die Drehsperre passiert. Zweck ist das Aufdecken von Kartenmissbrauch. Im Rahmen der Sachverhaltsabklärung haben wir insbesondere die Verhältnismässigkeit beurteilt. Die Sachverhaltsabklärung ergab Verbesserungsbedarf. So wurden unter anderem Empfehlungen im Zusammenhang mit der *Anzahl der erstellten Fotos*, der *Speicherdauer* derselben sowie den *Informationspflichten* ausgesprochen. Den Skifahrern war nämlich nicht bewusst, dass sie bei jeder einzelnen Fahrt fotografiert wurden.

Das **Löschbegehren bei Google** ist nach wie vor pendent.[49] Da es in Liechtenstein keine Niederlassung von Google im Sinne der Datenschutzrichtlinie gibt, stellte sich die Frage, ob wir eine solche Beschwerde selbst behandeln oder nur entgegennehmen und an eine Datenschutzbehörde eines Landes, in dem Google eine Niederlassung hat, zur Entscheidung weiterleiten können oder sollen (Zuständigkeitsfrage). In Deutschland hat Google eine Niederlassung in Hamburg. Nach deutschem Recht ist der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit für solche Fälle zuständig. Deswegen wendeten wir uns mit der Bitte um Unterstützung an den Hamburgischen Datenschutzbeauftragten (auch für den Fall, dass Google unsere Zuständigkeit ablehnen sollte) und erhielten eine positive Antwort. In der Folge prüften wir den Fall nach liechtensteinischem Recht in Anlehnung an die deutsche Praxis hinsichtlich Google-Anfragen und forderten Google zur Löschung auf. *Google ging zwar auf unser Anliegen ein*, informierte uns aber, dass sie unsere Rechtsauffassung nicht teilen würden. Nach Absprache mit dem Beschwerdeführer forderten wir Google mit Belegen zur Löschung der Links auf.

47 Medienmitteilung unter http://www.llv.li/files/dss/pdf-llv-dss-mm531-freiwillige-datenschutzprufung-concordia.pdf.

48 Melderegister des Amtes für Kommunikation, http://www.llv.li/files/ak/pdf-llv-ak-melderegister.pdf.

49 Tätigkeitsbericht 2014, 2.1.

4. INFORMATION UND SENSIBILISIERUNG DER ÖFFENTLICHKEIT

4.1 Veranstaltungen

Aus Anlass des 9. Europäischen **Datenschutztages** am 28. Januar organisierten wir wieder eine Veranstaltung, zu der die Bevölkerung an die Universität Liechtenstein eingeladen war. Unser Thema war diesmal das «*Internet der Dinge*». Der Referent, Dr. Jürgen Hartung, Rechtsanwalt mit Schwerpunkt Datenschutz, betrachtete *sowohl Nutzen als auch Risiken* und erörterte Fragen wie: «Welche Informationen benötigen die Geräte für die vielfältigen Entscheidungen?», «Wer erhält die gesammelten Daten und wofür nutzt er sie?» oder «Was sagen diese Daten über mich als Person aus?». Er machte deutlich, dass neben *Anbietern, Gesetzgeber und weiteren Beteiligten auch die Verbraucher und Nutzer gefordert* sind, sich zu informieren und mit persönlichen Angaben sparsam umzugehen. Begleitend führte der *IT Crowd Club Liechtenstein* eine interaktive Umfrage durch, bei der das Publikum seine Meinung kundtun konnte. Gleichzeitig mit dem Datenschutztag veröffentlichten wir eine *Empfehlung* zum «Internet der Dinge».

Am **Compliance Day** der Universität Liechtenstein konnten wir über die *laufende Datenschutzreform in Brüssel* berichten. Dort informierten wir über die Arbeit an der künftigen *Grundverordnung* und darüber, was hier zu erwarten ist.

Am **Zertifikatslehrgang Compliance Officer** der Universität hatten wir die Möglichkeit, detailliert über den Datenschutz zu informieren. Dabei ging es um folgende Themenblöcke: *Grundsätze des Datenschutzes und Tätigkeiten der Datenschutzstelle, Auslandstransfer, Aufgaben und Stellung eines Datenschutzverantwortlichen, Rechtsprechung zum Datenschutz, Datenschutz am Arbeitsplatz, die laufende Datenschutzreform in Brüssel, die Abgrenzung zwischen IT-Sicherheit und Datensicherheit, Anonymisierung und Pseudonymisierung sowie Datensicherheit auf mobilen Endgeräten, Verschlüsselung und Datenschutz im Internet*. Insgesamt konnten wir umfassende Informationen zum Thema Datenschutz zusammenstellen. Dieser Lehrgang soll alle zwei Jahre durchgeführt werden, wodurch wir ein regelmässiges Forum bekommen. Dies ist sehr zu begrüssen.

Die Ankündigung von Microsoft zur Einführung von Windows 10, und vor allem die damit verbundenen Aussagen über den Datenschutz, sorgten für einige Aufregung in der Presse. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) kündigte gar ein Verfahren gegen Microsoft an. Wir entschieden uns vorerst für einen anderen Weg. Zusammen mit dem IT Crowd Club Liechtenstein organisierten wir eine Veranstaltung zum Thema **«Windows 10: Microsoft als neue Datenkrake?».** Das Echo war gross. Wir konnten knapp einhundert interessierte Besucher begrüssen. Diese Veranstaltung führte auch in den Medien zu einer nicht-repräsentativen Umfrage. Diese ergab, dass 54 Prozent der insgesamt 274 Teilnehmer Windows 10 als problematisch empfanden. Kurz danach beschloss die WP 29 sich ebenfalls diesem Thema zu widmen.

Die Privatsphäre ist in der von **digitalen Medien** bestimmten Informationsgesellschaft besonders gefährdet. Dies gilt in besonderem Ausmass für Kinder und Jugendliche.[50] Wir nahmen wieder an verschiedenen Veranstaltungen teil und hatten entweder bei Multiplikatoren oder auch bei den betroffenen Jugendlichen selbst die Möglichkeit, auf Gefahren für die Privatsphäre hinzuweisen. So gestalteten wir unter der Leitung der Schulsozialarbeit einen Nachmittag beim freiwilligen 10. Schuljahr zum Thema *Medienkompetenz*. Hierbei informierten wir die Jugendlichen vor allem über die «Datensammler» im Internet und wie sich der Nutzer dagegen wehren kann. Am Gymnasium hielten wir bei einer Lehrerfortbildung einen Vortrag zum Thema Smartphone und Privatsphäre. Dabei führten wir vor allem in das Geschäftsmodell *«Privatsphäre gegen Dienstleistung»* ein. Weiters zeigten wir anhand verschiedener Beispiele, dass einmal im Internet veröffentlichte oder auch mit Freunden geteilte Fotos *nicht mehr gelöscht* werden können. Gerade bei Fotos gilt der Grundsatz der Zurückhaltung. Am Beispiel der bei Jugendlichen populären App Snapchat[51] wurde gezeigt, dass es kein «digitales Polaroid» gibt und das Versprechen, die Fotos unmittelbar nach dem Betrachten zu löschen, technisch nicht gehalten werden kann. Das Jahr schlossen wir mit zwei Veranstaltungen jeweils für Eltern und Erziehungsberechtigte in Eschen (Thema: *Cybermobbing und Datenschutz*) und Schaan (*Mit dem Smartphone immer online! Das Leben verpasst?!*).

