DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Tätigkeitsbericht 2016

Datenschutzstelle des Fürstentums Liechtenstein

INHALTSVERZEICHNIS

1. EINLEITUNG

Dies ist unser 15. Tätigkeitsbericht.

Im letzten Jahr ging die Anzahl der **Anfragen** erneut etwas zurück. Diese rein quantitative Betrachtung wird durch die Komplexität verschiedener Fragen relativiert. Wie üblich werden einige Anfragen in unserem Tätigkeitsbericht erwähnt: Zu nennen sind primär Anfragen/Beschwerden, bei denen es um die Einhaltung der gesetzlichen Bestimmungen ging. Neben dem «WhatsApp Fasnachts Lesereporter» und einem Fall, den wir an die österreichische Datenschutzbehörde weiterleiteten, ging es um Auskunfts- und Löschbegehren. Weitere Fragen betrafen Drohnen, Dash-Cams oder etwa Fragen zur Umsetzung des Gesetzes über den Automatischen Informationsaustausch (siehe Kapitel 2.1).

Der Rückgang von Anfragen oder Beschwerden durch private Personen mag darin begründet sein, dass die gesetzlichen Regelungen betreffend die Entscheidungskompetenz nach wie vor verbessert werden sollten (was im Rahmen eines **Vernehmlassungsberichts** der Regierung aus dem Jahr 2015 zur Änderung des Datenschutzgesetzes vorgeschlagen worden war). Diese Entscheidungskompetenz wurde bis heute noch nicht eingeführt (siehe Kapitel 2).

Für einzelne Anfragen mussten wir Gebühren verlangen. Diese **Gebührenpflicht** sahen wir von Anfang an kritisch, da sie sich als kontraproduktiv erweisen kann. Deshalb sind wir für die Aufhebung dieser Gebührenpflicht (siehe Kapitel 7).

Im Rahmen des Gesetzgebungsprozesses gaben wir verschiedene **Stellungnahmen** ab. Speziell zu erwähnen ist hier die Einführung eines Bedrohungsmanagements, das auch im Landtag kontrovers diskutiert wurde (siehe Kapitel 2.2).

Bei der Umsetzung der **4. Geldwäsche-Richtlinie** wurden wir eingebunden. Speziell die Frage der Schaffung eines Verzeichnisses der wirtschaftlichen Eigentümer inländischer Rechtsträger (WB-Register) beschäftigte uns intensiv. Hierzu leisteten wir einen aktiven Beitrag. Aber auch die Datenlöschung und das neu eingeführte indirekte Auskunftsrecht bei der Stabsstelle Financial Intelligence Unit oder die Volkszählung 2015 beschäftigte uns (siehe Kapitel 2.5).

In unserem letzten Tätigkeitsbericht hatten wir erwähnt, dass wir inskünftig *weniger Wert auf die Information und Sensibilisierung* legen wollen. Von prominenter Stelle wird nämlich immer wieder betont, dass sich der Staat auf seine Kernaufgaben beschränken müsse. Die **Aufsicht** ist eine staatliche Kernaufgabe. Einige Aufsichtstätigkeiten werden in diesem Bericht erwähnt (siehe Kapitel 3).

Seit 2014 gibt es die Möglichkeit, ein **Datenschutz-Gütesiegel** zu erhalten. Letztes Jahr war es soweit. Das erste Siegel konnte verliehen werden (siehe Kapitel 5).

Ab Ende Mai 2018 gilt die **Datenschutz-Grundverordnung** (DSGVO) in jedem Fall für Unternehmen, die Waren oder Dienstleistungen in der EU anbieten.[1] Damit ist ein strenger Aufsichtsmechanismus verbunden. Ob wir im Rahmen der Aufsicht über liechtensteinische Unternehmen überhaupt eine Rolle spielen werden, ist derzeit noch offen.

Als **EWR-Mitglied** wird die DSGVO auch in Liechtenstein anwendbar sein, wenn es für «Binnenunternehmen» auch zu Verzögerungen kommen kann. Im Ausland wurde schon sehr viel über die DSGVO geschrieben. Es herrscht weithin Einigkeit, dass sie einen «Quantensprung» im Datenschutzbereich bewirkt, der sich auch auf uns auswirken wird. Wir trafen bereits erste Schritte zur Vorbereitung. Dazu sind Kontakte zu anderen Datenschutzbehörden und nach Brüssel Gold wert. Die entsprechenden Absätze zur DSGVO sind in diesem Bericht speziell hervorgehoben.

Die DSGVO stand im Rahmen unserer Mitarbeit bei der **Artikel-29-Datenschutzgruppe** im Fokus. Daneben konnten wir in Abstimmung mit der Regierung einen Vorschlag zum WB-Register unterbreiten, der in einem Schreiben an die Europäische Kommission berücksichtigt wurde (siehe Kapitel 6.1)

Im vergangenen Jahr erwähnten wir ebenfalls, dass bei uns erneut eine **Schengen-Evaluation** stattgefunden hatte. Da die Evaluation Ende 2015 erfolgte, gab es bis Redaktionsschluss des Tätigkeitsberichts 2015 noch keine Handlungsempfehlungen. Bis Ende 2016 ging immer noch kein offizieller Bericht ein. Somit änderte sich nichts daran, dass wir im Schengen-Bereich unseren Aufgaben nicht mehr nachkommen können.

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

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 April 2017

Dr. Philipp Mittelberger
Datenschutzbeauftragter

2. ALLGEMEINE ORIENTIERUNG UND INDIVIDUELLE BERATUNG

Die Ausrichtung auf «weniger ist mehr» galt auch im vergangenen Jahr. Insgesamt erhielten wir 591 Anfragen. Wie schon im Vorjahr war wieder ein Rückgang zu verzeichnen. Wie im Folgenden gezeigt wird, hat dies nichts mit einem abnehmenden Interesse für den Datenschutz zu tun. Im Gegenteil, wir konnten durch verschiedene Massnahmen erreichen, dass wir uns mehr auf **Qualität statt Quantität** konzentrieren konnten. Dazu gehört, dass wir weniger Vorträge und Schulungen halten. Zudem erwähnen wir immer wieder, dass Anfragen eines gewissen Ausmasses gebührenpflichtig sind. Dies führte dazu, dass Anfragen zurückgezogen (oder wohl erst gar nicht gestellt) wurden.

Auffällig ist, dass nach wie vor Behörden die meisten **Anfragen** stellen. Das Niveau entspricht dem aus dem Vorjahr. Aus dem Bereich Industrie/Gewerbe/Dienstleistung ist nach wie vor ein Anstieg zu verzeichnen. Anfragen von Medien gingen seit 2014 um gut 50% zurück und auch Anfragen von Privatpersonen sind rückläufig. Anfragen von Gemeinden sind seit Jahren praktisch vernachlässigbar. Über die Gründe dieser Entwicklungen kann nur spekuliert werden. Der Bereich Industrie/Gewerbe/Dienstleistung zeichnet sich offenbar durch eine weiterhin steigende Sensibilisierung aus. Was Medien angeht, kann nur festgestellt werden, dass es sehr oft öffentlichkeitswirksame Entwicklungen rund um den Datenschutz gäbe. Und der Rückgang bei Privatpersonen mag damit zu tun haben, dass unsere gesetzlichen Möglichkeiten nach wie vor sehr beschränkt sind. Gemäss einem Vernehmlassungsbericht aus dem Jahr 2015 sollte die Datenschutzkommission abgeschafft werden. In diesem Rahmen wurden wir angefragt, ob die Kompetenz zur Fällung von bindenden (exekutierbaren) Entscheidungen auf uns übertragen werden sollte. Mit dieser Erweiterung würden wir auch eher als klassische Behörde, eben mit Entscheidungsfunktion, wahrgenommen. Zudem wäre eine Aufwertung unserer Tätigkeit die Folge.

«Weniger ist mehr» gilt auch bei der folgenden Darstellung der Anfragen. Wir erhalten regelmässig Anfragen zu denselben Themen. Solche Anfragen werden im Folgenden nur erwähnt, wenn deren Beantwortung einen Mehrwert oder eine Ergänzung zu früher erwähnten Anfragen mit sich bringt. Insgesamt wollen wir die Menge an dargestellten Anfragen reduzieren.

Die Anfragen kommen aus verschiedenen Bereichen. Bei der Darstellung folgen wir der Gliederung in früheren Tätigkeitsberichten. Wenn sich keine neuen Anfragen in den einzelnen Themenbereichen ergaben, wird auf eine Darstellung verzichtet.

2.1. Anfragen

Wahrnehmung gesetzlicher Rechte[2]

Die Fasnacht ist seit jeher eine närrische Zeit, während der Viele anerkanntermassen in andere Rollen schlüpfen. Nicht ohne Grund wird die Fasnacht auch die «5. Jahreszeit» genannt. Dabei kommt es auch vor, dass Personen in einer Situation beobachtet werden können, die ihnen spätestens nach der Fasnacht eher peinlich sein kann. In Anbetracht dieser Lage sahen wir das Vorhaben eines **«WhatsApp Fasnachts-Leserreporters»** einer Landeszeitung kritisch. Rasch gingen Beschwerden ein. Dabei wurde die Frage gestellt, wie dieses Vorhaben mit dem «Recht auf das eigene Bild» vereinbart werden könnte. Auch wenn es heute viele Fotogalerien von Medien gibt, war das Besondere an diesem Vorhaben, dass es während der Fasnacht realisiert werden sollte und die Leser dazu aufgerufen wurden, Fotos zu machen, die sie dann über WhatsApp an die Zeitung schicken sollten. Wir wiesen die Zeitung darauf hin, dass uns schon von professionellen Fotografen immer wieder die Frage gestellt wurde, wie das «Recht am eigenen Bild» berücksichtigt werden muss.[3] Zwar wurde durch die Zeitung Wert darauf gelegt, dass die Einwilligung der Fotografierten gegeben sein müsse, doch stellte sich für uns die Frage, wie diese Einwilligung durch die Leserreporter in der Praxis beschafft

2 Fall zu iPads für den Unterricht, siehe unter 3.

3 Im Fall «Google Street View» hielt das Schweizerische Bundesgericht (BGE 138 II 346) unter anderem Folgendes fest: *« Das Recht am eigenen Bild ist das Selbstbestimmungsrecht, das vor widerrechtlicher Verkörperung des eigenen Erscheinungsbildes schützt […] Das Recht auf Achtung der Privatsphäre [soll] verhindern, dass jede private Lebensäusserung, die in der Öffentlichkeit stattfindet, wie zum Beispiel ein Abschiedskuss auf der Strasse oder die Beerdigung eines Menschen der Allgemeinheit bekannt wird… Der Einzelne soll sich nicht dauernd beobachtet fühlen, sondern - in gewissen Grenzen - selber bestimmen dürfen, wer welches Wissen über ihn haben darf bzw. welche personenbezogenen Begebenheiten und Ereignisse des konkreten Lebens einer weiteren Öffentlichkeit verborgen bleiben sollen.» In einer anderen Passage heisst es: «Die Veröffentlichung des individualisierenden, das heisst nicht rein zufälligen Bildes ohne Einwilligung des Betroffenen stellt immer eine Persönlichkeitsverletzung dar, und zwar unabhängig davon, ob bereits die Aufnahme unrechtmässig erfolgte […]. Auch wenn sie [diese Personen] nur zufällig auf den Bildern als sog. «Beiwerk» oder «Staffage» erscheinen, kann ihr Recht am eigenen Bild verletzt sein […]. Eine abgebildete Person kann ohne Rechtfertigung durch ein Informationsinteresse des Publikums ins Zentrum des Bildes gerückt oder mittels der Zoom-Funktion derart vergrössert werden, dass sie nicht mehr als untergeordneter Teil eines belebten Strassenbildes erscheint.»*

wird. Dementsprechend rieten wir dazu, *dass vor allem unkritische Fotos veröffentlicht werden sollten, wie die Gesamtsicht einer Veranstaltung, Fotos, auf denen klar ersichtlich ist,* dass die *Einwilligung (zum Beispiel durch ein Lächeln in die Kamera) klar gegeben ist oder maskierte und damit nicht erkennbare Personen.* Diese Vorschläge wurden entgegengenommen. Wir wiesen auch darauf hin, dass an die Eigenverantwortung der Leserreporter appelliert wird und dass diese Fotos nach der Fasnacht von der Internetseite gelöscht werden. Daraufhin gingen keine Beschwerden mehr bei uns ein. Da das ganze Vorhaben über WhatsApp realisiert wurde, stellte sich hier zudem die Frage des Datentransfers in die USA und damit die Datenschutzkonformität von Facebook, das ja WhatsApp gekauft hat. Wir warten diesbezüglich erst einmal ab, wie die Haltung anderer europäischer Datenschutzbehörden aussieht und prüfen mögliche weitere Schritte zu einem späteren Zeitpunkt.

