DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN


# Tätigkeitsbericht 2017

## Datenschutzstelle des Fürstentums Liechtenstein

# INHALTSVERZEICHNIS

# 1. EINLEITUNG

Das Jahr 2017 stand für die Datenschutzstelle erneut im Zeichen der Entwicklungen rund um die **Datenschutz-Grundverordnung (DSGVO).** Auch wenn die DSGVO erst am 25. Mai 2018 in der EU unmittelbar anwendbar sein wird, warf sie bereits im Berichtsjahr ihre Schatten voraus und die Anfragen von Privatpersonen, Unternehmen und öffentlichen Ämtern zu den erwarteten Änderungen häuften sich. Schliesslich ist die DSGVO ein Rechtsakt mit Relevanz für den EWR und wird mit Übernahme der Verordnung in das EWR-Abkommen auch in Liechtenstein unmittelbare Anwendung finden. Selbst wenn die Übernahme erst nach dem 25. Mai 2018 erfolgen sollte, hat die DSGVO Auswirkungen auf datenverarbeitende Stellen in Liechtenstein, wenn diese Waren oder Dienstleistungen in der EU anbieten oder das Verhalten von Personen beobachten, die sich in der EU aufhalten. Als international ausgerichtetes Land wurde daher in Liechtenstein der Thematik im Berichtsjahr grosses Augenmerk geschenkt. Die entsprechenden Absätze zur DSGVO sind – wie schon zuletzt – auch in diesem Bericht speziell hervorgehoben.

Während die Kriterien für die Anwendung der DSGVO für die Unternehmen im Verordnungstext selbst geregelt sind, stellte sich die Situation für die Datenschutzstelle selbst weniger klar dar.[1] Denn die Anwendbarkeit für die Rechtsunterworfenen ist nicht gleichzusetzen mit der Geltung für die Aufsichtsbehörde, vor allem gesetzt den Fall, dass die Übernahme in das EWR-Abkommen nicht bis zum 25. Mai 2018 gelingen sollte. Angesichts dieser vielen Unbekannten war 2017 eines der herausforderndsten Jahre für uns und erschwerte die Planung und Vorbereitung der Prozesse, die notwendig sind, um gut ausgerüstet zu sein für die kommende europäische Neuregulierung des Datenschutzes. Im Rahmen unserer Möglichkeiten und unter Einbezug externer Unterstützung bauten wir aber insofern vor, als dass wir Grundlagen und Dokumente schufen, auf denen wir nun im kommenden Jahr aufbauen können.

Neben den intensiven Vorbereitungen zur DSGVO stand aber natürlich auch im Berichtsjahr die Bearbeitung von **Anfragen** im Mittelpunkt unserer Tätigkeit. Auch wenn die Anfragen quantitativ leicht zurück gingen, sind sie doch im Verhältnis zu unseren Personalressourcen auf einem nach wir vor sehr hohen Niveau und forderten uns vor allem durch eine zunehmende Komplexität. *(siehe Kapitel 2.1)*

Neben den konkreten Anfragen war die **Information und Sensibilisierung** der Öffentlichkeit ein weiteres wichtiges Anliegen, denn gerade im Hinblick auf die Änderungen ab Mai 2018 war der Bedarf hier sehr gross. Mit einem klaren Bekenntnis zu einem präventiven Datenschutz möchten wir die Öffentlichkeit für die Datenschutzrisiken sensibilisieren und auf technisch mögliche und wirtschaftlich tragfähige Lösungen für den Schutz der personenbezogenen Daten hinweisen. *(siehe Kapitel 4)*

Die Anzahl der **Stellungnahmen zu Vorlagen und Erlassen** war im Vergleich zum Vorjahr bescheidener, was vor allem daran lag, dass auf Grund des Regierungswechsels 2017 wenig Vernehmlassungen durchgeführt wurden. Wir gaben Stellungnahmen ab, wo wir direkt angesprochen wurden und Auswirkungen auf den Schutz der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten zu erwarten waren. *(siehe Kapitel 2.2)*

Grosses Augenmerk schenkten wir auch im Berichtsjahr wieder der frühzeitigen Berücksichtigung der **Datenschutzaspekte in Projekten** inner- und ausserhalb der Landesverwaltung. Eine frühzeitige Begleitung unsererseits erlaubt es zum einen mittel- und langfristig Kosten zu sparen und zum anderen sicherzustellen, dass der Schutz der personenbezogenen Daten bereits in der Entwicklungsphase die gebotene Beachtung findet. Beispielhaft kann hier das Projekt zur Modernisierung des Zentralen Personenregisters (ZPR) erwähnt werden. *(siehe Kapitel 2.5)*