50 Tätigkeitsbericht 2014, 4.
51 www.snapchat.com.

Wie jedes Jahr organisierten wir das **Treffen mit den Datenschutzverantwortlichen der Unternehmen.** Thema war ein Aspekt der derzeit laufenden Datenschutzreform in Brüssel, der in der Zukunft wichtig sein wird. Derzeit ist das DSG grundsätzlich auf jegliche Bearbeitung von Personendaten durch Behörden und durch Unternehmen anwendbar. Der Anwendungsbereich ist somit enorm. Wir hatten uns 2012 für die Themen Datensicherheit, Finanzplatz, Kinder und Jugendliche sowie Gesundheit und Soziales als thematische Schwerpunkte entschieden. Das heutige Gesetz unterscheidet bekanntlich zwischen «normalen» Daten einerseits und besonders schützenswerten Daten und Persönlichkeitsprofilen anderseits. Somit gibt es *zwei Schutzstufen*. Dieser Ansatz wird in der laufenden Datenschutzreform mit dem *risikobasierten Ansatz* (Risk Based Approach) ausgebaut. Dieser besagt, dass abhängig vom durch die Datenbearbeitung entstehenden Risiko für die betroffenen Personen, sich die notwendigen Sicherheitsmassnahmen ändern. Dieser Ansatz folgt dem Anliegen der Wirtschaft, mit der Reform Bürokratie abzubauen. An dieser Veranstaltung wurde ein Expertenpapier vorgestellt, das wir in Auftrag gegeben hatten und das bereits heute als Gradmesser herangezogen werden kann. Das Papier erlaubt es, einzuschätzen, ob und welcher Handlungsbedarf zum Schutz von Daten besteht. Dieses Expertenpapier ist auf unserer Internetseite veröffentlicht.[52]

Weiters thematisierten wir verschiedene **Sicherheitsaspekte von Internetseiten**. In der Vorbereitung zur Veranstaltung prüften wir die datenschutzkonforme Ausgestaltung von 77 Internetseiten. Den Fokus richteten wir auf die Datensicherheit (*Verschlüsselung von Kontaktformularen und Logins*), die Verwendung von Lösungen zur Erzeugung von Statistiken sowie die Informationspflichten. Wir stellten fest, dass nur etwa jede zehnte Seite eine ordnungsgemässe Datenschutzerklärung aufwies.[53] Auch wird von der Verschlüsselung nur unzureichend Gebrauch gemacht. Mehr als die Hälfte der überprüften Internetseiten übertrugen die Daten der Kontaktformulare ohne jegliche Massnahmen zum Schutz gegen unberechtigtes Einsehen. Selbst Benutzernamen und Passwörter für den Zugang zu geschützten Bereichen (Login) wurden bei mehr als einem Drittel der überprüften Seiten ohne jegliche Verschlüsselung über das Internet übertragen. Mehr als zwei Drittel der Betreiber hatten Drittanbieter-Software zur Erstellung von Besucherstatistiken im Einsatz. Mehrheitlich wurde Google Analytics eingesetzt.[54] Trotz der auffallenden Defizite bei der Datensicherheit wurden wir im Anschluss an die Veranstaltung lediglich von einem einzigen Betreiber einer Internetseite angesprochen und um Unterstützung bei der datenschutzkonformen Ausgestaltung gebeten. Dies zeigt uns, dass unser bisheriger Ansatz der blossen Information und Sensibilisierung zwar geschätzt wird, jedoch können wir die von uns gewünschten Ergebnisse – nämlich den gesetzeskonformen Umgang mit Personendaten – nicht erzielen.

Die Liechtensteinische Treuhandkammer organisierte eine **Veranstaltung** zum Thema **«Privatsphäre in Zeiten von Big Data und Datenaustausch»**, die etliche Aspekte rund um die Privatsphäre abdeckte.[55] Nach verschiedenen interessanten Vorträgen fand eine Podiumsdiskussion statt, an der wir vertreten waren. Bei den Vorträgen wurden teils ernüchternde Aussagen über den gegenwärtigen Schutz der Privatsphäre vor allem auf Grund der technischen Entwicklungen gemacht. Insbesondere wurde die Frage gestellt, ob es Zeichen dafür gäbe, dass sich dieses «Pendel», das sich von der Privatsphäre wegbewegte, kehren könnte. Generelle und wichtige Anzeichen einer «Gegenbewegung» sehen wir in der klaren *europäischen Rechtsprechung* der letzten Jahre, welche die Privatsphäre stützte (Stichwort: Vorratsdaten, Google Spain und Safe Harbor) sowie in der europäischen Datenschutzreform. Grundsätzlich ist *jeder selbst gefordert*, auf seine Privatsphäre zu achten.[56] Geradezu eine vorbildhafte Rolle nahm diesbezüglich Max Schrems ein, der sich im Safe-Harbor-Fall gerichtlich gewehrt und erreicht hatte, was weder europäische Regierungen noch die Europäische Kommission vorher geschafft hatte, nämlich entscheidende Schritte in Bezug auf den Datenschutz in den USA einzuleiten.

4.2 Veröffentlichungen in den Medien

Der Europäische Gerichtshof fällte wiederum ein bedeutendes Urteil, das als Meilenstein gilt. Es ging um die Frage, ob das sogenannte **Safe-Harbor-Abkommen** zwischen der Europäischen Kommission und den USA den europäischen Anforderungen entspricht (dieses Abkommen stellte

52 http://www.llv.li/#/112156/aufsatze.
53 Ein Muster findet sich unter http://www.llv.li/#/11884/datenschutzerklarung-fur-internetseitenbetreiber.
54 Siehe Ausführungen zu Google Analytics unter 2.1.
55 Die Folien können hier heruntergeladen werden: http://thk.li/.
56 Siehe dazu die Tipps und Hilfsmittel auf unserer Internetseite: http://www.llv.li/#/1299/selbstdatenschutz.

bis anhin eine zentrale Grundlage für den Datenaustausch mit US-Unternehmen dar). Dabei wurde nicht das Abkommen an sich kritisiert, sondern die Möglichkeit für US-Behörden, *uneingeschränkt auf Daten* bei US-Unternehmen *zugreifen* zu können. Ein solcher Zugriff ohne Einschränkungen ist sehr problematisch. Das Problem wurde noch dadurch verschärft, dass betroffene Personen keine Möglichkeit hatten, den Rechtsweg zu beschreiten und ihre *Rechte einzufordern*. Zu diesem letzteren Punkt heisst es in der Pressemitteilung des Gerichtshofs: «Eine solche Möglichkeit ist dem Wesen eines Rechtsstaates inhärent.» Zu diesem Fall erhielten wir Anfragen vom Radio. Zudem veröffentlichten wir einen Gastbeitrag in einer Tageszeitung[57] und aktualisierten unsere Internetseite.

Als Reaktion auf die Veröffentlichung unserer Empfehlung zum Internet der Dinge wurden wir von der Berliner Datenschutzrunde[58] angefragt, einen Beitrag für deren Blog zu erstellen. Unser Beitrag mit dem Titel **«Ist der Datenschutz beim Automatischen Informationsaustausch über Finanzkonten (AIA) gewährleistet?»** wurde am 17. August auf dem Blog veröffentlicht.[59] In diesem Beitrag wird der aktuelle Stand zur Datenschutzdiskussion wiedergegeben. Darin werden Parallelen zur Vorratsdatenspeicherung aufgezeigt und dementsprechend darauf hingewiesen, dass die entsprechende Rechtsprechung des EuGH zu beachten ist. Somit sind die Fragen eines klar definierten Zugriffs, der Aufbewahrungsdauer, der Datensicherheit und der unabhängigen Kontrolle im Fall eines Datentransfers in ein Drittland zu beantworten. Der Beitrag kommt zum Ergebnis, dass diese Fragen allesamt nicht genügend beantwortet sind.

Mit einem Presse-Beitrag zu **Smartphones** machten wir darauf aufmerksam, dass ein potenzielles Überwachungswerkzeug Einzug in die intimsten Bereiche des privaten Lebens der Nutzer gefunden hat.[60] Den *Einsatzmöglichkeiten von Smartphones* sind zusammen mit den sogenannten Wearables, wie beispielsweise Fitness-Armbänder oder Kleidung mit Sensoren, die Daten aufzeichnen und mit einem Smartphone austauschen können, *kaum Grenzen* gesetzt. Die Funktionalität ergibt sich insbesondere durch die installierten Apps. Diese können in vielen Fällen auf gespeicherte persönliche Daten wie Kontakte, SMS, Kalendereinträge usw. zugreifen. In den jeweiligen Stores finden sich deshalb auch zahlreiche Apps, die es auf die Daten der Nutzer abgesehen haben. Daher sollten Apps nur aus vertrauenswürdigen Quellen heruntergeladen werden. Kundenrezensionen auf dem Internet können bei der Wahl hilfreich sein und Hinweise auf schädliche oder nutzlose Apps geben. Weiter sollten Apps gelöscht werden, wenn sie nicht mehr benötigt werden; so wird Speicherplatz freigegeben und die Angriffsfläche reduziert. Unter bestimmten Umständen ist auch eine Rückgabe von Apps möglich. Ebenfalls sollten Bluetooth, WLAN und andere Schnittstellen deaktiviert werden, wenn sie nicht benötigt werden. Display-bzw. Tastatursperre und SIM/PIN-Sperre schützen vor unberechtigtem Zugriff. Die App-Entwickler sind verpflichtet, Informationen zur Datenbearbeitung in Form von Datenschutzerklärungen bereitzustellen. Nutzer sollten diese lesen.[61]