Wir wurden angefragt, ob es rechtskonform ist, dass die **österreichische Zollbehörde** ungefragt Daten von Personen, welche beim österreichischen Zoll die **Mehrwertsteuerausfuhrbestätigung** einholten, an den **schweizerischen Zoll weitergibt.** Gemäss dem Abkommen zwischen der Europäischen Gemeinschaft und der Schweiz in Zollsachen und dem Zusatzprotokoll über die gegenseitige Amtshilfe im Zollbereich ist die Amtshilfe grundsätzlich nur auf Antrag möglich. Für die obige Anfrage ist das Abkommen und die österreichische Gesetzgebung, insbesondere auch das österreichische Datenschutzgesetz, massgebend. Deshalb wandten wir uns an die österreichische Datenschutzbehörde. Diese teilte uns mit, dass sie rechtliche Auskünfte aufgrund der gesetzlichen Zuständigkeit der Datenschutzbehörde nur im Zuge eines konkreten Verfahrens erteilen könne und gab keine inhaltlichen Auskünfte. Wir mussten demgemäss der *betroffenen Person mitteilen, dass sie sich selbst an die österreichische Datenschutzbehörde wenden müsse.*

Anfragen zu Auskunftsbegehren kommen immer wieder vor. Diese Problematik wird im Folgenden dennoch dargestellt, da das Auskunftsrecht das zentrale Recht nach dem Datenschutzgesetz (DSG) darstellt; es ist der Ausgangspunkt, um das Sperr-, Berichtigungs- oder Löschrecht geltend machen zu können. Wird einem Auskunftsbegehren nicht nachgekommen, stehen auch die genannten Folgerechte «in der Luft».[4] Die folgenden **zwei Fälle** zeigen uns bekannte **Probleme zur Praxis des Auskunftsrechts:**

- Im ersten Fall wurden wir darüber informiert, dass ein **Auskunftsbegehren** seitens bestimmter **Behörden nicht innert** der gesetzlich vorgesehenen **Frist** von 30 Tagen beantwortet worden sei. Die Auskunft sei zwar später noch erteilt worden, doch war sie aus Sicht der betroffenen Person unbefriedigend. In diesem Zusammenhang wurden wir angefragt, wie der *Rechtsweg bei verweigerter bzw. unvollständiger Auskunftserteilung* durch Behörden sei. Wir teilten der betroffenen Person mit, dass sie nach *Art. 38 DSG* gegen Verfügungen von Behörden *Beschwerde bei der Datenschutzkommission und gegen die Entscheidung der Datenschutzkommission bzw.* gegen die Entscheidung der Regierung (als Kollektivorgan) *Beschwerde beim Verwaltungsgerichtshof erheben* kann.
- Im zweiten Fall bekamen wir dieselbe Frage zum Rechtsweg von einer Person, die ein **Auskunftsbegehren** bei einem **Unternehmen** stellte und **von diesem keine Antwort** bekommen hatte. Bei der Bearbeitung von Personendaten durch Private ist der Rechtsweg im Vergleich zur Bearbeitung von Personendaten durch Behörden anders geregelt. Nach dem DSG sind für Klagen und einstweilige Verfügungen (sichernde Massnahmen) zum Schutz der Persönlichkeit die Art. 39 bis 41 des Personen- und Gesellschaftsrecht (PGR) massgebend.[5] Dementsprechend verwiesen wir die betroffene *Person auf den Zivilrechtsweg.*

Über den Ausgang dieser Fälle wurden wir nicht informiert. Ganz allgemein ist uns nicht bekannt, ob die Rechte der betroffenen Personen, vor allem das **Auskunftsrecht,** in der Praxis so gelebt wird, wie es vom Gesetzgeber und vom Europäischen Gerichtshof (EuGH) gedacht ist. Naturgemäss erfahren wir von jenen Fällen, in denen es Probleme gab. Da sich aber immer wieder ähnliche Fragen stellen, werden wir in Zukunft Personen, die sich diesbezüglich bei uns melden, explizit bitten, uns darüber zu informieren, ob ihrem Recht Genüge getan wurde. Sollte dies nicht der Fall sein, werden wir uns Massnahmen überlegen, damit die Rechte des DSG deren Bedeutung (zurück) erlangen.

In einem anderen Fall beschwerten sich verschiedene Personen darüber, dass ihre **Adressdaten** bei einem Unternehmen zu Werbezwecken ohne Einwilligung weitergegeben oder diese **trotz Löschbegehren nicht gelöscht** worden waren. Eine entsprechende Nachfrage bzw. Intervention bei diesem Unternehmen ergab hierbei, dass das Unternehmen

4 Tätigkeitsbericht 2009, 1.1.3., wo die *Rijekeboer*-Entscheidung des EuGH erwähnt wird.

5 Art. 37 Abs. 1.

anstelle der Löschung eine Sperrung der Daten vorgenommen hatte. Eine Sperrung kann dann angezeigt sein, wenn die Daten aufgrund gewisser Umstände weiter aufbewahrt werden müssen, obwohl diese unmittelbar nicht weiter benötigt werden. Gründe hierfür können gesetzliche Bestimmungen sein, Vertrags- oder Standespflichten oder schutzwürdige Interessen des Betroffenen. Ob hier zu Recht eine Sperrung statt einer Löschung der Daten gewählt wurde, konnten wir offenlassen. Denn eine Prüfung dieser Fälle zeigte, ähnlich wie bei der Videoüberwachung zwischen Nachbarn,[6] dass *das öffentliche Interesse hier nicht überwog, so dass wir uns (noch) nicht gezwungen sahen, weiter zu intervenieren und verwiesen dementsprechend auf den Rechtsweg.*

Technologischer Datenschutz

Eine Anfrage betraf die **Aufzeichnung von 3D-Strassenansichten** mit einem Laserscanner. Wir erhielten von der Landespolizei die Information, dass in Vaduz ein Fahrzeug angehalten wurde, das einen auffälligen Dachaufbau besitzt und einem Google-Fahrzeug, wie sie zur Aufnahme von Strassenansichten (Google Street View) verwendet werden, ähnlich sieht. Unabhängig davon erreichte uns eine weitere Anfrage zum selben Sachverhalt durch eine Privatperson. Unsere Abklärungen ergaben, dass es sich um keine Fotoaufnahmen handelte. Uns gegenüber erklärte der Lenker des Fahrzeugs, dass es sich beim Aufbau auf dem Autodach um einen 3D-Laserscanner handelt. Es wurde uns direkt vor Ort eine Visualisierung der aufgezeichneten Rohdaten vorgeführt. Darauf waren Menschen- und Gebäudeumrisse lediglich als Gittermodell erkennbar. Die aufgezeichneten Daten würden in weiterer Folge als Grundlage für die Entwicklung und Forschung im Zusammenhang mit autonomen Fahrzeugen verwendet. Da Personen weder direkt noch indirekt identifiziert werden können, findet das *Datenschutzgesetz keine Anwendung*. Doch dies ist für einen Laien nicht zu erkennen. Die diesbezüglichen Reaktionen weisen auf eine gesteigerte Sensibilität gegenüber Fahrzeugen hin, die mit auffallenden Dachaufbauten im Strassenverkehr unterwegs sind.

Regelmässig erhalten wir Anfragen zum Betrieb eines WLAN-Netzes oder wir sensibilisieren betreffend die Gefahren bei der Nutzung.[7] Eine Anfrage betraf die **Voraussetzungen** für den **Betrieb eines öffentlichen WLAN-Netzes** im Zentrum einer Gemeinde. Da keine SMS- oder andere Authentifizierung der Nutzer stattfindet, kann der Betreiber zu keiner Zeit feststellen, wer sich mit dem WLAN verbunden hat. Entscheidet sich ein Betreiber *zwecks Vorbeugung oder Aufklärung möglichen Missbrauchs, wie z. B. Mobbing, entsprechende Nutzerinformationen zu speichern*, sind die Bestimmungen des DSG einzuhalten.[8] Dies sind beispielsweise die *Informationspflichten* gegenüber den Betroffenen oder die *Datensicherheitsmassnahmen* zum Schutz der bearbeiteten Personendaten.

Polizei, Sicherheit und Justiz

Wie bereits im vergangenen Jahr erhielten wir wieder zahlreiche Anfragen zu Kameraaufnahmen mittels **Drohnen**.[9] Die Anfragen betrafen beispielsweise die Zulässigkeit von Gebäudeaufnahmen oder allgemeine Übersichtsaufnahmen von Landschaften oder des Viehmarktes in Eschen. Bildaufnahmen von Drohnen bergen gewisse Risiken für die Privatsphäre, sind jedoch *nicht per se verboten*. Grundsätzlich unproblematisch sind Landschaftsbilder oder etwa Aufnahmen, auf denen Personen nicht identifizierbar sind. Sonst sind gewisse Voraussetzungen zu beachten, sodass *eine Bewilligung zur Videoüberwachung notwendig sein kann*.[10] In zwei Fällen ergab die nähere Prüfung des Sachverhalts eine solche Bewilligungspflicht gemäss Art. 6a DSG. Beiden Anträgen wurde mit entsprechenden Auflagen, wie beispielsweise die *Pflicht zur Information möglicher Betroffener*, entsprochen.

Eine Versicherung fragte uns nach dem zulässigen Rahmen für den Einsatz von **Dash-Cams.** Als Dash-Cams werden Videokameras bezeichnet, die zumeist auf dem Armaturenbrett oder an der Windschutzscheibe eines Fahrzeugs angebracht sind und das Verkehrsgeschehen vor dem Fahrzeug während der Fahrt fortwährend aufzeichnen. Dash-Cams sind ein modernes Mittel, um den Verkehr zu beobachten und gegebenenfalls, z. B. nach einem allfälligen Unfall, diesen nachvollziehen zu können. Wir sind der Ansicht, dass eine Dash-Cam im konkreten Ereignisfall ein probates Mittel sein kann, um sich zu schützen. Dabei ist jedoch zu beachten, dass Dash-Cams mit Drohnen und Videoüberwachungen vergleichbar sind, sodass die entsprechenden gesetzlichen Regelungen greifen. Dabei dürfte das Problem in der Praxis darin bestehen, dass die betroffenen Personen (Verkehrsteilnehmer) entsprechend dem Gesetz auf

6 Tätigkeitsbericht 2015, 7. Auch im vergangenen Jahr erhielten wir solche Fälle, die wir nicht anders behandelten.
7 Tätigkeitsbericht 2013, 1.3 und 2.3, Tätigkeitsbericht 2014, 2.1 und 4.1.
8 Andere Aspekte wie Fragen des Urheberrechts bleiben hier ausgeklammert.
9 Tätigkeitsbericht 2015, 6.1.
10 Siehe unter 4.3 oder auch http://www.llv.li/#/11538/videouberwachung.

eine stattfindende Datenbearbeitung hingewiesen werden müssen. Es gilt der Grundsatz der Verhältnismässigkeit. Auf die Zusatzfrage, ob in Liechtenstein für einen *gesetzwidrigen Einsatz von Dash-Cams mit Bussen zu rechnen* ist (wie dies in Österreich der Fall war), *verwiesen wir auf das Landgericht*, da wir gemäss Gesetz nicht die Kompetenz haben, über die Rechtmässigkeit selbst zu entscheiden.

Wirtschaft und Finanzen

Wir berichteten schon mehrfach über die europäische Datenschutzreform. Die bisher gültige Richtlinie 1995/46/EG wurde im vergangenen Jahr durch eine Verordnung, die **Datenschutz-Grundverordnung (DSGVO),** abgelöst. Hier sei nur kurz daran erinnert, dass diese Reform nicht zuletzt von der Wirtschaft gewünscht worden war, damit Rechtssicherheit geschaffen wird. Die allgemeine Datenschutzrichtlinie 1995/46/EG stammt zudem aus einer Zeit, als das Internet noch praktisch keine Rolle spielte. Die Reform soll auch die Trends der letzten Jahre aufnehmen. Sie soll Bürokratie abbauen, Unternehmen stärker verpflichten, den betroffenen Personen ihre Rechte zurückgeben und die Datenschutzbehörden stärken. Insgesamt kann von einem Quantensprung gesprochen werden, der nicht zuletzt im strengen Bussenregime begründet ist. Was die Datenschutzbehörden angeht, ist eine engere Zusammenarbeit vorgesehen, da der Europäische Datenschutzausschuss (EDPB) in Zukunft verbindliche Beschlüsse fassen wird.

Auf die DSGVO wird in mehreren Teilen dieses Berichts eingegangen.

Eine Rechtsanwaltskanzlei stellte uns einige – gebührenpflichtige – Fragen über die **künftige Geltung der DSGVO** für Schweizer Versicherer. Im Ergebnis hielten wir fest, dass der räumliche Anwendungsbereich im Verhältnis zur bestehenden allgemeinen Datenschutzrichtlinie entscheidend ausgebaut wird. Sie gilt nicht nur für Tätigkeiten im Rahmen einer Niederlassung im EWR, sondern auch, wenn betroffenen Personen im EWR Waren oder Dienstleistungen angeboten werden oder wenn das Verhalten betroffener Personen beobachtet wird, soweit ihr Verhalten im EWR erfolgt. Die Wirtschaft in Liechtenstein ist sehr stark auf das Ausland ausgerichtet. Ein wesentlicher Grund für den Beitritt zum EWR war damals das Argument, dass das Land somit gleichzeitig zwei Wirtschaftsräumen angehören kann. Damit sollten Schweizer Unternehmen angelockt werden, was auch gelang. Die DSGVO bestimmt nun, dass *für Schweizer Unternehmen, die keine Niederlassung im EWR haben, die DSGVO trotzdem gilt, wenn Waren oder Dienstleistungen angeboten werden.* Dies ist im Falle von Versicherungen klar zu bejahen.

Im Ausblick des letzten Tätigkeitsberichts hatten wir erwähnt, dass wir beabsichtigten, ein Merkblatt für die Verpflichteten zur **Meldung von Sicherheitsverletzungen** gemäss Gesetz über den internationalen automatischen Informationsaustausch in Steuersachen (AIA-Gesetz) zu erstellen. Dies wurde *hinfällig, nachdem das Gesetz nun vorsieht, dass nur die Steuerverwaltung unter eine solche Meldepflicht fällt.*

Wir wurden informell durch ein Unternehmen im Finanzbereich kontaktiert, bei dem eine solche Sicherheitsverletzung stattgefunden hatte und danach gefragt, ob es eine **Pflicht zur Meldung von Sicherheitsverletzungen** gibt. *Eine solche Pflicht gibt es* in Deutschland sowie in Österreich und ist ebenfalls in der DSGVO vorgesehen, aber *in Liechtenstein eben nicht.*

Die Steuerverwaltung stellte uns Fragen zu zwei Fällen betreffend die **Informationspflicht nach Art. 10** des AIA-Gesetz. Bei der ersten Anfrage ging es darum, in welchem Ausmass das meldende Finanzinstitut eine meldepflichtige Person über den Informationsaustausch aus datenschutzrechtlicher Sicht informieren muss. Insbesondere stand die Frage im Raum, ob ein Schreiben, mit dem das meldende Finanzinstitut eine betroffene Person[11] lediglich abstrakt informiert, der Informationspflicht gemäss Art. 10 AIA-Gesetz genügt oder ob die betroffene Person im Informationsschreiben namentlich anzuschreiben ist und die gemäss dem AIA-Gesetz zu übermittelnden Informationen konkret zu benennen sind. Unsere Antwort lautete dahingehend, dass *die betroffene Person namentlich angeschrieben werden und sie über die zu übermittelnden Informationen informiert werden muss.* Nur dies gewährleistet, dass die betroffene Person die Möglichkeit auf Berichtigung unrichtiger Daten wirklich wahrnehmen und von ihrem Berichtigungsrecht Gebrauch machen kann.