Eine weitere Kernaufgabe ist die **Aufsicht.** Wir identifizieren zum einen pro-aktiv Risiken für den Schutz personenbezogener Daten in verschiedenen Institutionen des öffentlichen und des privaten Sektors und reagieren zum anderen auf Meldungen Dritter, indem wir Sachverhalte abklären und Inspektionen vor Ort durchführen. Ein Beispiel ist hier die Prüfung der Datenschutzaspekte des elektronischen Zustelldienstes der Liechtensteinischen Post. *(siehe Kapitel 3)*

Die Arbeit in der **Artikel-29-Datenschutzgruppe** stand wie schon im letzten Jahr im Zeichen der DSGVO. Neben der Teilnahme an den Sitzungen in Brüssel richteten wir unser weiteres Augenmerk auf die Auswertung der publizierten Leitlinien, welche auch für die Anwendung der DSGVO in Liechtenstein richtungsweisend sein werden. *(siehe Kapitel 6.1)*

1 Vgl. kleine Anfrage im Mai-Landtag, Stichwort: Vorabumsetzung.

Eine wesentliche Veränderung gab es auf personeller Ebene. Der langjährige Datenschutzbeauftragte Dr. Philipp Mittelberger hat sein Amt per Ende 2017 niedergelegt, um sich neuen beruflichen Herausforderungen zu stellen. Mit viel Engagement hat er die Datenschutzstelle in Liechtenstein aufgebaut und während den letzten 15 Jahren den Datenschutz wesentlich geprägt. Unter seiner Leitung hat sich die Datenschutzstelle zu einer etablierten Anlaufstelle für Fragen rund um das Thema Schutz der Privatsphäre im Lande entwickelt. Auch international ist es vor allem ihm zu verdanken, dass wir heute über ein tragfähiges Netzwerk an Kontakten zu verschiedenen Datenschutzbehörden in ganz Europa verfügen.

Der Einsatz für die Belange der Privatsphäre und der informationellen Selbstbestimmung der Bürger 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 -mitarbeitenden sowie den Kolleginnen und Kollegen in der Landesverwaltung und nicht zuletzt dem ganzen Team in der Datenschutzstelle meinen Dank für die gute Zusammenarbeit aussprechen. Aber auch all jenen, die mit Anregungen, Anfragen oder Beschwerden dazu beitrugen, dass die Belange des Schutzes der Privatsphäre berücksichtigt und oft auch verbessert werden können, gilt mein aufrichtiger Dank.

Vaduz, im März 2018

Dr. Marie-Louise Gächter
Datenschutzbeauftragte

*In diesem Text wird aus Gründen der Lesbarkeit nur die männliche Form verwendet, jedoch beziehen sich die Angaben auf Angehörige beider Geschlechter.*

# 2. ALLGEMEINE ORIENTIERUNG UND INDIVIDUELLE BERATUNG

## 2.1 Anfragen

Die nachfolgend aufgeführten Anfragen kamen aus unterschiedlichen Bereichen. Bei der Darstellung folgen wir der Gliederung früherer Tätigkeitsberichte. Es werden somit jene Anfragen zuerst dargestellt, bei denen es um die Wahrnehmung gesetzlicher Rechte ging.

**Wahrnehmung gesetzlicher Rechte**

Eine betroffene Person hat uns folgenden Sachverhalt geschildert: Sie besitze die Schweizer und Liechtensteiner Staatsbürgerschaft und kürzlich wurde sie in der Schweiz geschieden. Um auch in Liechtenstein im Personalstand als geschieden anerkannt zu werden, benötige das Zivilstandsamt (ZSA) das Schweizer **Scheidungsurteil in vollem Umfang.** Einen Auszug daraus (mit oder ohne Schwärzung) bzw. eine reine Bestätigung des Schweizer Gerichts reiche offenbar nicht aus. Das Urteil beinhaltet jedoch sämtliche Vereinbarungen, wie Abfindungen, Unterhaltszahlungen, Einkommen beider Parteien usw., die von der betroffenen Person nicht bekanntgegeben werden möchten. Wir haben die Sachlage mit dem ZSA besprochen. Im Ergebnis verblieben wir so, dass *es für betroffene Personen ausreichend ist, wenn vom zuständigen Gericht eine Kurzfassung des Scheidungsvergleiches im Original mit Rechtskraftstempel beim ZSA abgegeben wird;* z. B. wird bestätigt, dass zu einem bestimmten Datum die Scheidung erfolgte.[2]