In der **Landesverwaltung** wurde 2015 eine **neue Mitarbeiterzeitung** geschaffen, die fünf Mal jährlich an sämtliche Mitarbeiter versandt wird. Wir bekamen die Möglichkeit, diesen Kanal regelmässig mit kurzen Sicherheitstipps zur Sensibilisierung zu nutzen. So wiesen wir in der ersten Ausgabe auf die Gefahren bei der Nutzung von *unverschlüsselten WLAN-Netzen* hin. Die über WLAN übertragenen Daten können mit wenig technischem Aufwand von jeder Person in Reichweite des Netzes abgefangen und mitgelesen werden. Der Tipp: Stets verschlüsselte WLAN-Verbindungen wählen, zu erkennen am Sicherheitsschloss-Symbol.[62] In einer weiteren Ausgabe thematisierten wir den Messenger *WhatsApp*. Seit 2014 gehört er zu Facebook. Nachrichten, Bilder und Videos können zwischen zwei Personen oder auch in Gruppen ausgetauscht werden. Ob und wie oft man WhatsApp nutzt, will der Nutzer unter Umständen lieber für sich behalten. Doch selbst wenn man alle Datenschutz-Optionen ausreizt, verrät WhatsApp zum Beispiel den Online-Status seines Nutzers – und zwar jedem, der die Rufnummer kennt. So kann mühelos auf das Nutzungsverhalten und potenziell sogar auf den Tagesablauf des Überwachten geschlossen werden. In diesem Zusammenhang beraten wir

57 http://www.llv.li/files/dss/pdf-llv-dss-volksblatt-gastkommentar-eugh-urteil-safe-harbor-20151010.pdf.

58 Die Berliner Datenschutzrunde ist nach eigenen Angaben «eine Multi-Stakeholder-Plattform, die aus zivilgesellschaftlichen Organisationen, Unternehmen und wissenschaftlichen Einrichtungen besteht. Als parteiunabhängige Datenschutzplattform setzen wir uns für ein modernes Datenschutzrecht ein, welches Privatsphäre in einer digitalisierten Welt schützt und datengetriebene Innovation ermöglicht».

59 https://www.berliner-datenschutzrunde.de/node/186.

60 Presse-Beitrag unter http://www.llv.li/files/dss/pdf-llv-dss-pece-2015-03-supertrend-smartphone.pdf.

61 Weitere Informationen auf unserer Internetseite unter http://www.llv.li/#/1619/mobile-datenbearbeitung.

62 Tätigkeitsbericht 2014, 4.1.

gerne über Alternativen und zeigen Wege der «unbeobachteten» Kommunikation.

Auf Anfrage der **Sektion Informatik der Wirtschaftskammer** (proIT) arbeiteten wir bei zwei Beiträgen für deren Mitglieder mit. Ein Beitrag sensibilisiert *allgemein für den Schutz der Privatsphäre*, wobei ein Überblick über verschiedenste technische Themenbereiche des Datenschutzes gegeben wurde, die für proIT-Mitglieder im eigenen Unternehmen relevant sein könnten. In einem zweiten Beitrag beantworteten wir Fragen bezüglich *«Programm Update Services via Internet»*. Diese Thematik ist deshalb datenschutzrechtlich relevant, weil Kundendaten abgefragt, gespeichert und zu Kontrollzwecken, beispielsweise für die Lizenzierung von Software, ausgewertet werden. Beide Beiträge wurden auf der Internetseite von proIT veröffentlicht.[63]

Immer mehr Unternehmen nutzen die Möglichkeit der Auftragsdatenbearbeitung, um sich besser auf ihr Kerngeschäft konzentrieren zu können. Für ein Unternehmen spielt es heutzutage vielfach keine Rolle, ob der eigene oder ein weit entfernter Computer eine Aufgabe löst. Cloud Computing eröffnet hier grenzenlose Möglichkeiten. Doch aus Datenschutzsicht ist diese Entwicklung nicht ganz unproblematisch.[64] Für ein Magazin fassten wir die wesentlichen Punkte betreffend **Outsourcing und Cloud Computing** zusammen. So muss beispielsweise beachtet werden, dass die Dateninhaber und somit die Unternehmen bei einer Auslagerung der Daten weiterhin die *Verantwortung* für diese *tragen* und diese auch nicht an einen Dienstleister abgeben können. Im Falle einer rechtswidrigen Datenbearbeitung haftet grundsätzlich der Dateninhaber gegenüber jenen Personen, deren Daten in der Cloud sind. Ebenso muss die *Zusammenarbeit* mit einem Cloud-Anbieter *vertraglich geregelt* werden. Bereits bei der Suche nach einer geeigneten IT-Lösung oder einem Geschäftspartner spielt Vertrauen eine entscheidende Rolle. Unternehmen sollten sich von den vermeintlich unbegrenzten Chancen des Cloud Computing nicht blenden, aber auch von den Gefahren und Risiken nicht völlig abschrecken lassen. Vor einer Entscheidung über die Auslagerung der Datenbearbeitung an Dritte sollte jedenfalls im Rahmen einer *Risikoanalyse* die Organisationsstruktur und Funktionsweise der Cloud genauestens analysiert werden.[65] Ganz generell ist auch hier darauf hinzuweisen, dass Cloud-Lösungen amerikanischer Anbieter seit dem Safe-Harbor-Urteil des EuGH höchst problematisch sind. Europäische oder liechtensteinische Lösungen im Sinne des Datenstandorts Liechtenstein sollten bevorzugt werden.

4.3 Internetseite

Auf unserer **Internetseite** informieren wir regelmässig über aktuelle Themen, die für die Öffentlichkeit relevant sind. Die folgenden Themen sind nicht abschliessend und können an einer anderen Stelle dieses Berichts beschrieben werden.

«Smarte Dinge» begegnen uns in zahlreichen Lebensbereichen, wie beispielsweise in unseren Häusern, Autos, im Arbeitsumfeld oder in der alltäglichen Kommunikation. Sie scheinen unser Leben zu vereinfachen. So können im Gesundheitsbereich oder im Bereich Energie vernetzte Geräte unser Verhalten im positiven Sinn verändern: Wir leben gesünder und reduzieren unseren Energieverbrauch. Auf der anderen Seite dürfen die Auswirkungen auf die Privatsphäre der Betroffenen nicht unbeachtet bleiben. Durch den Einsatz «smarter Dinge» entstehen immer grössere Datenmengen, die gespeichert und ausgewertet werden. Sei es, um «nur» umgebungsspezifische Daten des Nutzers zu messen oder gezielt dessen Gewohnheiten zu beobachten und zu analysieren. Mit dem Internet der Dinge finden potenzielle Überwachungswerkzeuge Einzug in die intimsten Bereiche des privaten Lebens der Nutzer. Wir haben dies zum Anlass genommen, eine **Empfehlung zum Internet der Dinge** auszuarbeiten und zu veröffentlichen.[66] Der Fokus wird dabei auf die drei Bereiche *Wearable Computing*[67]*, Quantified Self*[68] *und Heimautomatisierung*[69] gelegt. Das Dokument enthält neben allgemeinen Empfehlungen, Empfehlungen für

63 http://www.pro-it.li/.

64 Tätigkeitsbericht 2011, 1.6 (Finanzbereich) und 1.8 (Bereich Bildung) sowie Aufsatz mit dem Titel «Datenschutzrechtliche Chancen und Risiken von Cloud Computing» von Philipp Mittelberger und Gabriele Binder, in: Jus & News 2011/2, S. 163 ff.

65 Vgl. http://www.llv.li/#/1584/cloud-computing.

66 http://www.llv.li/files/dss/pdf-llv-dss-empfehlung-zum-internet-der-dinge.pdf.

67 Wearable Computing bezieht sich insbesondere auf Alltagsgegenstände, beispielsweise Armbanduhren oder Brillen sowie Kleidung, deren Funktionalität durch den Einbau von Sensoren erweitert wird.