Der zweite Fall betraf die Frage der **rechtzeitigen Zustellung einer Informationsmitteilung nach Art. 10 AIA-Gesetz,** wenn anstelle der direkten Zustellung an die meldepflichtige Person die betroffene Person mit dem meldenden Finanzinstitut eine andere Form der Zustellung (z. B. Hinterlegung oder Zustellung an eine Drittperson) vereinbart hat. Hier waren wir der Meinung, dass das *meldende Finanzinstitut seiner Informationspflicht gemäss Art. 10 AIA-Gesetz Genüge tat, wenn es sich an die Zustellvereinbarung hält.*

11 Z. B. Begünstigte, wirtschaftlich Berechtigte der X-Stiftung.

Das meldende Finanzinstitut muss insbesondere nicht prüfen, ob durch die Zustellform gemäss Zustellungsvereinbarung eine Information gemäss dem AIA-Gesetz einer meldepflichtigen Person rechtzeitig zugehen wird. Das Risiko des rechtzeitigen Informationszugangs liegt vielmehr bei der betroffenen Person, wenn diese eine von der üblichen (direkten) Zustellung abweichende Zustellform wählt.

Datenbekanntgabe im Inland

Wir wurden vom Amt für Informatik angefragt, ob es datenschutzkonform ist, **Fotos aller Mitarbeitenden der Landesverwaltung im Intranet** zu veröffentlichen. Dies ist heute (noch) nicht der Fall. Heute ist die Lage so, dass jeder Mitarbeiter selbst bestimmen kann, ob sein Foto von anderen angesehen werden darf oder nicht. *Fotos sind nicht direkt arbeitsbezogen und damit auch nicht notwendig*, um kontaktiert zu werden. Das Amt für Personal und Organisation wies zu Recht auf Art. 46 des Staatspersonalgesetzes hin. Danach dürfen Personendaten von Angestellten «zu verwaltungsinternen Informationszwecken» bekannt gegeben werden. Damit ist eine Rechtsgrundlage gegeben. Wir wiesen dennoch darauf hin, dass es zur Zeit der Anfrage nicht wenige Angestellte gab, welche die Fotos nicht freigegeben hatten. Dies wohl aus verschiedenen Gründen. Vor allem bei Personen mit Vollzugsaufgaben ist dies verständlich. *Wir sprachen uns dafür aus, alle Personen einzubeziehen, damit ein allfälliger Systemwechsel akzeptiert wird.*

Die Liechtensteinischen Kraftwerke (LKW) und die Liechtensteinische Gasversorgung (LGV) haben die Frage aufgeworfen, ob sie Daten über den **Energieverbrauch aufgeschlüsselt nach Parzellen** an ein **Unternehmen bekannt geben** dürfen. Das Unternehmen soll im Auftrag von Gemeinden die Energieverbrauchsdaten so aufbereiten, dass sie im Gemeinde-GIS hinterlegt werden können und beim jeweiligen Anklicken von Parzellen abrufbar sind. Bei der Prüfung der Rechtslage stellte sich heraus, dass zur *Datenweitergabe keine gesetzliche Grundlage besteht. Es wurde daher angeregt, eine solche zu schaffen.* Die Regierung nahm diese Anregung zur Kenntnis und prüft die Anpassung der entsprechenden Spezialgesetze, wie z. B. LKWG und LGVG.[12]

12 Gesetz über die Liechtensteinischen Kraftwerke (LKWG) und Gesetz über die Liechtensteinische Gasversorgung (LGVG).

2.2 Stellungnahmen zu Vorlagen und Erlassen

Der Grundsatz «weniger ist mehr» gilt fortan auch für **Vernehmlassungsberichte.** Die Rechtsordnung ist darauf ausgerichtet, das Leben der Gesellschaft zu ordnen. Dabei geht es meist um Personendaten. Deshalb bekommen wir alle Vernehmlassungsvorlagen 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.

Nachstehend werden unsere Stellungnahmen erwähnt, zuerst die für uns wichtigsten:

Im Rahmen der Übernahme und Umsetzung der **4. Geldwäsche-Richtlinie** wurden wir frühzeitig beigezogen. Gemäss der Richtlinie gilt die allgemeine Datenschutzrichtlinie.[13] Bekanntlich ist das DSG ein allgemeines Gesetz, das als Rahmen gilt. Wenn es Spezialregelungen gibt, sind diese zu beachten. Deshalb machten wir in der entsprechenden Arbeitsgruppe den Vorschlag, die Grundsätze des DSG[14] für die Bedürfnisse der Wirtschaft sektorspezifisch festzulegen. Dieser Vorschlag wurde als nicht notwendig erachtet. Offensichtlich passen diese Grundsätze für die Praxis. Demgemäss wird in der Vorlage neben Bestimmungen, die die Richtlinie speziell vorgibt, allgemein auf die Geltung des DSG verwiesen. *Wir regten an, dass die Grundsätze des DSG zumindest in den Erläuterungen zur Gesetzesvorlage erwähnt werden. Dies soll die Handhabung des Gesetzes in der Praxis erleichtern.*

Wir wurden durch das Ministerium für Inneres, Justiz und Wirtschaft angefragt, ob es in Bezug auf die **Richtlinie (EU) 2016/680** zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der **Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung** (Datenschutzrichtlinie für Polizei und Justiz DSRL-PJ)[15] einen rechtlichen Handlungsbedarf

13 Art. 41 Abs. 1 Satz 1 der Richtlinie (EU) 2015/849 lautet: «Für die Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie gilt die in nationales Recht umgesetzte Richtlinie 95/46/EG.»

14 Neben den Bestimmungen, welche von der Richtlinie vorgegeben sind, betrifft dies folgende Aspekte: Verhältnismässigkeit, Bearbeitung nach Treu und Glauben, Datenrichtigkeit, Bekanntgabe ins Ausland, Outsourcing, Datensicherheit, automatisierte Einzelentscheidungen, Rechtsschutz, Zuständigkeit der DSS.

15 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständi-

in Liechtenstein gibt.[16] Datenschutzbestimmungen kommen in der bestehenden Gesetzgebung vor. Es war aber nicht möglich, uns einen Gesamtüberblick im Hinblick auf die neue Richtlinie zu verschaffen. Dazu fehlte uns eine Grundprüfung durch die beteiligten Ämter. *Im Sinne der Schaffung von Synergien schlugen wir vor, dass erst ein Vergleich der bestehenden Gesetzgebung (insbesondere Polizeigesetz, Strafprozessordnung, DSG) durch die entsprechenden Ämter mit dieser neuen Richtlinie gemacht wird.* Auf Grund dieses Vergleichs können wir dann unseren konkreten Input liefern. Unabhängig vom oben gesagten und dem nationalen Gesetzgebungsprozess überlässt die DSRL-PJ den einzelnen Mitgliedsstaaten einen gewissen Umsetzungsspielraum und so hängt die konkrete Ausgestaltung der im Einzelfall einzuhaltenden Regelungen wesentlich vom jeweiligen nationalen (Materien-)Gesetzgeber ab. Der sachliche Anwendungsbereich der DSRL-PJ liegt im Bereich der Strafrechtspflege, des Strafvollzugs und der öffentlichen Sicherheit, welche insbesondere in der StPO, dem PolG und dem StVG von der Landespolizei, der Staatsanwaltschaft und dem Landgericht noch umzusetzen sein werden.[17] Die zweijährige Umsetzungsfrist für die DSRL-PJ endet gleichzeitig mit dem Inkrafttreten der DSVGO am 25. Mai 2018.

Zur **Integration des Notrufs 144** (Sanitätsnotruf beim Landesspital) in die Landesnotruf- und Einsatzzentrale der Landespolizei gaben wir ebenfalls eine Stellungnahme ab und sahen einige Punkte kritisch. Es war geplant, dass nach der Zusammenlegung auf die Nummer 144 kein Sanitäter oder anderes medizinisches Personal, sondern ein Polizist das Gespräch entgegennehmen wird. Wir wiesen darauf hin, dass hier *zwei grundlegend verschiedene Zwecke*, erstens die Erstversorgung bei Notfällen und zweitens die Strafverfolgung und Gefahrenabwehr, miteinander verbunden werden. Auch wenn dies gesetzlich verankert werden soll und somit dem *Zweckbindungsprinzip*[18] entspricht, sehen wir dies äusserst problematisch.

Eine weitere Stellungnahme gaben wir zur **Einführung eines Bedrohungsmanagements** ab, da in diesem Zusammenhang umfassende Personendaten (z. B. die «Vorgeschichte» sowie das Verhalten einer Person) bearbeitet werden. Ziel des Bedrohungsmanagements ist es, aufgrund möglichst vieler Informationen aus einzelnen Vorfällen oder Ereignissen das mögliche Gefährdungspotenzial einer Person zu bestimmen. Eine solche umfassende Datenbearbeitung birgt naturgemäss die Gefahr von Datenschutzverletzungen. *Wir befürworten ein Bedrohungsmanagement grundsätzlich, dennoch haben wir diverse Kritikpunkte angebracht.* So wird beispielsweise für eine Meldung an die zuständige Stelle bei der Landespolizei – anders als in der Rezeptionsvorlage von Solothurn – auf die Hürde einer hohen Gewaltbereitschaft verzichtet. Dies lässt objektive Kriterien für eine Abgrenzung zu relevanten Fällen missen und ermöglicht willkürliches staatliches Handeln. Ohne objektive Kriterien ist von subjektiven Kriterien auszugehen, was in einem solchen sensiblen Bereich kritisch ist. Daher regten wir an, dass unbedingt *objektive Kriterien erstellt werden sollten*, welche als *Vorgaben und Leitplanken für Meldende* (Ärzte, Behörden und Private) dienen sollten. Zudem handelt es sich um *besonders schützenswerte Personendaten, welche eines erhöhten Schutzes bedürfen.* Zu guter Letzt fügten wir an, dass die in der Vorlage mehrfach erwähnte *Expertenrunde eine ausreichende gesetzliche Grundlage benötigt*, um die erforderlichen Personendaten bearbeiten und austauschen zu dürfen.

Zu folgenden Gesetzesprojekten gaben wir ebenfalls eine Stellungnahme ab:[19]

- Gemeindegesetz (GemG)
- Gesetz über den internationalen automatischen Austausch länderbezogener Berichte multinationaler Konzerne (CbC-Gesetz)
- Abänderung des Kommunikationsgesetzes (KomG) und der Strafprozessordnung (StPO) im Zusammenhang mit der Vorratsdatenspeicherung
- Abänderung des Gesetzes über die Durchsetzung internationaler Sanktionen (ISG)
- Gesetz zur Durchführung der Verordnung (EU) Nr. 596/2014 über Marktmissbrauch (EWR-Marktmissbrauchsverordnungs-Durchführungsgesetz; EWR-MDG)
- Schaffung eines Wirtschaftsprüfungsgesetzes (WPG) und die Abänderung weiterer Gesetze

gen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

16 In der Schweiz wurde zur Richtlinie ein Handlungsbedarf festgestellt und eine Revision des Datenschutzgesetzes lanciert, siehe unter 8.

17 Strafprozessordnung vom 18. Oktober 1988, LGBl. 1988 Nr. 62, Gesetz vom 21. Juni 1989 über die Landespolizei, LGBl. 1989 Nr. 48, und Strafvollzugsgesetz vom 20. September 2007, LGBl. 2007 Nr. 295.

18 Art. 4 Abs. 3 DSG.

19 Die Stellungnahmen sind zum Teil abrufbar unter http://www.llv.li/#/12458/externe-stellungnahmen-zu-vernehmlassungsberichten.

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

Im letzten Tätigkeitsbericht hatten wir erwähnt, dass ein für den Datenschutz wichtiger StGH-Entscheid betreffend die Datenbekanntgabe zwischen Behörden ergangen ist.[20] Im Urteil hielt der Staatsgerichtshof fest, dass im konkreten Fall die **proaktive Zurverfügungstellung von Daten keine gesetzliche Grundlage habe und daher unverhältnismässig sei.**[21] Die Steuerverwaltung als Datenempfänger könne jedoch die notwendigen Daten bei Zweifeln über die vollumfängliche Erfüllung der Steuerpflicht im Einzelfall im entsprechenden Umfang anfordern. Wie angekündigt **prüften wir die neu entwickelte Praxis** im Hinblick darauf, ob diese den Anforderungen des Urteils genügt. Wir stellten dabei fest, dass die neu entwickelte Praxis so aussah, dass *jede Verlassenschaftsakte der Steuerverwaltung (ohne konkrete Anfrage und ohne konkrete und begründete Zweifel der Steuerverwaltung) zugestellt wird.* Es war daher für uns nicht erkennbar, inwiefern sich die neue von der alten Praxis im Hinblick auf die proaktive Zurverfügungstellung von Daten unterscheidet, weshalb wir sie als datenschutzwidrig einstuften. Die neue Praxis wurde in der Folge wieder aufgegeben.