In den vergangenen Jahren haben sich bei uns immer wieder Stellensuchende gemeldet und Fragen zu einer datenschutzkonformen **Datenbearbeitung beim Arbeitsmarktservice (AMS)** aufgeworfen.[3] Bei Erörterungen zwischen uns und dem Amt für Volkswirtschaft (AVW) war regelmässig das sogenannte Subordinationsverhältnis[4] Gegenstand für Diskussionen. So werden anlässlich von Anmeldungen beim AMS Stellensuchende unter anderem aufgefordert, ein Anmeldeformular zu unterzeichnen. Mit der Unterschrift willigen sie unter anderem ein, dass die persönlichen Daten in einem für die Stellenvermittlung erforderlichem Umfang bearbeitet und an Dritte weitergegeben werden dürfen. Sollten Stellensuchende dieses Formular nicht unterfertigen, werden von Seiten des AMS zwar keine direkten Sanktionen ausgesprochen, doch ändert dies nichts an der Praxis. *Aufgrund des erwähnten Subordinationsverhältnisses gehen wir grundsätzlich von keiner gültigen Einwilligung aus, da eine solche immer die Freiwilligkeit voraussetzt.* Wir erachten die aktuell eingeholten Einwilligungserklärungen daher als ungültigen Rechtfertigungsgrund für die Datenbearbeitung durch das AMS. *Aus diesen Gründen haben wir beim Ministerium für Infrastruktur, Wirtschaft und Sport angeregt, die einschlägigen Rechtsgrundlagen entsprechend anzupassen und eine Änderung der Praxis dahingehend vorgeschlagen, dass Stellensuchende zeitnah darüber informiert werden, an welche Arbeitgeber ihre Daten (Personalien und Lebenslauf) zum Zwecke von Stellenzuweisungen weitergeleitet werden.* Das Ministerium sieht gegenständlich keine Notwendigkeit für eine Änderung der Rechtsgrundlagen oder eine Abkehr von der bisherigen Praxis beim AMS. *Wir teilen die Ansicht des Ministeriums nicht und werden die Praxis weiter beobachten und im Zuge der Umsetzung der DSGVO gegebenenfalls erneut prüfen.*

Im Rahmen eines Löschbegehrens wurden wir angefragt, ob auch das **Löschbegehren** selbst gelöscht werden müsse. Wir hielten dazu fest, dass das Löschrecht umfassend sei und somit auch das Begehren selbst umfasse. Andererseits führt dies dazu, dass die Umstände der Löschung nicht dokumentiert werden, sodass bei einer erneuten Anfrage dieser Person darüber keine Auskunft gegeben werden kann. Deshalb rieten wir dem Datenbearbeiter, vor der Löschung vom Betroffenen eine *Einwilligung zur Aufbewahrung des Löschbegehrens zwecks Dokumentation des Vorgangs einzuholen.* Dieser Ansatz ist unserer Meinung nach jenem gegenüber zu bevorzugen, bei dem die Daten nicht gelöscht, sondern nur intern gesperrt werden. Zum Thema Löschen haben wir eine spezifische Empfehlung publiziert.[5]

Ein Dienstleistungsbetrieb fragte bei uns an, wie sich ein Beschwerdeführer oder eine Person, die einen **Austragungsanspruch durchsetzen oder Auskunftsanspruch per E-Mail einholen** möchte, dem Dienstleistungsbetrieb gegenüber legitimieren müs-

2 Art. 89 Abs. 1, 3 und 4 PGR.
3 Tätigkeitsbericht 2012, 1.1.
4 Das öffentliche Recht definiert die Beziehung zwischen Staat und dem einzelnen Bürger. Der Staat ist dem Bürger übergeordnet und ist so berechtigt, in klar definierten Bereichen rechtsgestaltend zu wirken. Das Verhältnis zwischen Staat und Bürger wird in diesem Fall als Subordinationsverhältnis bezeichnet.