68 Dinge und Softwarelösungen im Zusammenhang mit Quantified Self unterstützen die Nutzer bei der Aufzeichnung und Analyse der eigenen personenbezogenen Daten. Die Nutzer sind vor allem an einer Auswertung – meist über einen längeren Zeitraum – ihrer persönlichen, gesundheitlichen oder sportlichen Gewohnheiten interessiert.

69 Beispielsweise mit dem Internet verbundene Glühbirnen, Thermostate, Rauchmelder, Wetterstationen, Waschmaschinen oder Backöfen, die teilweise gar die Möglichkeit des Fernzugriffs über das Internet bereitstellen.

Gerätehersteller, App-Entwickler und Nutzer. Sie orientiert sich an verschiedenen Stellungnahmen der WP 29: beispielsweise jene zum Internet der Dinge[70], der Stellungnahme zu Apps auf intelligenten Endgeräten (engl. smart devices)[71] sowie der Stellungnahme zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten[72]. Auch der Datenschutztag 2015 stand unter dem Titel «Internet der Dinge».[73]

Im Zuge der Vorbereitung für die Schengen-Evaluation (siehe unten, Internationale Zusammenarbeit) wurden die Informationen auf der Internetseite komplett überarbeitet. Sämtliche Informationen sind jetzt zweisprachig vorhanden.[74]

70 Artikel-29-Datenschutzgruppe, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, angenommen am 16. September 2014 (WP 223), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_de.pdf.

71 Artikel-29-Datenschutzgruppe, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, angenommen am 27. Februar 2013 (WP 202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf.

72 Artikel-29-Datenschutzgruppe, Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, angenommen am 16. Mai 2011 (WP 185), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_de.pdf.

73 Siehe unter 4.1.

74 http://www.llv.li/#/1189/schengendublin.

5. WEITERE AUFGABEN

Am 1. Februar 2014 trat die Verordnung über die **Datenschutzzertifizierungen** in Kraft.[75] Hersteller von Datenbearbeitungssystemen oder -programmen sowie private Personen oder Behörden, die Personendaten bearbeiten, können ihre Produkte, Systeme, Verfahren sowie ihre Organisation einer Bewertung durch anerkannte, unabhängige Zertifizierungsstellen unterziehen und ein Datenschutzgütesiegel erwerben. Damit können Unternehmen und Behörden nach aussen klar sichtbar machen, dass das Thema Datenschutz einen hohen Stellenwert geniesst. Wir sehen in einem solchen Gütesiegel einen *möglichen Wettbewerbsvorteil* und ein wichtiges, *Vertrauen schaffendes Element*. Zertifizierungsverfahren führen zu einer Stärkung der Selbstverantwortung der Datenbearbeiter und tragen dazu bei, den Datenschutz zu fördern. Wir waren diesbezüglich mit mehreren interessierten Unternehmen in Kontakt. Wir waren diesbezüglich mit mehreren interessierten Unternehmen in Kontakt. Bis Ende 2015 wurde jedoch *noch kein Datenschutzgütesiegel* vergeben. Hier müssen weitere Anreize oder bei sensiblen Datenbearbeitungen gar Verbindlichkeiten geschaffen werden. Als Beispiel können hier die Datenannahmestellen nach dem Krankenversicherungsgesetz (KVG) genannt werden. So muss jede Kasse über eine Datenannahmestelle verfügen, welche nach dem DSG oder nach einem anderen gleichwertigen und vom Amt für Gesundheit anerkannten Gütesiegel zertifiziert ist. Wir haben eine Liste der zertifizierten Datenannahmestellen auf unserer Internetseite veröffentlicht.[76] Weitere Möglichkeiten sehen wir im Kommunikationsgesetz (KomG) etwa bei der Bearbeitung von Vorratsdaten oder im Finanzbereich beim Austausch von Steuerdaten.

75 https://www.gesetze.li/konso/2013.403.

76 http://www.llv.li/#/113189/drg-datenannahmestellen.

6. INTERNATIONALE ZUSAMMENARBEIT

6.1 Artikel-29-Datenschutzgruppe

Im Rahmen des **automatischen Austauschs von Steuerdaten** (AIA) hatte die WP 29 im Vorjahr der OECD und der Europäischen Kommission ein *Schreiben* zukommen lassen und Bedenken geäussert. Die Kommission bat die WP 29 um die Schaffung von Richtlinien, damit die jeweiligen Abkommen und Gesetze den Datenschutz angemessen berücksichtigen.[77]

Folgende Aspekte sind hier hervorzuheben:

- Als Folge veröffentlichte die WP 29 ein *«Statement»*, das sich an die nationalen Gesetzgeber richtet.[78] In diesem Statement wird betont, dass die Einhaltung der *Verhältnismässigkeit* und der *Zweckgebundenheit* zentral ist. Dies auch, da ein massenhafter Austausch von Daten grössere Sicherheits- und Haftungsrisiken beinhaltet. Deshalb wird ein Dialog mit den Datenschutzbehörden empfohlen und unter anderem ein *Fragebogen* an die zuständigen Behörden ausgearbeitet. Bei der Ausarbeitung dieses Fragebogens konnten wir einen aktiven Beitrag leisten und insbesondere bewirken, dass der Bezug zum Urteil des EuGH zu den Vorratsdaten verstärkt wurde. Damit sollte der Fragebogen an sich mehr Gewicht bekommen. In diesem Statement erinnert die Gruppe an die erste Evaluation vom September 2014,[79] die nach wie vor Gültigkeit hat.[80]
- Die Hauptarbeit zum AIA wurde in der *Financial Matters Subgroup* geleistet. Aufgrund der Wichtigkeit des Themas nahmen wir ausnahmsweise an dieser Subgroup teil und konnten bewirken, dass die Kommission um Stellungnahme zu diesem kritischen Expertenbericht gebeten wurde.
- Im genannten «Statement» wurde die Kommission auch aufgefordert, ein Privacy Impact Assessment (PIA) durchzuführen, worauf keine Reaktion erfolgte. Auf unsere Initiative wurde die Kommission daran erinnert.
- Die genannten *Richtlinien* stützen sich insbesondere auf den Fragebogen[81] und weisen auf die Wichtigkeit des Datenschutzes hin. Diese Richtlinien, bei deren Erarbeitung wir ebenfalls aktiv mitarbeiteten, sind auf unserer Internetseite verfügbar.[82] Inhalt dieser Richtlinien sind die Datenschutzkriterien, die beim AIA zu berücksichtigen sind, sei es innerhalb der EU oder in Bezug auf ein Drittland.

Als Reaktion auf das **Safe-Harbor-Urteils** des EuGH kündigte die WP 29 in einer ersten Pressemitteilung an, das Urteil zu analysieren, um die Folgen auf den Auslandsdatentransfer beurteilen zu können.[83] In einer weiteren Pressemitteilung weist sie darauf hin, dass die Massenüberwachung ein zentrales Element des Urteils war. Dieses Problem könne nur gelöst werden, indem *Verhandlungen mit den USA* zu einem Ergebnis führen, welches das Urteil umsetzt. Eine *Lösung* müsse *bis Ende Januar 2016* gefunden werden. In der Zwischenzeit können alternative Transfermechanismen wie Binding Corporate Rules oder Standardvertragsklauseln weiterhin verwendet werden. Sollte bis zu diesem Datum keine angemessene Lösung gefunden werden, wird mit kollektiven Durchsetzungsmassnahmen gedroht.[84]

Der Einsatz von **Minidrohnen** nimmt kontinuierlich zu. Deshalb ist es wichtig, für ausreichend Schutz vor einer missbräuchlichen Nutzung zu sorgen, ohne den sinnvollen und vorteilhaften Einsatz von Drohnen einzuschränken. Die WP 29 fordert in einer Stellungnahme die Regelung des Einsatzes von Drohnen auf nationaler und europäischer Ebene. Eine der möglichen Massnahmen wäre, zur leichteren Identifikation der Betreiber von Drohnen elektronische Kontrollschilder einzuführen. Wir erstellten eine