2.4 Auslandsdatentransfer und Empfehlungen bei Auslandsdatentransfer

Obwohl der gesetzwidrige Transfer von Daten ins Ausland strafbar ist,[22] erhielten wir in der Vergangenheit nur sehr wenige Meldungen.

Vereinzelt wurden wir im vergangenen Jahr über **Datenbekanntgaben in Drittstaaten unter der Verwendung von Standardvertragsklauseln** informiert.[23] Bei einer Meldung wurden wir gebeten, vorgängig die Übereinstimmung mit den Vorgaben der EU zu überprüfen, weil entsprechende Ergänzungen vorgenommen wurden. Die *Standardvertragsklauseln, welche von der EU vorgegeben sind, dürfen grundsätzlich nur unverändert übernommen werden, um in den Genuss von Art. 6 Abs. 5 Datenschutzverordnung (DSV) zu kommen. Werden Standardvertragsklauseln unverändert übernommen, ist gemäss Art. 6 Abs. 5 DSV keine Genehmigung der Bekanntgabe von Daten ins Ausland nach Art. 8 Abs. 3 DSG durch das Ressort Justiz erforderlich. Der Inhaber der Datensammlung muss in einem solchen Fall vielmehr nur die diesbezügliche Datenbekanntgabe ins Ausland der Datenschutzstelle bekannt geben.* Im konkreten Fall wurden uns Standardvertragsklauseln unterbreitet, die ergänzt worden waren. Wir waren der Ansicht, dass die unterbreiteten Standardvertragsklauseln inhaltlich die zu verwendenden Standardvertragsklauseln veränderten und teilten dem Verfasser mit, dass ein Datentransfer gestützt auf diese geänderten Standardvertragsklauseln nicht den gesetzlichen Vorgaben entspricht. Die konkrete Abklärung war zudem als Stellungnahme oder Gutachten zu qualifizieren und aufgrund der Einführung der Gebührenpflicht im Jahr 2014 kostenpflichtig.[24]

Im Rahmen des **Aussenverhältnisses eines Unternehmens, das genehmigte Binding Corporate Rules (BCR) eingeführt hat,** stellte sich die Frage, wie der Fall zu beurteilen wäre, wenn eine Tochtergesellschaft, z. B. in Hong Kong, Daten an Externe bekannt geben möchte. In einem solchen Fall sind die verschiedenen Ausgestaltungsmöglichkeiten von BCR, von verbindlichen Unternehmensrichtlinien, genauer zu betrachten. Der *materielle Anwendungsbereich von BCR kann vom Unternehmen selbst definiert werden.* So kann beispielsweise die Anwendbarkeit von BCR lediglich auf Mitarbeiterdaten beschränkt sein. Des Weiteren können Unternehmen die Anwendbarkeit der BCR auf Datenbekanntgaben beschränken, welche aus dem EWR in ein bestimmtes Drittland erfolgen. Allein schon aus den genannten zwei Einschränkungen hängt die Antwort in Bezug auf die obige Fragestellung – Datenbekanntgabe an Externe einer Tochtergesellschaft in Hong Kong – davon ab, um welche Daten es sich handelt und ob die Datenkategorie sowie der konkrete Datenfluss von den BCR gedeckt sind. Um einen datenschutzkonformen Datenfluss auch an Subunternehmen zu gewährleisten, gibt es verschiedene Möglichkeiten. *Externe Datenbearbeiter in einem Drittland können z. B. mittels ad-hoc-Verträgen oder Standardverträgen in die Pflicht genommen werden.* Zudem können Auftragsdatenbearbeiter in Bezug auf die eigenen Personendaten den BCR unterworfen werden.[25]

Insgesamt halten sich die **Meldungen von Datentransfers ins Ausland** sehr im Rahmen. Bei Veranstaltungen über die kommende DSGVO weisen wir

20 Tätigkeitsbericht 2014, 2.3, sowie Tätigkeitsbericht 2015, 2.3.
21 StGH 2014/107 vom 09.02.2015 Erw. 3.3 (in: LES 2015, 69, Heft 2).
22 Art. 40 Abs. 2 Buchstabe c DSG.
23 Art. 6 Abs. 5 DSV.
24 Art. 33 Abs. 1 DSV.
25 Arbeitsdokument zu «Häufig gestellte Fragen» (FAQ) über verbindliche unternehmensinterne Datenschutzregelungen (BCR), WP 155 rev. 04, Frage 2, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp155_rev04_de.pdf.

Unternehmen immer wieder darauf hin, dass es diesbezüglich eine **(strafbare) Meldepflicht** gibt, die mit der **DSGVO** um ein Vielfaches verschärft wird. Somit raten wir Unternehmen, zu prüfen, ob sie diesen Anforderungen nachkommen.

2.5 Projektbegleitung

Im Rahmen der Übernahme und Umsetzung der **4. Geldwäsche-Richtlinie** wurden wir frühzeitig beigezogen.[26] Die Richtlinie sieht unter anderem in jedem Mitgliedsstaat ein zentrales Register vor, in dem Angaben zu wirtschaftlichen Eigentümern von Gesellschaften oder sonstigen juristischen Personen gespeichert werden müssen; das sogenannte **Register über die wirtschaftlich Berechtigten** (WB-Register). Wir wurden in eine Arbeitsgruppe zur Erarbeitung möglicher Ausgestaltungsvarianten des Registers eingeladen. Für uns hatte in den Diskussionen vor allem die *Sicherstellung eines besonders hohen Standards der Datensicherheit Priorität*. So sind insbesondere erhöhte Sicherheitsmassnahmen bei der Datenübermittlung, Vergabe der Zugriffsrechte, Datenaufbewahrung, Löschung sowie bei der Protokollierung zu berücksichtigen. Wir erachten es gerade aufgrund der Sensitivität der im Register bearbeiteten Daten als sinnvoll, dass vor der Inbetriebnahme sowohl die Abläufe als auch die konkrete technische Implementierung durch eine unabhängige Stelle überprüft werden.

Im Rahmen der Abänderung des Gesetzes über die Stabsstelle Financial Intelligence Unit (FIUG) wurde mit Art. 10 ein **indirektes Auskunftsrecht** geschaffen: Werden Daten bei der Stabstelle Financial Intelligence Unit (SFIU) im Rahmen der Bekämpfung von Geldwäscherei, organisierter Kriminalität oder Terrorismusfinanzierung bearbeitet, kann die betroffene Person nicht selbst, sondern nur über uns Auskunft von der SFIU darüber begehren, ob Daten über sie bearbeitet werden. Um unserer neuen Aufgabe zu entsprechen, besprachen wir gemeinsam mit der SFIU die bestehenden Abgrenzungen, beispielsweise in Bezug auf die Akteneinsicht oder Auskunft gemäss Art. 11 DSG, das Verfahren und die damit zusammenhängenden Abläufe gemäss den gesetzlichen Vorgaben. *Bis Jahresende erhielten wir einige diesbezügliche Anfragen*, die wir nach einer entsprechenden Überprüfung der Rechtmässigkeit der Datenbearbeitung bei der SFIU allesamt wie vorgesehen gleichlautend beantworteten.

Weiter sieht das FIUG vor, dass Daten nach längstens zehn Jahren zu löschen sind.[27] Wir wurden durch die Stabsstelle angefragt, ob wir sie bei der Umsetzung der Bestimmung betreffend das **ordnungsgemässe Löschen von Daten** beraten. In diesem Zusammenhang tauschten wir uns mit der SFIU über verschiedene Verfahren und Ausgestaltungen zur Vernichtung von Daten aus. Wir sind hier weiter mit der Stabstelle im Kontakt und werden die konkrete organisatorische und technische Umsetzung begleiten. Ungeachtet dessen hatten wir uns vorgenommen, eine entsprechende *Empfehlung zur Vernichtung von Personendaten* zu veröffentlichen. Dies vor allem, weil aktuell in verschiedenen Entwürfen für Gesetzesänderungen Löschbestimmungen aufgenommen werden und wir den Datenbearbeitern eine Hilfestellung zur Einhaltung dieser Bestimmungen geben wollen. Aus Ressourcengründen mussten wir dies bisher jedoch verschieben.

Bei der öffentlichen Ankündigung der **Volkszählung 2015** erwähnte das Amt für Statistik, dass wir die Durchführung der Volkszählung begleiten,[28] bei der alle fünf Jahre wichtige Daten der ganzen Bevölkerung erhoben werden. Die Informationen, die sich aus Volkszählungen ergeben, stellen ein wichtiges Steuerungsinstrument für den Landtag und die Regierung dar. Wie schon 2010 werden zahlreiche Daten erhoben, wobei abermals nicht sämtliche Daten direkt bei den Betroffenen erfragt, sondern teils aus Registern (z. B. aus dem ZPR, dem Zentralen Personenregister) bezogen werden.[29] Die Daten aus den Fragebögen sowie aus den Registern sind jeweils sehr detailliert. Dies führt dazu, dass die Daten der Volkszählung Persönlichkeitsprofile darstellen, die für die automatische Qualitätsprüfung und für Vervollständigungen notwendig sind. Wir liessen uns die Datenbearbeitung beim Amt für Informatik sowie beim Amt für Statistik erläutern und bestimmte Aspekte vorführen. Der Fokus lag dabei auf der Zweckbindung sowie den organisatorischen Abläufen und Schutzmassnahmen. Der Sinn der Volkszählung ist die statistische Auswertung. Somit dürfen die erhobenen Daten auch nur für statistische Zwecke verwendet werden. Das Statistikgeheimnis findet hier Anwendung. *Die bisherige Begleitung zeigte, dass die einschlägigen Bestimmungen sowie die Datenschutzgrundsätze eingehalten werden.* Es waren bisher keine Empfehlungen betreffend die Datenbearbeitung auszusprechen. Im Dezember 2016 wurden bereits erste Ergebnisse publiziert.[30] Wir begrüssen die gute

26 Siehe unter 2.2.

27 Art. 8 Abs. 2 FIUG.
28 Tätigkeitsbericht 2015, 8., sowie http://www.llv.li/#/116050.
29 Tätigkeitsbericht 2009, 4.
30 http://www.llv.li/#/116050/volkszahlung.

Zusammenarbeit und werden diese mit dem Amt für Statistik weiter fortsetzen und dadurch unseren Beitrag dazu leisten, damit die Volkszählung das von Regierung und Landtag gewünschte Steuerungsinstrument bleibt.

Anfang Jahr führte die **Landesverwaltung ein neues Informatikreglement** ein. Es hat das Ziel, die ordnungsgemässe Nutzung der Informatikmittel der Verwaltung sicherzustellen und einen störungsfreien Betrieb zu gewährleisten. Es hat zum Zweck, die Datenbestände zu schützen, den sicheren und wirtschaftlichen Einsatz der Informatikmittel zu gewährleisten sowie die Persönlichkeitsrechte der Anwender zu wahren. Unter anderem werden die geschäftliche und private Nutzung von Informatikmitteln, die Nutzung von Internet, E-Mail, Kalender und Festnetz- sowie Mobiltelefonie geregelt. Bis anhin gab es hier innerhalb der Verwaltung Lücken in den Regelungen, was in der Vergangenheit regelmässig zu Anfragen bei uns führte oder sich allgemein Fragen zur datenschutzkonformen Bearbeitung stellten.[31] Ein eigenes Kapitel widmet sich der Informationssicherheit und dem Datenschutz.

Da sich gerade im Zusammenhang mit der Verwendung von Informatikmitteln Fragen zum Schutz der Privatsphäre der Mitarbeiter stellen, wie beispielsweise bei der Protokollierung, bekamen wir die Gelegenheit bei der inhaltlichen Ausgestaltung mitzuwirken.Unsere Anregungen wurden zum grossen Teil übernommen.

Das Thema **eHealth** kam in den vergangenen Jahren nicht weiter voran.[32] Seit der Gründung des Vereins eHealth bekommt dieses Thema die Bedeutung, die es auch verdient. Wir wurden durch den Verein kontaktiert und um Mitarbeit gebeten. Es ging dabei um die Frage, wie das Thema möglichst erfolgsversprechend behandelt werden kann. Diskutiert wurden dabei die Modelle der Schweiz und jenes von Österreich. Nach Rücksprache mit dem zuständigen Ministerium wurde ein Projekt zur Schaffung eines gesetzlichen Rahmens gestartet. Unser Fokus richtete sich dabei darauf, dass der Datenschutz hier eine hohe Beachtung findet. Denn nur ein datenschutzkonformes und sicheres eHealth wird das notwendige Vertrauen der Bevölkerung geniessen können.

31 Tätigkeitsbericht 2011, 1.7 (Allgemein Arbeitsbereich) und 4. (Auswertung von Protokollen) sowie Tätigkeitsbericht 2013, 1.2 (Nutzung von privaten Geräten – Bring Your Own Device).

32 Tätigkeitsbericht 2011, 1.4 und 2.1.

3. AUFSICHT

Im Folgenden führten wir verschiedene Fälle auf, bei denen wir unsere **Aufsichtsaufgaben** wahrnahmen oder wahrnehmen mussten. Dies wird, nicht zuletzt im Rahmen der künftigen DSGVO, vermehrt der Fall sein. Gerade aus diesem Grund möchten wir unseren Fokus von der Information und Sensibilisierung wegnehmen und mehr im Bereich Aufsicht tätig sein, wenn sich die Notwendigkeit dazu ergibt.[33]

Wir untersuchten die Datensicherheit der **elektronischen Steuererklärung (eTax).** Das Programm ermöglicht das einfache Ausfüllen der jährlichen Steuererklärung. Die Lösung kann sowohl für natürliche als auch juristische Personen auf der Internetseite der Steuerverwaltung heruntergeladen werden.[34] Aufgrund einer Anfrage untersuchten wir die konkrete Implementierung des seit 2010 vorhandenen Passwortschutzes.[35] Als Ergebnis stellten wir fest, dass *der Passwortschutz der eTax-Applikation für das Steuerjahr 2015 nicht dem Stand der Technik entspricht und einfach umgangen werden kann.* Es wird gegenüber einem Nutzer der Eindruck erweckt, dass entsprechende Schutzmechanismen vorhanden sind, obwohl diese in der Praxis einem Angriff nicht standhalten. Wir informierten umgehend die Steuerverwaltung und das Amt für Informatik über diesen Sachverhalt, da hier eine Korrektur zwingend notwendig war. Im Zuge der Diskussion stellte sich die Frage, ob der Passwortschutz nicht einfach weggelassen werden kann, da eine Datenbearbeitung ausschliesslich im Verfügungsbereich des Steuerpflichtigen erfolgt. Es lässt sich nachvollziehbar die Ansicht vertreten, dass die vollständige Verantwortung beim Steuerpflichtigen liegt und ein Passwortschutz daher nicht zwingend notwendig ist. Wir sehen ungeachtet dessen und angelehnt an eine Stellungnahme der Artikel-29-Datenschutzgruppe[36] dennoch eine gewisse Mitverantwortung der Steuerverwaltung. *Wir traten in diesem Punkt gegen die Entfernung und für die Implementierung eines sicheren Passwortschutzes der einzelnen Dateien der Steuererklärungen ein.* Die Steuerverwaltung teilte unsere Ansicht nicht und kündigte an, den Passwortschutz zu entfernen und die Nutzer entsprechend darüber zu informieren. Wir raten Nutzern bei der Verwendung der elektronischen Steuererklärung darauf zu achten, dass die Software nur auf einem geschützten Computer (aktueller Virenscanner aktiv, Betriebssystem-Updates eingespielt, Nutzerpasswort vergeben, Festplatte bei Notebooks verschlüsselt usw.) verwendet wird.[37] Die Dateien der Steuererklärung sollten nicht in einer öffentlichen Cloud oder einer anderen externen Ablage gespeichert werden, wo Dritte möglicherweise Zugriff darauf haben.

Zudem liessen wir uns die Datenbearbeitung im Zusammenhang mit dem Foreign Account Tax Compliance Act **(FATCA)** bei der Steuerverwaltung vorführen.[38] Liechtensteinische Finanzinstitute sind nach dem FATCA-G[39] dazu verpflichtet, bestimmte Informationen der Steuerverwaltung zu melden, die ihrerseits diese Informationen automatisch an die US-Steuerbehörde (IRS) weiterleiten. *Aufgrund der Sensitivität der Daten ist das damit verbundene erhöhte Sicherheitsniveau zu berücksichtigen.* Eine datenschutzkonforme und sichere Datenbearbeitung ist hier zwingend. So hat beispielsweise die gesamte Kommunikation zwischen den Behörden verschlüsselt zu erfolgen.[40] Unsere Abklärung bei der Steuerverwaltung erfolgte anlasslos. Es ging uns darum, einen Überblick über die verwendeten Systeme und technischen Implementierungen zu bekommen. Dies vor allem, weil für die technischen Umsetzungen weiterer Abkommen (z. B. AIA-Gesetz) auf die für FATCA geschaffene Infrastruktur aufgebaut werden soll. Im Rahmen der Vorführung zeigte sich, dass sich unsere gute Zusammenarbeit mit dem Amt für Informatik bewährt. Dies insbesondere um das für die Datenbearbeitung im internationalen Steueraustausch notwendige Sicherheitsniveau sicherzustellen. An dieser guten Zusammenarbeit soll von beiden Seiten festgehalten werden.

Eltern zweier Schüler der Primarschule Ruggell kontaktierten uns in Bezug auf ein Vorhaben der Schule. Dabei ging es darum, dass sämtlichen Schülern der ersten Klassen ein persönlich zugewiesenes **iPad für den Unterricht** übergeben werden sollte. Zum Zeitpunkt der ersten Anfrage waren noch nicht sämtliche Fragen seitens der Projektverantwortlichen geklärt. So stand beispielsweise noch nicht fest, welche Apps auf den Geräten in-

33 Tätigkeitsbericht 2015, 8.
34 http://www.llv.li/#/11939/etaxelektronische-steuererklarungen.
35 Tätigkeitsbericht 2010, 1.2.
36 Stellungnahme zu den Begriffen «für die Verarbeitung Verantwortlicher» und «Auftragsverarbeiter» (WP169), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.
37 Weitere Tipps in der Rubrik Selbstdatenschutz unter http://www.dss.llv.li.
38 Tätigkeitsbericht 2014, 2.2 und 6.1.
39 LR 359.131.2.
40 http://www.oecd.org/ctp/exchange-of-tax-information/keeping-it-safe.htm.

stalliert werden. Auch waren noch nicht sämtliche technischen Aspekte definiert und festgelegt worden. Wir wiesen die Projektverantwortlichen darauf hin, dass insbesondere die *Bestimmungen des Auskunftsrechts* zu beachten sind. Je nach technischer Ausgestaltung und verwendeter Apps könnte auch eine *Auftragsdatenbearbeitung* vorliegen. Falls die Schulkinder persönlich Daten auf den zugewiesenen iPads speichern (z. B. E-Mails oder Fotos), sind diese grundsätzlich als vertraulich zu betrachten. Ein vollumfänglicher anlassloser und *uneingeschränkter Zugriff auf die persönlichen Daten durch Lehrpersonen ist nicht zulässig*. Die zweite Anfrage betraf insbesondere die Frage der **Notwendigkeit der Einwilligung** der Eltern. Wir informierten daraufhin die Primarschule dahingehend, dass eine Einwilligung nach dem DSG lediglich in jenen Fällen erforderlich ist, in denen es an einer genügend bestimmten Rechtsgrundlage fehlt. Dies wird bei der Verwendung von Cloud-Diensten (z. B. iCloud) in der Regel anzunehmen sein. Je nach Art und Umfang der in Frage stehenden bearbeiteten Daten ist zudem von unterschiedlichen Erfordernissen hinsichtlich der Einwilligung auszugehen.[41] Aus Sicht des Datenschutzes bestehen beim genannten Projekt durchaus kritische Themenfelder, wie beispielsweise Datentransfer, Informationspflichten, Rechtsgrundlage (Lehrplan), «Überwachung» usw., die diskutiert werden sollten.

Die Anforderungen an die Datenbearbeitung bei Behörden ändern sich regelmässig. So werden immer wieder Systeme aktualisiert oder neue beschafft. Damit neben den IT-Sicherheitsaspekten zusätzlich die Datenschutzaspekte berücksichtigt werden können, sprachen wir uns mit dem Amt für Informatik wie folgt ab: Von den Ämtern sind bei der Beschaffung von neuen Systemen oder wenn sich bestehende Systeme ändern, **Schutzbedarfsanalysen** durchzuführen. Diese sind an das Amt für Informatik und an uns zu senden, wodurch wir die Projekte frühzeitig auf Datenschutzaspekte hin überprüfen können. Wir werden somit von Beginn an in Vorhaben einbezogen und das Risiko, dass im Nachhinein unter Umständen kostspielige Anpassungen notwendig werden, sinkt. *Nach einer ersten Pilotphase ist abzuwarten, inwieweit sich die Vorgehensweise in der Praxis bewährt und daran festgehalten wird.*

Beim Ausländer- und Passamt (APA) überprüften wir Ende 2014 die Praxis in Bezug auf die **Datenbearbeitung im Schengener Informationssystem (SIS).**[42] Der Fokus der Kontrolle lag auf der inhaltlichen Ausgestaltung der Protokollierung und stichprobenartig wurden der jeweilige Grund sowie die Rechtmässigkeit einzelner Abfragen durch die APA-Mitarbeiter geprüft. Die Kontrolle ergab Nachbesserungsbedarf bei der Protokollierung. Die notwendigen technischen Anpassungen an der Protokollierung konnten durch die verantwortliche Stelle bis zur Schengen-Evaluation Ende 2015[43] abgeschlossen werden. Bei der Nachkontrolle konnten wir nun feststellen, dass *sämtlichen Empfehlungen aus dem Abschlussbericht der ursprünglichen Kontrolle im 2014 vollumfänglich entsprochen wurde.*

41 siehe Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen), Artikel-29-Datenschutzgruppe, WP160 angenommen am 11. Februar 2009, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_de.pdf.

42 Tätigkeitsbericht 2014, 3.

43 Tätigkeitsbericht 2015, 6.3.

4. INFORMATION UND SENSIBILISIERUNG DER ÖFFENTLICHKEIT

Im letzten Tätigkeitsbericht hatten wir darüber informiert, dass wir fortan den Fokus von der Information zur **Aufsicht** wechseln wollen. Demgemäss reduzierten wir unsere Informations- und Sensibilisierungsarbeit primär was Veranstaltungen angeht. Im Sinne «von der Quantität zur Qualität» ist es sinnvoller, wenn wir statt an Veranstaltungen auf unserer Internetseite informieren. Dort sind die Informationen länger und für ein grösseres Publikum verfügbar.

4.1 Veranstaltungen

Aus Anlass des **Europäischen Datenschutztages** führten wir wiederum eine öffentliche Veranstaltung zum Thema «*Verdatet und verkauft! Wer bestimmt über mein digitales Ich*?» durch. In den vergangenen Jahren hatten wir den Fokus meist auf technische Themen gelegt. Doch was bedeutet dies für unsere Gesellschaft insgesamt, wenn wir ständig online und vernetzt sind? Es sollte der Frage nachgegangen werden, in welche Richtung diese Reise geht. Hauptreferentin war Karin Frick, Leiterin Research des Gottlieb Duttweiler Instituts (GDI). In ihrem *Vortrag zum Thema «Wie man Überwachung ausübt oder sich ihr entzieht»* ging sie auf Trends für die Zukunft ein und forderte insbesondere ein «Panoptikum der Selbstkontrolle». Ein solches würde es jedem Einzelnen erlauben, die Herrschaft über seine Daten zu bewahren oder sie zurück zu erhalten.[44] Daneben führte Jeffrey Nigg vom IT Crowd Club Liechtenstein (ITCC) eine interaktive Umfrage unter den über einhundert Teilnehmern durch. Bei dieser Umfrage ging es allgemein um die Wichtigkeit, die den verschiedenen Aspekten der Privatsphäre beigemessen wird.[45]

Neben dem Datenschutztag waren wir dieses Jahr wieder an der **LIHGA** präsent. Als kleine Amtsstelle suchten wir auch dieses Mal wieder die Zusammenarbeit mit Kooperationspartnern und nahmen unter dem Dach der Fachgruppe Medienkompetenz[46] zusammen mit dem IT Crowd Club Liechtenstein (ITCC) und der Universität Liechtenstein teil. Als Hauptthema stellten wir einen der kommenden Trends vor: *virtuelle Realität (VR)*. Ein Datenschutz-Quiz und weitere Materialien die wir an der LIHGA abgegeben haben, stehen auf unserer Internetseite bereit.[47]

Wie jedes Jahr hatten wir wieder einen **Erfahrungsaustausch mit den Datenschutzverantwortlichen von Unternehmen** durchgeführt. An dieser sehr gut besuchten Veranstaltung thematisierten wir *die DSGVO*. Sie findet ab Mai 2018 Anwendung und wird bedeutende Veränderungen mit sich bringen. Anpassungen der liechtensteinischen Datenschutzgesetzgebung und der Praxis werden nötig sein. Auch auf Unternehmen kommen in diesem Hinblick bedeutende Änderungen zu.

4.2 Veröffentlichungen in den Medien

Wir wurden von den Medien angefragt, was die **DSGVO für Liechtenstein bedeutet.** Wie bei allen Rechtsakten aus Brüssel stellt sich in Liechtenstein primär die Frage der Übernahme in den EWR. Bei der Grundverordnung ist dies jedoch etwas anders. Sie ist insbesondere dann anwendbar, wenn betroffenen Personen in der Europäischen Union Waren oder Dienstleistungen angeboten werden, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist. Die Wirtschaft in Liechtenstein ist bekanntermassen sehr exportorientiert. *Somit wird die Grundverordnung für zahlreiche Unternehmen, unabhängig von der Übernahme in den EWR, ab Mai 2018 gelten.* Sie bringt zahlreiche Änderungen mit sich. Eine drastische Änderung besteht im neuen Sanktionsmechanismus. Während Verstösse gegen den Datenschutz heute praktisch keine merkbaren Folgen nach sich ziehen, sind in bestimmten Fällen in Zukunft Maximalbussen bis zu 20'000'000 EUR oder 4% des weltweiten Jahresumsatzes (je nachdem, welcher der Beträge höher ist) möglich. Hierauf machten wir aufmerksam. Ob wir als nationale Datenschutzbehörde in diesem Zusammenhang überhaupt irgendeine Rolle spielen, hängt dagegen von der EWR-Übernahme ab.

4.3 Internetseite

Die **DSGVO** stand im Mittelpunkt unserer Veröffentlichungen auf unserer Internetseite, damit sich betroffene Unternehmen und Behörden bereits frühzeitig mit dieser Thematik beschäftigen können.[48]

Der Europäische Gerichtshof äusserte sich erneut zur **Vorratsdatenspeicherung.** In dem Fall bestä-

44 Siehe GDI Impuls, Nummer 3, 2015.
45 Die Dokumentation dieser Veranstaltung kann hier heruntergeladen werden: http://www.llv.li/#/117623/datenschutztag-.
46 http://www.medienkompetenz.li/.
47 http://www.dss.llv.li, unter Selbstdatenschutz.
48 http://www.llv.li/#/117565/datenschutzgrundverordnung-dsgvo. Siehe unter 6.1.

tigte er das bereits bestehende Urteil[49] und betonte erneut die Wichtigkeit des Datenschutzes in der Bekämpfung der Kriminalität. Wir wiesen auf unserer Internetseite auf dieses wichtige Urteil hin und ebenso darauf, dass das erste Urteil aus dem Jahr 2014 in Liechtenstein immer noch nicht umgesetzt ist. Es gab zwar eine Arbeitsgruppe, welche mit der Umsetzung beauftragt war und in der wir mitwirken konnten.[50] Die Gesetzeslage war bis Ende 2016 aber unverändert.