77 Tätigkeitsbericht 2015, 6.1.
78 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp230_en.pdf.
79 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140918_letter_on_oecd_common_reporting_standard.pdf.pdf.
80 Auch ein *Expertenbericht* der Europäischen Kommission kam unter anderem zum Schluss, dass es beim automatischen Austausch von Steuerdaten ein Problem mit der Verhältnismässigkeit gibt. In diesem Bericht wurde ausserdem auf das Problem hingewiesen, dass Daten möglicherweise nicht im gewünschten Ausmass geschützt sind, wenn sie in Drittländer gelangen. Dieser Expertenbericht unterstützt die Meinung der WP 29, da er ebenfalls Parallelen zum genannten Urteil des EuGH zieht und damit auch die Wichtigkeit der Beachtung der Privatsphäre und des Datenschutzes betont. Der Expertenbericht kann hier heruntergeladen werden: http://ec.europa.eu/taxation_customs/resources/documents/taxation/tax_cooperation/mutual_assistance/financial_account/first_report_expert_group_automatic_exchange_financial_information.pdf.
81 Tätigkeitsbericht 2015, 6.1.
82 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.
83 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151006_wp29_press_release_on_safe_harbor.pdf.
84 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

Zusammenfassung dieser Stellungnahme und veröffentlichten sie auf unserer Internetseite.[85]

Ziel der Datenschutzreform in Brüssel ist unter anderem die Schaffung von Rechtssicherheit und -einheitlichkeit in Europa. Die Datenschutzbehörden des EWR haben, auf Grund der bisherigen Richtlinie, teils unterschiedliche Zuständigkeiten und Kompetenzen. Diese Unterschiede, aber auch die Gemeinsamkeiten, kommen immer wieder an den Sitzungen zum Vorschein. Es wurde beschlossen, diese Gemeinsamkeiten und Unterschiede näher zu beleuchten und, wenn möglich, Schlussfolgerungen daraus zu ziehen. In diesem Sinne wurde ein sehr ausführlicher **Fragebogen zu den Zuständigkeiten und Kompetenzen** der einzelnen Datenschutzbehörden verschickt, den wir ebenfalls beantworteten. Damit sollen weitere Synergien geschaffen werden, die gerade kleinen Datenschutzbehörden, wie wir es sind, zugutekommen sollten.

6.2 Europarat

Der **Konventionsausschuss** beschäftigte sich mit verschiedenen Themen wie unter anderem der *Revision der Datenschutzkonvention.* Dabei wurde insbesondere der Entwurf eines erläuternden Berichtes zur neuen Konvention behandelt. Ebenso war der AIA ein Thema, bei dem die Verhältnismässigkeit oder der Schutz in Drittländern zentrale Elemente darstellen. Wir empfahlen zu untersuchen, ob diese beiden Elemente vor allem im Hinblick auf die europäische Rechtsprechung erfüllt sind. Der Vorschlag wurde gutgeheissen. Dabei sollte die OECD einbezogen werden, um zu einem koordinierten Ergebnis zu kommen.

6.3 Weitere internationale Zusammenarbeit

Seit Dezember 2011 ist Liechtenstein Mitglied des Schengenraums. Im Kern des Abkommens von Schengen steht das Schengener Informationssystem der zweiten Generation (SIS II). Im Zusammenhang mit der Schengen-Mitgliedschaft finden seither regelmässig **Evaluationen im Bereich Datenschutz statt. Nach 2011 wurden wir erneut evaluiert.** Da sich der Rechtsrahmen der Evaluationen inzwischen geändert hat, war es sinnvoll zur Vorbereitung unserer eigenen Evaluation zunächst an einer in einem anderen Land teilzunehmen. Bei dieser erneuten Evaluation ging es in erster Linie darum zu prüfen, ob die Empfehlungen der letzten Evaluation umgesetzt wurden.[86] Eine Empfehlung bestand beispielsweise darin, die breite Bevölkerung über ihre Rechte zu informieren.[87] Zudem hielten die Experten fest, dass wir in der Datenschutzstelle *zusätzliche Ressourcen* benötigen, um den neuen und zusätzlichen Aufgaben, wie insbesondere den regelmässigen Kontrollen des Schengener Informationssystems (SIS) und des Visa Informationssystems (VIS), nachkommen zu können.[88] Seit dem Schengenbeitritt 2011 veränderten sich unsere Ressourcen nicht, wodurch wir beispielsweise nicht mehr an VIS- und Eurodac-Sitzungen teilnehmen können. Bis zum Jahresende waren noch keine Ergebnisse der Evaluation verfügbar.

85 http://www.llv.li/#/117244/drohnen.

86 Tätigkeitsbericht 2011, 1.5.
87 Informationen in Deutsch und Englisch unter http://www.llv.li/#/1189/schengendublin.
88 Tätigkeitsbericht 2011. 1.5.

7. IN EIGENER SACHE

Im letzten Tätigkeitsbericht hatten wir erwähnt, dass wir generell bei unseren Tätigkeiten mehr in Richtung *Qualität statt Quantität* gehen wollten. Dabei hatten wir festgehalten, dass wir versuchen werden, mehr in die Tiefe zu gehen, und dies vor allem bei unseren Schwerpunktthemen. Wir kündigten eine **Straffung der vorhandenen Ressourcen** an, wodurch andere Tätigkeiten reduziert werden müssen.[89] Diese Straffung führte zu folgenden Ergebnissen:

- In der Vergangenheit hatten wir auf unserer Internetseite einen *Pressespiegel*, auf dem wir Themen sammelten und für die breite Öffentlichkeit aufbereitet darstellten. Diese Presseberichte stellten wir unkommentiert dar, was im Sinne unserer gesetzlichen Aufgabe der Information der Öffentlichkeit gedacht war. Diese Tätigkeit wurde gestrichen.
- Ebenso hatten wir den Kontakt zu den Datenschutzverantwortlichen der Behörden und der Unternehmen aktiv gesucht und jeweils eine Veranstaltung organisiert. Diese Veranstaltung war auch eine Gelegenheit, den Kontakt mit Datenschutzverantwortlichen mit denen wir weniger zu tun hatten, zu pflegen. Aus Ressourcengründen entschieden wir uns dafür, *keine jährlichen Veranstaltungen mit den Datenschutzverantwortlichen von Behörden* mehr durchzuführen.
- Im Rahmen der Revision des DSG erinnerten wir die Regierung an Praxisprobleme rund um die *Bewilligungspflicht der Videoüberwachung im öffentlichen Raum*. Die Erfahrung zeigt, dass dieser Vorschrift nicht im erwünschten Ausmass nachgekommen wird. Dies hat unserer Ansicht nach damit zu tun, dass es an einer Durchsetzungsbestimmung fehlt. Daher machten wir den Vorschlag, diesem unbefriedigenden Umstand ein Ende zu setzen. Wir orientieren uns nach Möglichkeit an Entwicklungen aus Brüssel, die im Hinblick auf die laufende Datenschutzreform zu erwarten sind. Dort spielt die Videoüberwachung keine Rolle. In den letzten Jahren sind schwerwiegendere Möglichkeiten des Eingriffs in die Privatsphäre entstanden, so dass bei Beibehaltung der gegebenen Ressourcen eine *Abschaffung der Bewilligungspflicht* Sinn machen würde.
- Die Genehmigungspflicht der Videoüberwachung im öffentlichen Raum betrifft grundsätzlich nicht nur Behörden und Unternehmen, sondern auch private Personen. So erhielten wir vereinzelt Beschwerden in Bezug auf eine *Videoüberwachung durch Nachbarn*. Auf Grund der fehlenden Durchsetzungsmöglichkeit und auf Grund unserer Ressourcenlage verwiesen wir diese Fälle auf den ordentlichen Rechtsweg.
- Im letzten Tätigkeitsbericht hatten wir noch über Tätigkeiten der *SIS Supervision Coordination Group*, der *Eurodac Supervision Coordination Group* und der *VIS Supervision Coordination Group* berichtet. Die Arbeit in diesen Gruppen können wir bestenfalls noch am Rande mitverfolgen. An Sitzungen der Eurodac- und der VIS-Gruppe können wir nicht mehr teilnehmen. An den SIS-Sitzungen nehmen wir aufgrund der höheren Relevanz vorläufig von Fall zu Fall teil.
- Zu guter Letzt werden wir unsere Stellungnahmen zu Vernehmlassungsvorlagen reduzieren müssen.