Im Berichtsjahr setzten wir uns vertieft mit dem Auslandsdatentransfer, und dabei insbesondere mit **Binding Corporate Rules (BCRs)** auseinander. Dies vor allem, weil sich ein international tätiges Unternehmen mit Sitz in Liechtenstein für die Implementierung von BCRs in ihrer Unternehmensgruppe interessierte. Im konkreten Fall kämen wir für das europaweite Genehmigungsverfahren als federführende Aufsichtsbehörde in Frage und somit auch als zentraler Ansprechpartner. Aus gegebenem Anlass ergänzten wir unsere Internetseite und brachten sie auf den aktuellen Stand.[51] Sie soll interessierten Unternehmen, insbesondere international tätigen, als erste Informationsquelle und Hilfestellung dienen.

Das gemeinsam mit dem Schulamt erarbeitete **Merkblatt über den Datenschutz an Schulen** wurde nun veröffentlicht.[52] Es gibt Erläuterungen und Hinweise, wie mit Personendaten in den öffentlichen und in den von der Regierung bewilligten privaten Schulen umzugehen ist.

Drohnen sind rechtlich Flugmodellen gleichgestellt und die Verwendung richtet sich in Liechtenstein nach dem schweizerischen Luftfahrtrecht sowie dem liechtensteinischen Datenschutzgesetz. Aufgrund verschiedener Zuständigkeiten bewährte sich eine enge Zusammenarbeit zwischen dem Amt für Bau und Infrastruktur, der Landespolizei und uns. In dieser Zusammenarbeit entstand ein *einheitlicher Internetauftritt und ein Flyer* wurde erstellt.[53] Auf unserer Internetseite informieren wir insbesondere über die Risiken für die Privatsphäre (z. B. durch die Sammlung und Bearbeitung von Bild- oder Tonaufnahmen) und über die Voraussetzungen einer möglichen Bewilligungspflicht, wie z. B. wenn ein öffentlich zugänglicher Ort von den Aufnahmen erfasst wird und die Aufnahmen nicht zum ausschliesslich persönlichen Gebrauch bearbeitet werden. So stellt beispielsweise eine Veröffentlichung von Aufnahmen aus dem nicht frei einsehbaren Privatbereich ohne Einwilligung der Betroffenen (Haus-/Grundstückbesitzer) eine ungerechtfertigte Persönlichkeitsverletzung dar.

Im Zusammenhang mit der Ausübung der Selbstkontrolle überarbeiteten und aktualisierten wir die **Informationen auf unserer Internetseite zum Thema «Selbstdatenschutz».**[54]

49 Tätigkeitsbericht 2014, 4.3.
50 Tätigkeitsbericht 2015, 2.5.
51 http://www.llv.li/#/11913/binding-corporate-rules.
52 Tätigkeitsbericht 2015, 2.1, sowie http://www.llv.li/#/117500/schule
53 http://www.llv.li/#/117244/drohnen und http://www.llv.li/files/dss/flyer-fl.pdf.
54 http://www.llv.li/#/1299/selbstdatenschutz.

5. WEITERE AUFGABEN

Am 1. Februar 2014 trat die Verordnung über die Datenschutzzertifizierungen in Kraft. Hersteller von Datenbearbeitungssystemen oder -programmen sowie private Personen oder Behörden, die Personendaten bearbeiten, können seither ihre Produkte, Systeme, Verfahren sowie ihre Organisation einer Bewertung durch anerkannte, unabhängige Zertifizierungsstellen unterziehen und ein Datenschutz-Gütesiegel erwerben.[55] Als erstes Unternehmen in Liechtenstein hat die **FKB** dieses **Datenschutz-Gütesiegel** erhalten. Im Zuge des Zertifizierungsverfahrens wurden bei der FKB die bestehenden Datenbearbeitungsprozesse analysiert und gegenüber einer externen Zertifizierungsstelle der Nachweis erbracht, dass die Bearbeitung der Versichertendaten im Zusammenhang mit der *Datenannahmestelle SwissDRG* für die elektronische Rechnungsstellung und -prüfung sämtlichen Datenschutzanforderungen entspricht. Die FKB macht damit nach aussen klar sichtbar, dass das Thema Datenschutz innerhalb der Organisation und im Umgang mit den Versichertendaten einen hohen Stellenwert geniesst. Das Gütesiegel schafft Vertrauen, was die Grundlage jeder Geschäftsbeziehung ist.[56]

55 Tätigkeitsbericht 2014, 5.

56 Datenschutzzertifizierung unter http://www.llv.li/#/12093/zertifizierung.

6. INTERNATIONALE ZUSAMMENARBEIT

6.1 Artikel-29-Datenschutzgruppe

Auch bei der Artikel-29-Datenschutzgruppe stand die DSGVO im Mittelpunkt.

Zu folgenden Themen der Grundverordnung wurden drei Papiere verabschiedet, die alle auf unserer Internetseite verfügbar sind (und zu denen betroffene Kreise Stellung nehmen konnten):

Art. 20 DSGVO führt das neue **Recht auf Datenübertragbarkeit** ein. Dieses Recht unterscheidet sich in vielerlei Hinsicht vom Auskunftsrecht. So hat nun eine betroffene Person unter bestimmten Umständen das Recht, dass sie die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen (Datenbearbeiter) bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format erhält. Die betroffene Person hat zudem das Recht, diese Daten einem anderen Datenbearbeiter ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten ursprünglich bereitgestellt wurden, zu übermitteln. Dieses neue Recht soll die betroffene Person stärken und ihr mehr Kontrolle über die persönlichen Daten geben. So erleichtert es den Wechsel zwischen verschiedenen Dienstleistern. Die *Artikel-29-Datenschutzgruppe hat eine Stellungnahme dazu veröffentlicht.*[57] Diese Stellungnahme beschreibt insbesondere die Bedingungen, unter denen dieses neue Recht gilt. Es berücksichtigt dabei die Rechtsgrundlage der Datenbearbeitung (Einwilligung der betroffenen Person oder die Notwendigkeit, einen Vertrag zu erfüllen) und die Tatsache, dass dieses Recht auf jene Daten beschränkt ist, die von der betroffenen Person selbst zur Verfügung gestellt wurden. Die Stellungnahme enthält auch konkrete Beispiele und Empfehlungen für die Praxis.

Bereits heute gibt es in Liechtenstein die Möglichkeit, einen **Datenschutzverantwortlichen** zu benennen. Aus dieser Möglichkeit wird mit Einführung der DSGVO eine Pflicht (wobei die Bezeichnung sich zum **Datenschutzbeauftragten** ändert). Mit der DSGVO wird die Institution des Datenschutzbeauftragten europaweit aufgewertet und der Datenschutz massgeblich gestärkt. Als wichtige Kernpunkte der DSGVO zum Datenschutzbeauftragten, die in ihrer Gesamtheit zu einer massgeblichen Stärkung des Datenschutzes führen, sind zu nennen:

- Unternehmen müssen einen *Datenschutzbeauftragten zwingend benennen, wenn die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche, regelmässige und systematische Überwachung von betroffenen Personen erforderlich machen.* Als Beispiele werden die Bearbeitung von Patientendaten in einem Spital oder die Überwachung von Geschäften oder dem öffentlichen Raum durch eine Sicherheitsfirma genannt. Auf der anderen Seite fallen Standardlösungen zur Lohnzahlung von Angestellten nicht unter den Begriff der «Kerntätigkeit». Zudem ist ein Datenschutzbeauftragter zu bestellen, wenn die Kerntätigkeit des betreffenden Unternehmens in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten, also vorwiegend besonders schützenswerter Daten, besteht.
- Der Datenschutzbeauftragte ist bei der Erfüllung seiner Aufgaben an *keine Weisungen in der Ausübung seiner Aufgaben gebunden* und darf als Folge der Erfüllung seiner Aufgaben als Datenschutzbeauftragter *nicht abberufen oder benachteiligt werden.*
- Ein Datenschutzbeauftragter kann neben seiner Tätigkeit als Datenschutzbeauftragter auch *andere Aufgaben wahrnehmen*, vorausgesetzt, dass derartige *Aufgaben und Pflichten zu keinem Interessenkonflikt führen.* Zu Interessenkonflikten würde beispielsweise die gleichzeitige Position des Datenschutzbeauftragten mit der eines IT-Verantwortlichen oder die gleichzeitige Position auf Senior-Management-Ebene bilden.
- Neben der allgemeinen fachlichen Qualifikation hat sich das *Fachwissen des Datenschutzbeauftragten insbesondere an der Komplexität der Bearbeitungsprozesse sowie am Schutzniveau der zu bearbeitenden Daten zu orientieren.*
- Eine *Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten benennen*, wenn dieser leicht erreicht werden kann. Neben der zeitlich schnellen Erreichbarkeit muss hierbei auch die sprachliche Verständigungsmöglichkeit gewährleistet sein.

Das dritte Papier beschäftigt sich mit dem **Begriff der federführenden Behörde.** Die DSGVO bewirkt eine Harmonisierung des Datenschutzes in Europa. Dazu gehört auch, dass Unternehmen, die eine Idee in verschiedenen Mitgliedsländern lancieren wollen, sich nicht mehr an jede einzelne Datenschutzbehörde wenden müssen: es wird ein One-Stop Shop

57 http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

eingeführt. Dies, damit sich Situationen wie beispielsweise bei Google Street View nicht mehr wiederholen, wo Google die Datenschutzbehörden in den einzelnen Ländern kontaktieren musste und teils sehr unterschiedliche Antworten bekam. Zukünftig wird sich die Zuständigkeit einer Datenschutzbehörde bei grenzüberschreitenden Fällen primär danach richten, wo ein Unternehmen seinen *Hauptsitz* hat. Ist dies z. B. in Wien, ist die österreichische Datenschutzbehörde federführend. Verfügt dieses Unternehmen z. B. in Madrid über eine Niederlassung oder Kunden, ist auch die spanische Behörde als «*betroffene Behörde*» beizuziehen. Dies führt auch zu einer *Harmonisierung der Aufsicht*, über Sanktionen befinden die federführende und die betroffenen Behörden. Dieses dritte Papier geht auf wichtige Einzelheiten ein und wird deswegen für die Unternehmen, aber auch für die Datenschutzbehörden in der Praxis bedeutend sein.

Zu diesen genannten sowie zu weiteren Themen hatte im Vorfeld ein *Workshop mit Interessenvertretern* stattgefunden. Die Ergebnisse des Workshops sollten dann in die erwähnten Papiere einfliessen und sind ebenfalls auf unserer Internetseite abrufbar.[58]

Noch bevor die **4. Geldwäsche-Richtlinie** überhaupt in Kraft ist, schlug die Europäische Kommission vor, sie bereits zu ändern und zu verschärfen. Zentral aus Datenschutzsicht ist der öffentliche Zugang auf Daten von *wirtschaftlich Berechtigten*.[59] Diese Revision der 4. Geldwäsche-Richtlinie war ein Thema in der Artikel-29-Datenschutzgruppe. In Abstimmung mit der Regierung nahmen wir in der *Financial Matters Subgroup* teil, welche mit dieser Sache befasst war. In dieser Gruppe äusserten wir Zweifel an der Verhältnismässigkeit eines öffentlichen Zugangs zu Daten. Wir äusserten uns in dem Sinne, dass ein Zugriff bei berechtigtem Interesse gegeben sein soll, nicht aber ein Zugriff der breiten Öffentlichkeit. In diesem Zusammenhang konnten wir auf einen Fall hinweisen, der in Frankreich vor Gericht ausgetragen wird und der unsere Ansicht bestätigt.[60] Das verabschiedete Schreiben an die Kommission nahm diese Punkte auf. Dies zeigt, was eine kleine Datenschutzbehörde bewirken kann. Es bleibt aber abzuwarten, wie die Kommission auf dieses Schreiben reagieren wird.

Ende Januar war eine von der Artikel-29-Datenschutzgruppe gesetzte Frist zur Lösungsfindung in der Sache **Safe-Harbor** abgelaufen. Der Europäische Gerichtshof (EuGH) hatte nämlich im Oktober 2015 die bis zu diesem Zeitpunkt geltende Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig erklärt.[61] Auf der Grundlage der Safe-Harbor-Entscheidung war bis zu diesem Zeitpunkt der Grossteil des Datenverkehrs zwischen den Unternehmen in Mitgliedsstaaten der Europäischen Union und den USA genehmigungsfrei. Knapp nach dem Ablauf der Frist präsentierte die Europäische Kommission eine neue Lösung, die mit den USA erzielt werden konnte, den **EU-US Privacy Shield.**[62] Die EU-Kommission traf zum Shield eine Angemessenheitsentscheidung. Unternehmen können nunmehr den Datentransfer in die USA auf den Shield stützen. Hierzu ist, wie nach Safe-Harbor, die Selbstzertifizierung des US-Datenempfängers gegenüber dem US-Department of Commerce (DoC) erforderlich, die im Rahmen einer Re-Zertifizierung jährlich zu wiederholen ist. Trotz der grundsätzlichen Begrüssung des Shields verweist die Artikel-29-Datenschutzgruppe auch auf kritische Punkte, wie die Frage nach der Massenüberwachung oder effektiver Rechtsschutzmechanismen. Zur Klärung verschiedener Fragen schuf die Gruppe FAQs für Unternehmen und betroffene Privatpersonen.[63] Es bleibt abzuwarten, wie die Datenschutzgemeinschaft dieses EU-US Privacy Shield in der Praxis aufnimmt und lebt und ob es allenfalls nochmals zu einer Überprüfung durch den EuGH kommen wird.

6.2 Europarat

Schon länger wird beim Europarat über den grenzüberschreitenden Zugriff auf Daten durch Strafverfolgungsbehörden diskutiert. Diesbezüglich fand ein Treffen der **Cloud Evidence Group** mit Datenschutzbehörden statt.[64] Zu den Plänen des Cybercrime Convention Committee (T-CY)[65] nahm die Artikel-29-Datenschutzgruppe zweimal Stellung.[66] Dabei hielt sie im Allgemeinen fest, dass es teils an einer Harmonisierung des Rechts fehle. Zudem stellen sich hier *souveränitätspolitische Fragen.* Ein Zugriff auf Daten ist schon im Inland nicht immer zu beantworten, wie auch der Europäische Gerichtshof im Urteil von 2014

58 http://www.llv.li/#/117565/datenschutzgrundverordnung-dsgvo.
59 Siehe unter 2.5.
60 http://www.conseil-etat.fr/Actualites/Communiques/Registre-public-des-trusts.
61 Tätigkeitsbericht 2015, 4.2.
62 http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.
63 WP 245 und WP 246, abrufbar unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.
64 http://www.coe.int/en/web/cybercrime/exchange-of-views.
65 http://www.coe.int/en/web/cybercrime/tcy.
66 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150925__letter_of_the_art_29_wp_on_cybercrime@octopus_ccc.pdf und http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

zur Vorratsdatenspeicherung festgehalten hat. Wenn nun Strafverfolgungsbehörden eines *anderen Landes* auf Daten eigener Unternehmen zugreifen könnten, verlöre der eigene Staat eine wichtige Rolle, die ihm bisher im Rahmen von Amts- und Rechtshilfeverfahren zukommt. Der gegenwärtige Zustand wurde wiederholt als ein «Dschungel» bezeichnet, in dem jeder etwas anderes mache und zum Teil unilateral auf Daten zugreife. Ein grosses Problem besteht also in der mangelnden Rechtsharmonisierung in diesem wichtigen Bereich. Schliesslich besteht auch das Risiko, dass bestehende Amts- und Rechtshilfeverfahren ausgehöhlt werden.[67] Das Thema ist weiterhin aktuell und soll weiter behandelt werden.[68]

6.3 Weitere internationale Zusammenarbeit

Hauptthema der Europäischen **Datenschutzkonferenz** war die verabschiedete Datenschutzreform in Brüssel. An dieser Konferenz wurden verschiedene wichtige Aspekte der DSGVO behandelt. Für uns war speziell interessant, wie sich die verschiedenen Datenschutzbehörden auf die Grundverordnung vorbereiten. Synergien zu nutzen ist uns aufgrund unserer Ressourcensituation sehr wichtig. So gab es ein Referat zum Thema: «*GDPR – what next? Practical implications for national legislators, DPAs, and Data Controllers*».[69] Bei diesem Referat wurde darüber informiert, wie die nordischen Länder (Dänemark, Finnland, Schweden, Norwegen und Island) zusammenarbeiten. Diese Zusammenarbeit scheint vorbildlich zu sein. Wir benutzten unsere Kontakte, um an wichtige Informationen zu gelangen, die uns dabei helfen, uns selbst auf die Grundverordnung vorbereiten zu können.

67 Mehr zum Thema: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168065927d.

68 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680654b2b.

69 Die Präsentation kann hier heruntergeladen werden: http://naih.hu/budapest-springconf/documents.html.

7. IN EIGENER SACHE

Im letzten Tätigkeitsbericht hatten wir darüber informiert, dass wir «weg von der Sensibilisierung, hin zu mehr Aufsicht» gehen wollen. Diese Entscheidung führte auch dazu, dass wir das Thema **Jugendliche** nicht mehr prioritär behandeln. Die Sensibilisierung von Kindern und Jugendlichen ist zwar wichtig, doch stellt sich auch die Frage der Ressourcen. Wir müssen Prioritäten setzen. Demgemäss wiesen wir bereits letztes Jahr darauf hin, dass wir uns mehr an den staatlichen Kernaufgaben orientieren wollen, wozu die Sensibilisierung von Kindern und Jugendlichen nicht gehört.

Ebenfalls im letzten Tätigkeitsbericht hatten wir über unsere erneute Evaluation im Bereich **Schengen** darüber informiert, dass bis Jahresende keine Empfehlungen aus Brüssel eingegangen waren. Daran änderte sich auch 2016 nichts: In Sachen Datenschutz ging kein Schlussbericht ein. Somit konnten wir auch im Berichtsjahr unseren Aufgaben in Bezug auf Schengen/Dublin nicht nachkommen.

Im Rahmen der **Landtagsdiskussion über unseren Tätigkeitsbericht** werden immer wieder Fragen von Abgeordneten gestellt. Wir hatten uns vor Jahren mit dem Regierungssekretär dahingehend abgesprochen, dass er die Fragen aufnimmt und bei Fragen an die Regierung diese an die jeweiligen Ministerien zur Beantwortung an den Parlamentsdienst verschickt. Im vergangenen Jahr gab es einige Fragen, die direkt an uns gerichtet waren. Die Antworten auf diese Fragen haben wir schriftlich dem Parlamentsdienst zukommen lassen. Es wurde auch eine Frage an die Regierung gestellt. Uns ist nicht bekannt, ob diese Frage beantwortet wurde.

2014 wurde die Datenschutzverordnung um eine **Gebührenpflicht** für Gutachten auf Stellungnahmen erweitert.[70] Hintergrund war eine Anregung im Landtag. Dies vor allem, um unseren beratenden Dienstleistungen etwas mehr Wert beizumessen und auch um eine kleine staatliche Einnahmequelle zu schaffen.[71] Wir wurden danach von der Regierung nach unserer Meinung gefragt. Wir gaben zu bedenken, dass sich eine solche Pflicht als kontraproduktiv erweisen könnte. Unser Ziel war und ist es, Hürden abzubauen und diejenigen zu unterstützen, die den Schutz der Privatsphäre ernst nehmen. Die eingeführte Gebührenpflicht beinhaltet einen Stundensatz zwischen 100 bis 500 Franken. Darauf haben wir bei einer Anfrage hinzuweisen. *Dies hat 2016 dazu geführt, dass Anfragen zurückgezogen oder wohl erst gar nicht gestellt wurden.*[72] Damit scheint sich die Befürchtung zu bewahrheiten, dass sich diese Pflicht zumindest teilweise als kontraproduktiv erweist. *Anfragen an andere Amtsstellen sehen eine solche Gebührenpflicht nicht vor, womit sie auch umgangen werden kann. Deshalb sprechen wir uns für eine Abschaffung der Pflicht aus. Es sollte vielmehr eine Möglichkeit zur Gebührenerhebung eingeführt werden, wenn offensichtlich Arbeit an uns «abgeschoben» wird.*

Bis anhin hatten wir einen **internen Kriterienkatalog,** der festlegte, unter welchen Voraussetzungen wir einer **Beschwerde** nachgehen. In Folge der Entscheidung, dass die Aufsicht wichtiger werden soll, haben wir diesen Kriterienkatalog angepasst und die Kriterien gelockert. Ziel ist eine einfache Handhabung und eine einheitliche Behandlung von Beschwerden. Trotz dieser Anpassung verwiesen wir in verschiedenen Fällen auf den ordentlichen Rechtsweg.[73]

Bei Abklärungen können wir Akten herausverlangen, Auskünfte einholen und uns Datenbearbeitungen vorführen lassen.[74] In der Vergangenheit stellten wir bei Kontrollen elektronischer Datenbearbeitungen fest, dass wir uns nicht in allen Fällen allein auf die Dokumentation sowie auf Systemvorführungen stützen können. In der Dokumentation sind in der Regel sämtliche Schutzmassnahmen datenschutzkonform beschrieben. Doch nicht selten weicht die **technische Implementierung** von der Dokumentation ab oder es wurden geltende Standards oder eben der **Stand der Technik ungenügend berücksichtigt.** Wir nehmen dies zum Anlass, unsere internen Vorgaben für Datenschutzkontrollen entsprechend anzupassen. Insbesondere bei sensitiven Datenbearbeitungen *werden wir zukünftig darauf achten,* inwieweit es sinnvoll ist, die *konkrete Implementierung einer organisatorischen oder technischen Schutzmassnahme zu prüfen* oder uns diese für die anschliessende Beurteilung im Detail erläutern oder vorführen zu lassen.

Die **DSGVO** bringt auch bei den Datenschutzbehörden wichtige Änderungen mit sich. Bis heute haben wir nicht einmal die gesetzliche Kompetenz über

70 Art. 33 Abs. 1 DSV.
71 Landtagsprotokoll vom 22. Mai 2013, Traktandum 11, Votum Pio Schurti.
72 Einige Fälle werden weiter oben erwähnt, siehe unter 2.1. und 2.4.
73 Siehe oben, 2.1.
74 Art. 29 und 30 DSG.

Datenschutzverstösse zu entscheiden. Dies wie auch andere Aspekte werden sich mit der DSGVO ändern. So erwähnt Art. 57 nicht weniger als 22 Pflicht-Aufgaben, wobei diese teils sehr unbestimmt sind.[75] Das heutige DSG erwähnt in den Artikeln 29 bis 32 elf solcher Aufgaben, die in der Praxis sehr unterschiedlich zu gewichten sind. Rein quantitativ wird es also zu einer Verdoppelung der Aufgaben kommen. Die DSGVO bezweckt eine Vereinheitlichung des Datenschutzes in Europa. Dies dient auch den Unternehmen, da sie sich in Zukunft nicht mehr an verschiedene Datenschutzbehörden wenden müssen. Diese Vereinheitlichung führt auch zu einer engeren Zusammenarbeit mit den anderen Datenschutzbehörden im EWR, weshalb hier mit einer Arbeitszunahme zu rechnen ist. Wir informierten im Laufe des Jahres einige Male auf unserer Internetseite zur DSGVO.

Auch intern lancierten wir ein Projekt, um uns selbst vorzubereiten.

Hinsichtlich der künftigen Errichtung der Datenschutzbehörde schlugen wir vor, die bestehende Beschränkung der Amtsdauer des Leiters der Datenschutzbehörde von acht Jahren wieder aufzuheben.[76] Eine solche Beschränkung ist nicht in allen EWR-Ländern vorgesehen, die allesamt grösser sind als Liechtenstein, sodass dort auch die Personalauswahl grösser ist. Der Hauptgrund für eine Aufhebung der Beschränkung ist jedoch, dass eine beschränkte Amtsdauer mit der Unabhängigkeit einer Datenschutzbehörde kollidieren kann.

Schliesslich bleibt abzuwarten, was aus dem Vernehmlassungsbericht aus dem Jahr 2015 zur Abschaffung der Datenschutzkommission wird, der uns auch betrifft.[77] Denn bisher ist die Vorbereitung des Budgets umständlich geregelt: teils ist das Landtagspräsidium und teils die Geschäftsprüfungskommission zuständig. Eine einheitliche Zuständigkeit wäre zu bevorzugen.

75 Vgl. Art. 57 Abs. 1 Buchstabe v: «jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten».

76 Art. 28a DSG.

77 Siehe unter 2.

8. AUSBLICK

Die DSGVO war schon im abgelaufenen Jahr ein **Schwerpunkt unserer Tätigkeiten.** Als kleine Amtsstelle sind wir gehalten, früh auf wichtige Entwicklungen zu reagieren. Da die DSGVO EWR-relevant ist, ist die Übernahme höchstens eine Frage der Zeit. Sie wird bedeutende Änderungen mit sich bringen. Die DSGVO wird uns in verschiedenen Belangen beschäftigen:

Es ist wichtig, darauf zu achten, dass die DSGVO möglichst zeitgleich mit der EU anwendbar sein wird. Dies ist nicht nur im Sinne des Datenschutzes, sondern auch vor allem derjenigen Unternehmen, die Waren oder Dienstleistungen in der EU anbieten. Ansonsten besteht das Risiko, dass sie sich nach zwei Rechtsräumen richten müssen. Dies führt zu Rechtsunsicherheit und unnötigem Aufwand bei den Unternehmen und sollte deshalb vermieden werden. Selbst die Schweiz, die die DSGVO auf Grund einer fehlenden EWR-Mitgliedschaft nicht übernehmen wird, hat bereits begonnen, gesetzgeberisch tätig zu sein. Der Bundesrat erkannte einen Bedarf zur Modernisierung der Datenschutzgesetzgebung.[78] Die DSGVO ist EWR-Materie und wird damit umzusetzen sein. Es wäre im Sinne der Rechtssicherheit, wenn die Arbeit diesbezüglich bald starten würde. Wir leisten gerne unseren Beitrag hierzu.

Dies gilt nicht nur für die Schaffung eines neuen DSG, sondern auch für die Spezialgesetzgebung, die sehr viele datenschutzrelevante Bestimmungen enthält. Es wird zu prüfen sein, ob diese den Anforderungen der DSGVO genügen.[79] Dabei ist aber zu betonen, dass unsere gesetzliche Aufgabe darin besteht, zu Gesetzesentwürfen Stellung zu nehmen und sie nicht etwa selbst auszuarbeiten. Die Mitarbeit bei der Schaffung eines gesetzlichen Rahmens rund um die DSGVO wird mit Sicherheit ein weiterer Schwerpunkt für 2017 darstellen.

Bisher bestand eine unserer gesetzlichen Aufgaben unter anderem in der Aufsicht über Unternehmen, auch in grenzüberschreitenden Fällen. Dies könnte in Zukunft nicht mehr der Fall sein. Die Aufsicht wird eben auch harmonisiert. Ob wir hierbei überhaupt eine Rolle spielen werden, ist noch nicht geklärt. Möglich und wünschbar ist natürlich, dass wir als nationale Datenschutzbehörde federführende Behörde für Unternehmen mit Hauptsitz in Liechtenstein sein können. Denkbar ist aber auch, dass wir da gar nicht mitbestimmen können. Diese Frage hängt von der EWR-Übernahme ab. Und die ist noch nicht entschieden.