Nach wie vor sind wir bestrebt, wo möglich **Synergien** zu schaffen. Hauptpartner bei der Durchführung des Europäischen Datenschutztages sind die *Universität Liechtenstein* und der *IT Crowd Club Liechtenstein*. Weitere Partner sind das *IKT Forum Liechtenstein* sowie (ab 2016) der *Verein Sicheres Liechtenstein*. Mit diesen Partnern wurde vereinbart, dass nach dem Europäischen Datenschutztag weitere Veranstaltungen folgen sollen, an denen Themen zum Datenschutz öffentlich diskutiert werden. Neben den Synergien ist auch eine bessere Nachhaltigkeit das Ziel.

89 Tätigkeitsbericht 2014, 8.

8. AUSBLICK

Bisher lag unser **Hauptaugenmerk** darauf, über Belange des Datenschutzes **zu informieren und zu sensibilisieren**. Die Erfahrung hat jedoch gezeigt, dass dies nur beschränkt dazu führt, dass die gesetzlichen Bestimmungen eingehalten werden. Dieser Ansatz bedeutet eine *eigentliche Selbstregulierung*, wenn staatliche Aufsicht ausbleibt. Die Datenschutzrichtlinie enthält eine Bestimmung zur Selbstregulierung, die in Liechtenstein nicht übernommen wurde. Das Gesetz enthält aber Bestimmungen zur Aufsicht, womit der Gesetzgeber eine gewisse Aufsicht wünscht. Von prominenter Stelle wird immer wieder betont, dass sich der Staat auf seine Kernaufgaben konzentrieren müsse. Die Aufsicht ist eine staatliche Kernaufgabe. Dieser Wandel von der Information zur Aufsicht nimmt diesen Wunsch auf. Dies wurde auch in einer repräsentativen Umfrage bestätigt, die wir 2012 durchführen liessen. Da waren 83.85 Prozent der Ansicht, dass wir bei Verstössen gegen den Datenschutz handeln sollten.[90] In diesem Tätigkeitsbericht sind einzelne Punkte erwähnt, bei denen wir unsere Aufsichtsaufgaben wahrnahmen oder wahrnehmen mussten. Dies wird, nicht zuletzt im Rahmen der künftigen Datenschutz-Grundverordnung, ein Weg sein, den wir so oder so beschreiten müssen. In diesem Sinne möchten wir unseren *Fokus von der Information und Sensibilisierung wegnehmen* und *mehr im Bereich Aufsicht tätig sein*, wenn sich die Notwendigkeit dazu ergibt.

Neben den im DSG allgemein genannten Aufgaben, die wir vom Gesetzgeber erhielten, gibt es auch **Aufgaben in Spezialgesetzen**, denen wir nur in einem beschränkten Rahmen nachkommen können.[91] Auch im vergangenen Jahr wurden solche Aufgaben geschaffen: Im Rahmen der Abänderung *des Gesetzes über die Stabsstelle Financial Intelligence Unit* (FIUG) wurde mit Art. 10 ein indirektes Auskunftsrecht geschaffen, für das wir in der Praxis zuständig sein werden. Nach Art. 17 Abs. 4 AIA-Gesetz sind wir für die Überwachung der gesetzmässigen Bearbeitung von auszutauschenden Informationen zuständig. Nach Art. 18 Abs. 5 AIA-Gesetz hat uns die Steuerverwaltung über Sicherheitsverletzungen zu informieren. *Die 4. Geldwäscherei Richtlinie* sieht in Art. 30 ein Register über wirtschaftlich Berechtigte vor. Der Zugang zu den Angaben wirtschaftlicher Eigentümer erfolgt dabei «im Einklang mit den Datenschutzvorschriften». Was dies genau bedeutet, wird bei der Umsetzung dieser Richtlinie zu definieren sein.

Diese neu in Kraft getretenen gesetzlichen Bestimmungen werden wir im kommenden Jahr prioritär behandeln.

- Wir werden darum bemüht sein, mit der Stabsstelle Financial Intelligence Unit (SFIU) ein *Verfahren zur Handhabung des indirekten Auskunftsrechts* und zur damit verbundenen *Prüfung der Rechtmässigkeit der Datenbearbeitung bei der SFIU* zu definieren.

- Die Pflicht zur *Meldung von Sicherheitsverletzungen* ist neu in Liechtenstein. Wir erachten dies als eine wichtige Bestimmung, die auch mit der künftigen Datenschutz-Grundverordnung Pflicht wird. Wir werden zur Ausarbeitung eines Merkblattes für die Verpflichteten nach dem Gesetz den Kontakt zur Steuerverwaltung suchen.

- Das *Register über die wirtschaftlich Berechtigten* nach der 4. Geldwäscherei Richtlinie schlägt bereits vor der Umsetzung derselben in Liechtenstein hohe Wellen. Wir wurden ja schon verschiedentlich nach unserer Meinung angefragt und werden darauf achten, dass wir zu dieser sehr wichtigen Frage unseren Beitrag leisten können.

Letztes Jahr wurde durch das Amt für Statistik öffentlich angekündigt, dass es bei der Durchführung der **Volkszählung** durch uns begleitet wird.[92]

Das neue FIUG sieht vor, dass Daten nach längstens zehn Jahren zu löschen sind.[93] Wir wurden durch die Stabsstelle angefragt, ob wir sie bei einer ordnungsgemässen **Löschung von Daten** begleiten könnten.

Das Vorhaben der Regierung im Rahmen des **«Datenstandortes Liechtenstein»** ist ein komplexes Projekt, das noch nicht abgeschlossen ist. Wir sehen mögliche Folgen des Safe-Harbor-Urteils des EuGH vor allem in diesem Zusammenhang. Noch ist von Seite der WP 29 nicht klar, welche Folgen dieses Urteil in der Praxis haben wird. Als Beobachter in dieser Gruppe verfolgen wir diese Entwicklung mit

90 Die Details dieser Umfrage können im Tätigkeitsbericht 2012, 2.1, nachgelesen werden.
91 Z.B. Art. 16 des Gesetzes über das Zentrale Personenregister, Art. 76 Krankenversichertenverordnung, Art. 3b Zustellverordnung.
92 http://www.llv.li/#/116050.
93 Art. 8 Abs. 2.

Interesse. Auch die Möglichkeit, Lead Authority im Rahmen von *BCR-Verfahren* zu sein, wollen wir weiter näher prüfen. Dies stellt nämlich eine Lösung dar, bei der ein Mehrwert für Unternehmen geschaffen werden kann.

In den **Arbeitsgruppen** «Datenstandort», «Vorratsdatenspeicherung», AIA und der Fachgruppe Medienkompetenz werden wir weiterhin aktiv mitarbeiten, uns aber im Rahmen der ZPR-Kommission auf das unbedingt Notwendige beschränken.

Auch die bereits erwähnte **Datenschutz-Reform** in Europa steht kurz vor einem Abschluss. Erfahrungsgemäss wird es dauern, bis die beschlossene Grundverordnung in den EWR übernommen wird. Das Thema ist jedoch sehr komplex und wird vorwiegend in der *WP 29* behandelt. Wir werden die dortigen *Arbeiten* mit Interesse *verfolgen*.

Das erwähnte **Rechtsmittelverfahren**, und konkret die Umsetzung des Entscheides des StGH, wird weiterhin ein Thema sein.

Auch im kommenden Jahr werden wir mit bewährten Partnern wiederum an der **Lihga** teilnehmen und uns in diesem Rahmen um wertvolle Sensibilisierung bemühen.

Insgesamt nehmen die Aufgaben und Anforderungen weiterhin zu. Eine Wahrnehmung der gesetzlichen Aufgaben ist teils nicht mehr möglich. Wir sind weiterhin bestrebt, Prioritäten optimal zu setzen.