Wir werden unseren «Weckruf» an betroffene Unternehmen fortsetzen. Ziel ist es, dass sie sich auf die neuen Regelungen vorbereiten können. Dies scheint vor allem dann wichtig zu sein, wenn sie in Zukunft mit Datenschutzbehörden der EU arbeiten müssen.

Ausserdem müssen wir Vorbereitungen treffen, damit wir selbst (bei rechtzeitiger EWR-Übernahme) ab Mai 2018 startklar sind.

Auch im Hinblick auf die DSGVO wollen wir unsere Kontakte ins Ausland intensivieren. Dazu bietet sich der deutschsprachige Raum speziell an. Datentransfers in Drittländer waren dem Gesetzgeber in Liechtenstein speziell wichtig, da sie mit einer Strafnorm verbunden sind. Daran wird sich auch mit der DSGVO nichts ändern. Globalisierung und Cloud Computing führten zu einer Vereinfachung solcher Datentransfers. Anbieter z. B. aus den USA stehen hier in der ersten Reihe. Wir stehen nach wie vor hinter der Idee des «Datenstandorts Liechtenstein» und werden einige ausgewählte Unternehmen darauf hin untersuchen, ob hier das DSG eingehalten wird. Dabei werden wir uns auf Vorarbeiten aus Bayern stützen.[80]

Im Ausblick des letzten Tätigkeitsberichts hatten wir erwähnt, dass wir die Stabsstelle Financial Intelligence Unit (SFIU) bei einer ordnungsgemässen **Löschung von Daten** begleiten können. Dies mussten wir leider verschieben, möchten es aber im kommenden Jahr nachholen.

Ende 2016 wurde eine erste Publikation zur **Volkszählung 2015** veröffentlicht.[81] Die bisherige Zusam-

78 https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2016/2016-12-21.html.

79 Ein Überblick auf gesetze.li zeigt eine Anzahl von über 150 Gesetzen und Verordnungen: https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=ext_search&search_text=Datenschutz&search_loc=text&lrnr=&lgblid_von=&observe_date=13.03.2017&sel_lawtype=conso&tablesel=0&submit_button=suchen.

80 https://www.lda.bayern.de/de/international_audit.html.

81 Download unter http://www.as.llv.li/ oder direkt unter http://www.llv.li/files/as/vz2015-erste-ergebnisse.pdf.

menarbeit war gut, weshalb wir auch für die Fortsetzung zuversichtlich sind. Hier gilt unser Augenmerk vor allem der Vernichtung bzw. Anonymisierung möglicher zusätzlicher «Hilfsdaten», die während der Auswertung und der Erstellung der Publikation generiert wurden.

Im Rahmen der Revision des **Sorgfaltspflichtsgesetzes** war die Löschung von Personendaten ein spezielles Thema. Wir hatten angekündigt, *eine eigene Richtlinie zum Thema Löschen zu publizieren.*[82]

Die erwähnte **Richtlinie Polizei** und Justiz[83] ist als Teil des Schengenbesitzstandes in die liechtensteinische Gesetzgebung zu übernehmen. Wir werden mit den entsprechenden Stellen Kontakt aufnehmen. Ziel ist ein richtlinienkonformer Schutz der betroffenen Bevölkerung.

Im Zuge der Einführung des **Bedrohungsmanagements** wurden unsere Anregungen anlässlich der ersten Lesung im Landtag beachtet und diskutiert. Die Regierung stellte in Aussicht, dass sie dies für die Ausarbeitung der Stellungnahme erneut prüfen wird.[84]

Die **Vorratsdatenspeicherung** ist seit langem ein Thema. Nach dem ersten Urteil aus dem Jahr 2014 äusserte sich der EuGH im vergangenen Jahr erneut zum Thema. Die Massgaben wurden bis heute nicht in Liechtenstein umgesetzt. Wir werden uns dafür einsetzen, dass dies geschieht.

Wir werden mit den beteiligten Stellen im Kontakt bleiben und unseren Beitrag zur sicheren Systemgestaltung rund um FATCA, und damit zum Automatischen Informationsaustausch (AIA), leisten.

Wir werden in Zukunft auch vermehrt darauf achten, dass betroffene Personen ihre Rechte, und vor allem das **Auskunftsrecht,** besser wahrnehmen können. Hierzu planen wir, Informationen auf unserer Internetseite auszubauen und damit Behörden/Unternehmen darüber zu informieren, wie eine Antwort auf ein Auskunftsbegehren aussehen sollte. Betroffene Personen können somit in Erfahrung bringen, was für eine Antwort sie erwarten dürfen.

Ganz allgemein werden wir vermehrt darauf achten, dass gesetzliche Bestimmungen zur vorgängigen Information bei Unternehmen gelebt werden. Denn nur wer ausreichend informiert ist, kann auch seine Rechte wahrnehmen.

Die Arbeit wird auch in Zukunft nicht ausgehen.

82 Bericht und Antrag Nr. 159/2016, S. 111.
83 Siehe unter 2.2.
84 Landtagsprotokoll vom 4. November 2016, Traktandum 26, Replik Thomas Zwiefelhofer, S. 14, 31 und 35.

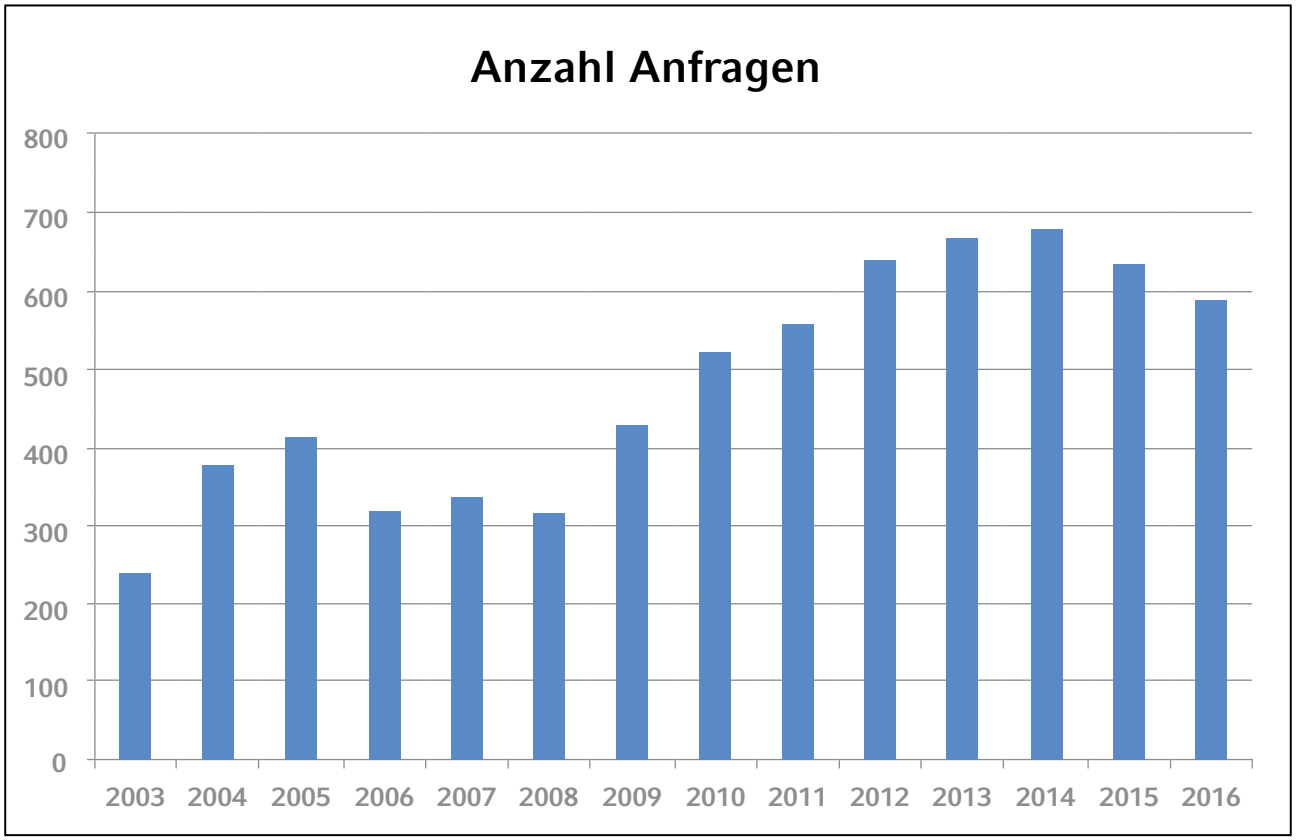
9. ANHANG

9.1 Anfragestatistik

Die Beratung privater Personen und Behörden ist eine **Kernaufgabe.** Im Berichtsjahr bearbeiteten wir insgesamt 591 Anfragen. Gegenüber dem Vorjahr bedeutet dies neuerlich einen leichten Rückgang. Die meisten Anfragen stammen nach wie vor von der Landesverwaltung und anderen Behörden. Die zweitmeisten Anfragen kamen von Unternehmen, wobei gegenüber dem Vorjahr hier eine weitere Zunahme zu verzeichnen war. Thematisch sind die meisten Anfragen genereller Natur. Zugenommen haben vor allem die Anfragen im Zusammenhang mit der Datenbekanntgabe ins Ausland sowie zur Geltendmachung gesetzlicher Rechte.

Anzahl Anfragen im Vergleich zu den Vorjahren

Die nachfolgende Abbildung zeigt die Entwicklung der Anzahl Anfragen über die vergangenen 14 Jahre:



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	2	20		41	13	21	4
Arbeitsbereich	1	1	11		4		2	1
Datenbekanntgabe Inland	6	12	5		23	1	3	5
Datenbekanntgabe Auslandsbezug	18		22	14	30		6	
Geltendmachung gesetzlicher Rechte	1		6		7	8	23	
Gesetzesvorhaben					13			
Gesundheit/Soziales				2	19	3	1	
Keine Zuständigkeit DSS			3		1		2	
Polizei/Sicherheit			1	1	7	11	1	1
Register der Datensammlungen	6		11		6			1
Schengen/Dublin				12				
Technologischer Datenschutz		2	9	9	19	2	6	4
Umsetzung/Anwendung europäischen Rechts	11		7		6	4	2	
Vernehmlassungen ohne Stellungnahme					19			
Videoüberwachung	7	2	24	7	7	2	14	3
Wirtschaft, Finanzen, Gewerbe, Versicherungen			3		1		1	
Gesamtergebnis	**57**	**19**	**122**	**45**	**203**	**44**	**82**	**19**

9.2 Newsletter

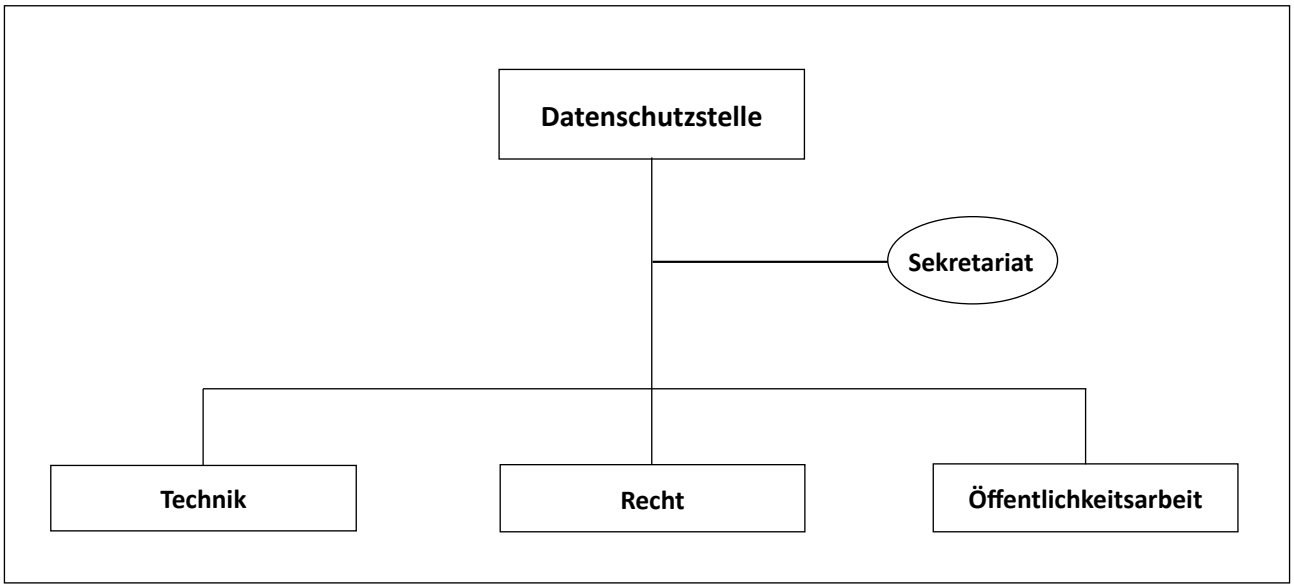
Über einen **Newsletter** informieren wir laufend über aktuelle Entwicklungen zum Datenschutz.[85] Im Jahr 2016 versandten wir 17 Newsletter; z. B. zum Thema EU-US Privacy Shield, zur DSGVO und zum Selbstdatenschutz. Wir erreichten im Januar 518 Abonnenten und konnten die Anzahl bis Dezember auf 559 Abonnenten steigern.

9.3 Veröffentlichte Publikationen

Folgende Publikationen wurden erstellt oder überarbeitet:

- Merkblatt über den Datenschutz an Schulen, Juni 2016
- Flyer mit den wichtigsten Informationen zu Drohnen, August 2016

9.4 Organigramm



85 Anmeldung zum Newsletter auf der Internetseite unter http://www.llv.li/#/49/.

DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Postfach 684
FL-9490 Vaduz

Telefon +423 236 60 90

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