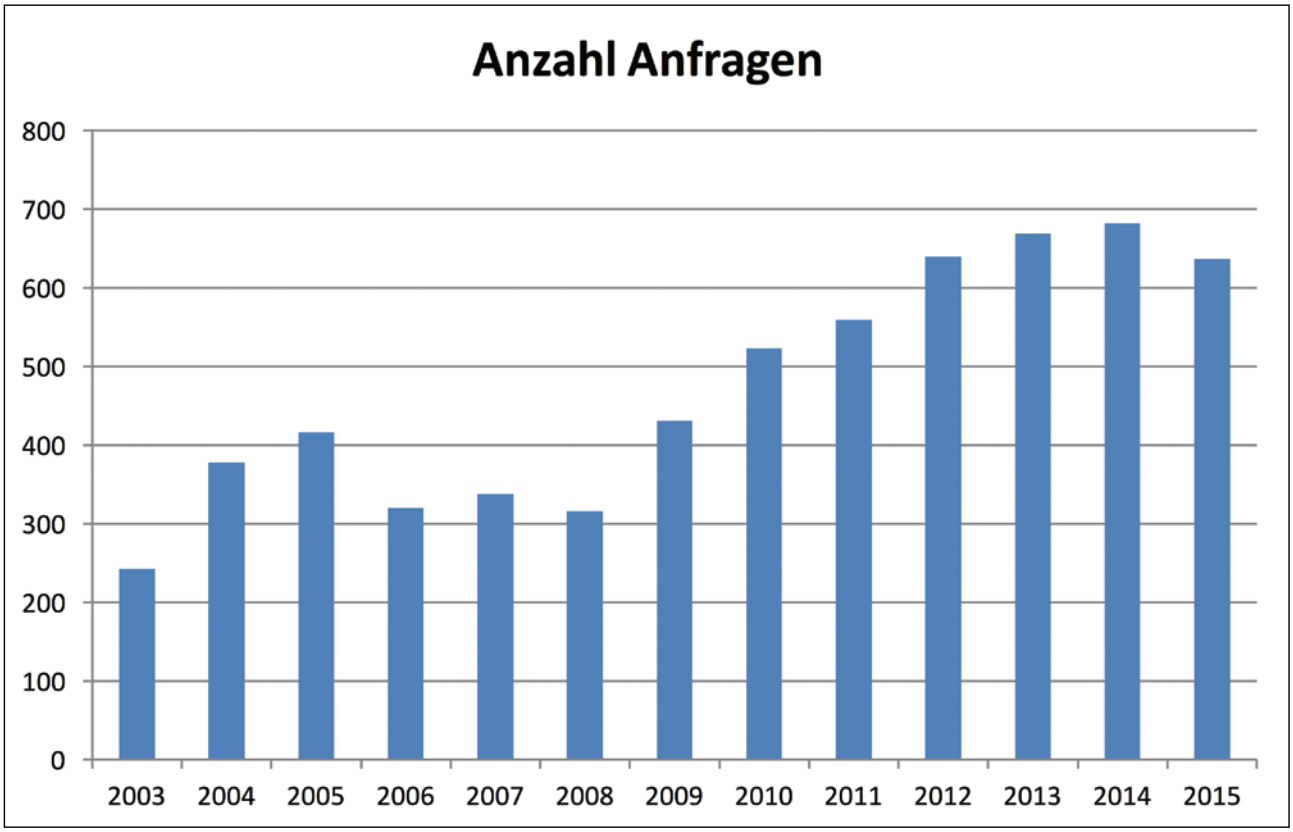
9. ANHANG

9.1 Anfragestatistik

Die Beratung privater Personen und Behörden ist eine Kernaufgabe. Im Berichtsjahr erhiel-ten wir insgesamt 637 Anfragen. Gegenüber dem Vorjahr bedeutet dies einen leichten Rückgang. Dieser leichte Rückgang kann teils damit erklärt werden, da es nun eine Gebüh-renpflicht für Gutachten und Stellungnahmen gibt. Einzelne Anfragen wurden nach Hinweis auf diese Gebührenpflicht zurückgezogen.

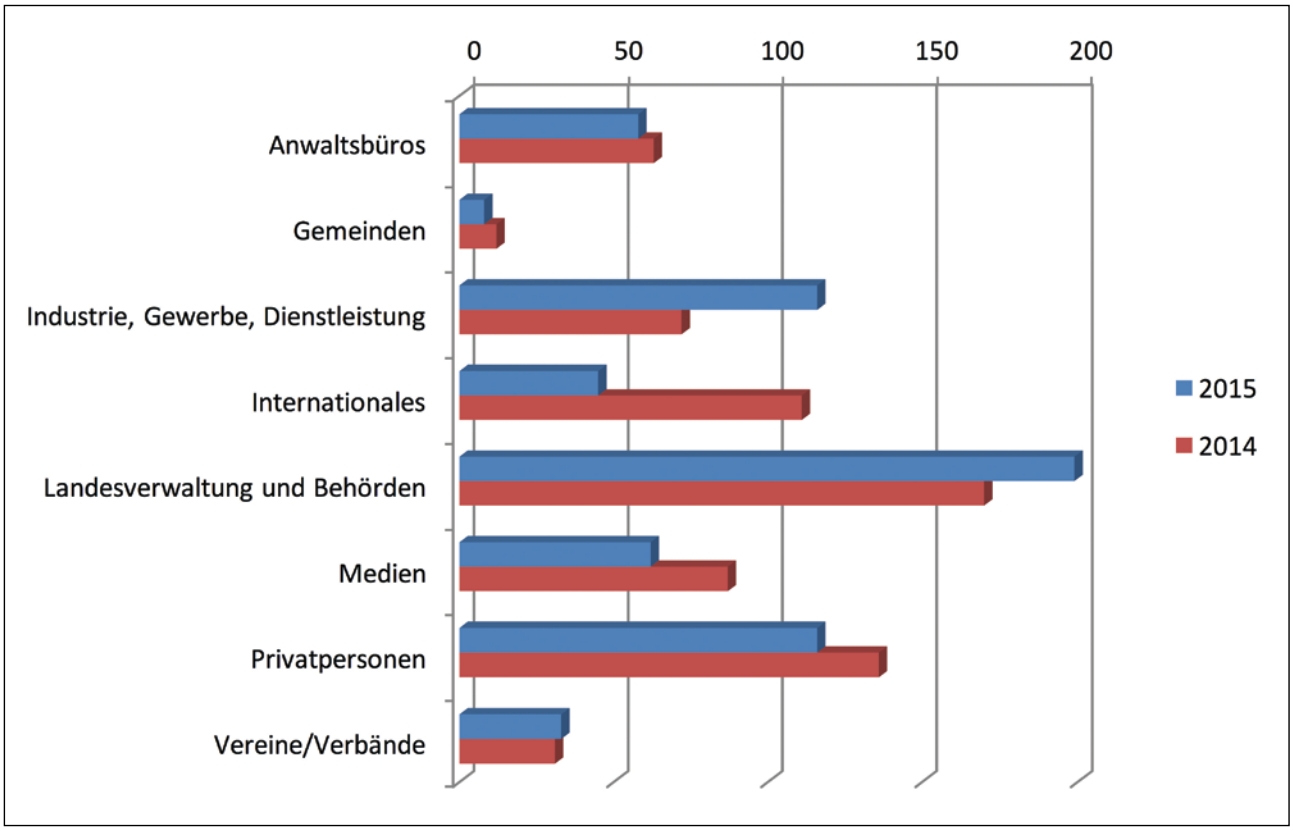
Anzahl Anfragen im Vergleich zu den Vorjahren

Die nachfolgende Abbildung zeigt die Entwicklung der Anzahl Anfragen über die vergangenen 13 Jahre:



Anzahl Anfragen pro Personengruppe

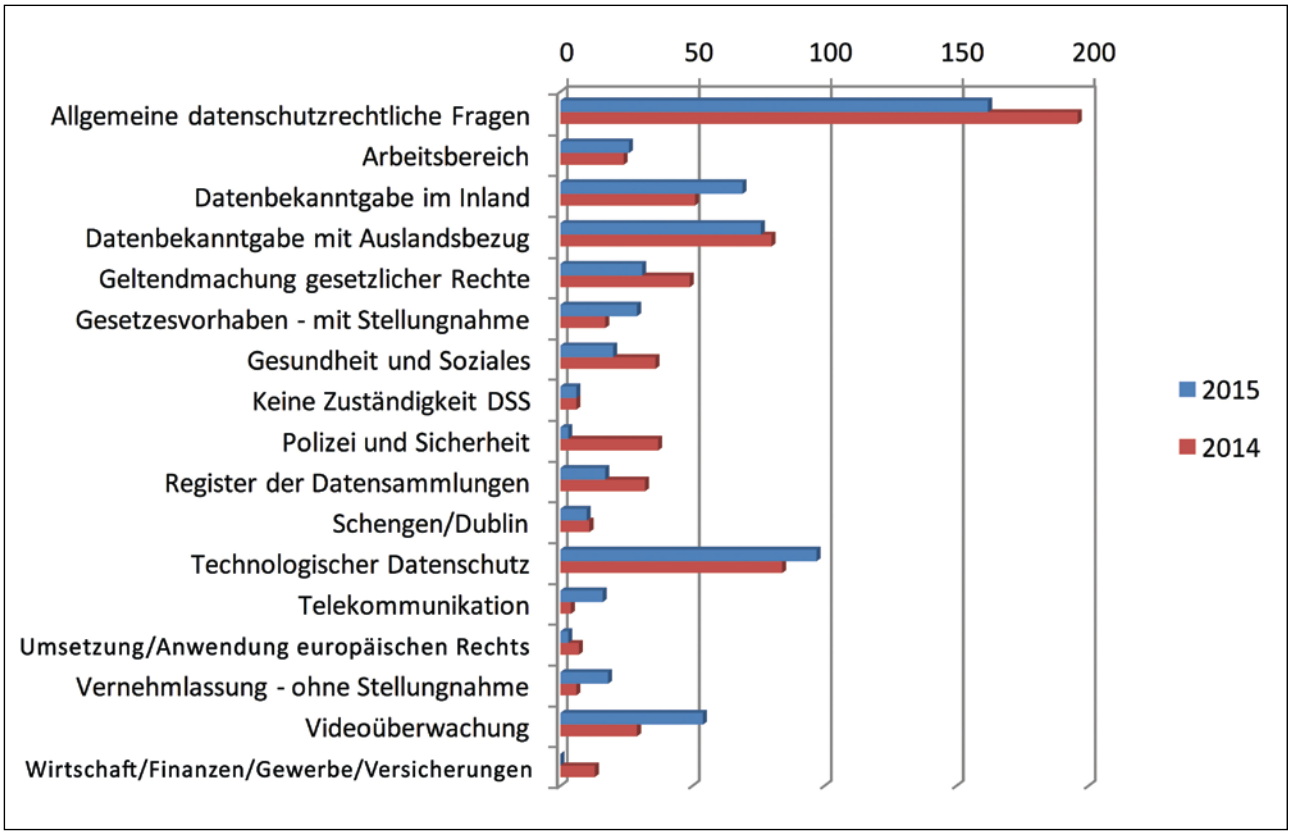
In der folgenden Abbildung ist ersichtlich, von welchen Personengruppen bzw. Organisationen die Anfragen eingegangen sind:



Die meisten Anfragen stammen nach wie vor von der Landesverwaltung und anderen Behörden. Die zweitmeisten Anfragen kamen von privaten Einzelpersonen und Unternehmen, wobei bei Unternehmen eine Zunahme von etwa 60 Prozent zu verzeichnen war. Rückläufig sind vor allem beantwortete Anfragen im Bereich Internationales, sodass insgesamt eine weitere Zunahme von inländischen Anfragen festzustellen ist. Anfragen ausländischer Datenschutzbehörden werden aus Ressourcengründen nur noch ausnahmsweise beantwortet und nur dann, wenn sie gezielt an uns gerichtet sind.

Anzahl Anfragen pro Sachgebiet

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



Die meisten Anfragen sind genereller Natur. Stark zugenommen haben Fragen im Bereich der Telekommunikation, was unter anderem auf die Entwicklungen im Bereich der Vorratsdatenspeicherung zurückzuführen ist. Ebenfalls zugenommen haben Anfragen zum technologischen Datenschutz und zur Videoüberwachung.

Anzahl Anfragen pro Personengruppe und Sachgebiet

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

	Anwaltsbüros	Gemeinden	Industrie, Gewerbe, Dienstleistung	Internationales	Landesverwaltung, Behörden	Medien	Privatpersonen	Vereine, Verbände
Datenschutz allgemein	7	1	30	11	31	37	35	10
Arbeitsbereich			18		3		5	
Datenbekanntgabe Inland	6	3			40		11	9
Datenbekanntgabe Auslandsbezug	25	2	22	3	14	2	8	
Geltendmachung gesetzlicher Rechte	2		1		4		24	
Gesetzesvorhaben					29			
Gesundheit/Soziales	1		8		8		2	1
Keine Zuständigkeit DSS					1		3	2
Polizei/Sicherheit	1				1	1		
Register der Datensammlungen	1		7		6			3
Schengen/Dublin				9	1			
Technologischer Datenschutz	3		18	22	29	7	10	8
Telekommunikation						13	3	
Umsetzung/Anwendung europäischen Rechts					1	2		
Vernehmlassungen ohne Stellungnahme					18			
Videoüberwachung	12	2	12		13		15	
Gesamtergebnis	58	8	116	45	199	62	116	33

9.2 Newsletter

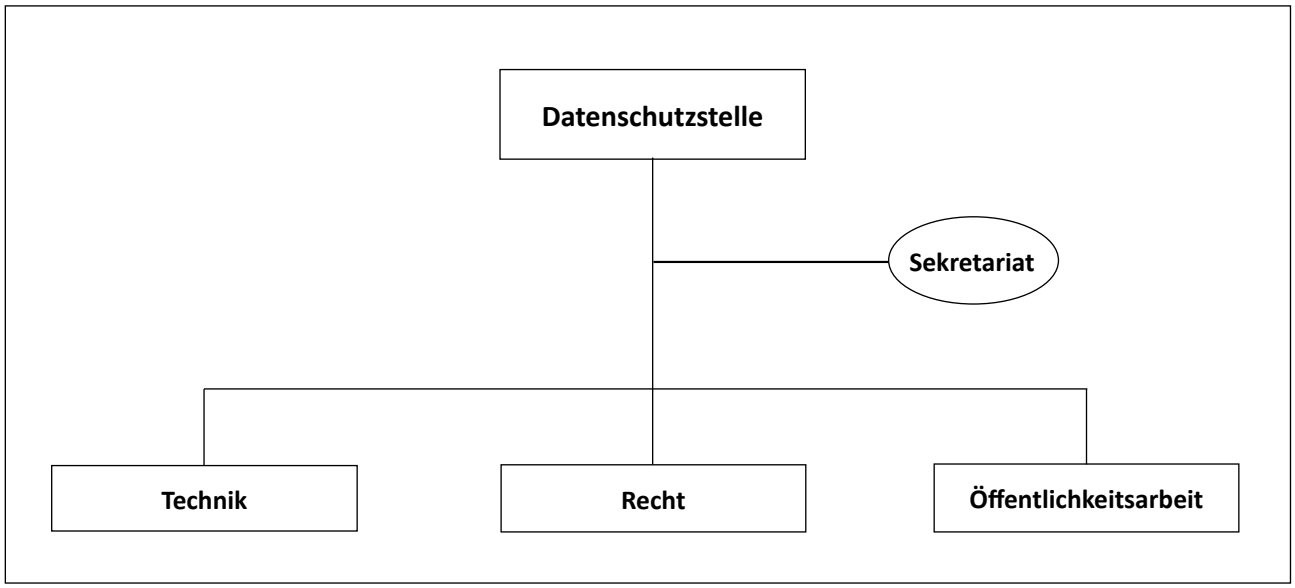
Über einen Newsletter informieren wir laufend über aktuelle Entwicklungen zum Datenschutz.[94] Im Jahr 2015 versandten wir 13 Newsletter; z. B. zum Thema Windows 10, zur EuGH-Entscheidung Safe Harbor, zu Drohnen, zum automatischen Informationsaustausch in Steuerangelegenheiten. Wir erreichten dabei im Januar 441 Abonnenten und konnten die Anzahl bis Dezember auf 514 Abonnenten steigern.

9.3 Veröffentlichte Publikationen

Folgende Publikationen wurden erstellt oder überarbeitet:[95]

- Empfehlung zum Internet der Dinge, Januar 2015 (neu erstellt)
- Expertenpapier: Datenschutz-Grundverordnung der Europäischen Union: Risikobasierter Datenschutz – eine Zwischenbilanz im andauernden Trilog-Verfahren der EU, Christine Wohlwend, elleta AG, August 2015 (neu erstellt)
- Handout Windows 10 Datenschutzeinstellungen
- «Ist der Datenschutz beim Automatischen Informationsaustausch über Finanzkonten (AIA) gewährleistet?» (neu erstellt)

9.4 Organigramm



94 Anmeldung zum Newsletter auf der Internetseite unter http://www.llv.li/#/49/.
95 Auf der Internetseite unter http://www.llv.li/#/12550/richtlinien.

DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Kirchstrasse 8
FL-9490 Vaduz

Telefon +423 236 60 90

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