5 Kapitel 4.3 sowie https://www.llv.li/files/dss/pdf-llv-dss-empfehlung-vernichtung-von-daten.pdf.

se. Jedenfalls muss sichergestellt sein, dass keiner falschen Person die Auskunft erteilt wird oder Daten Dritter gelöscht werden. *Das DSG legt fest, dass jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen kann, ob Daten über sie bearbeitet werden.* Der Inhaber der Datensammlung muss der betroffenen Person alle in der Datensammlung vorhandenen Daten und deren Herkunft mitteilen.[6] Die betroffene Person, die vom Inhaber einer Datensammlung Auskunft verlangt, *hat dies in der Regel in schriftlicher Form zu beantragen und sich über ihre Identität (z. B. durch die Vorlage einer Kopie eines amtlichen Dokuments) auszuweisen.*[7] Nachdem das DSG die Art des Nachweises der Identität jedoch nicht näher definiert, orientierten wir uns bei der Beantwortung der Frage an der DSGVO.[8] Danach können beispielsweise die Vereinbarung einer Sicherheitsfrage oder die telefonische Abfrage von Kundendetails, wie Geburtsdatum oder Mobilfunknummer, sofern diese Informationen dem Verantwortlichen zum Zeitpunkt des Ersuchens bereits vorliegen, geeignete Nachweismöglichkeiten sein. *Auch das Einloggen und Bestätigen der Anfrage in einem (Online-)Kundenportal ist eine Möglichkeit.*[9]

### Allgemeines

Der Liechtensteinischen Industrie- und Handelskammer (LIHK) ist es ein Anliegen, einen Beitrag zur **Lösung der Verkehrsproblematik während der Stosszeiten** zu leisten. Deshalb besteht seit Jahren die Arbeitsgruppe Mobilitätsmanagement, in der neben LIHK-Mitgliedsunternehmen auch die Landesverwaltung und die LIEmobil vertreten sind. Zur zielgerichteten Entwicklung von Lösungen in der Verkehrsproblematik ist die LIHK auf Informationen angewiesen, wie viele Menschen wo wohnen und arbeiten. Die in der Mobilitätsgruppe vertretenen Unternehmen sollten in diesem Zusammenhang die Wohnadresse und die Arbeitsadresse ihrer Mitarbeitenden *(keine Namen)* an das Energieinstitut Vorarlberg zur Erstellung sogenannter Arbeitspendlerströme senden. Wir teilten der LIHK mit, dass eine Datenbearbeitung zu dem obengenannten Zweck (Lösung der Verkehrsproblematik) *aufgrund des überwiegenden öffentlichen Interesses grundsätzlich mit dem Datenschutz vereinbar sei, d.h. es brauche keine explizite Einwilligung der einzelnen Mitarbeitenden.* Die der Mobilitätsgruppe angeschlossenen Unternehmen dürfen demnach die zuvor genannten anonymisierten Adressdaten an das Energieinstitut Vorarlberg senden. Wir wiesen auf die Notwendigkeit einer schriftlichen Vereinbarung mit dem Energieinstitut Vorarlberg hin, wonach die anonymisierten Adressdaten ausschliesslich zum oben genannten Zweck genutzt werden dürfen. Falls die Daten für einen anderen, in diesem Zusammenhang stehenden Zweck dienlich wären und genutzt werden sollten, müsste die Datenbearbeitung neu geprüft und bewertet werden. *Die Daten sind, sobald sie nicht mehr benötigt werden, vom Energieinstitut Vorarlberg vollständig zu löschen.*

Eine Anfrage betraf den Aufdruck des **Geburtsnamens (Ledigname) auf der Stimmkarte der Landtagswahl** 2017. Sensibel ist dies vor allem in jenen Fällen, in denen sich der Name nach Legitimationen, wie z. B. nach einer Namensänderung von unehelich geborenen oder adoptierten Kindern, zu einem späteren Zeitpunkt geändert hat. Die Regelungen betreffend das Stimmregister und insbesondere der Stimmkarten finden sich im Volksrechtegesetz (VRG).[10] Das Gesetz verlangt keine Nennung des Ledignamens auf der Stimmkarte. Nach Rücksprache mit der Regierung wird auch keine anderweitige Notwendigkeit gesehen, den Ledig- bzw. Geburtsnamen weiterhin bei Wahlen oder Abstimmungen auf der Stimmkarte aufzuführen. *Wir haben die Regierungskanzlei und das Zivilstandsamt über unser Prüfergebnis informiert. Zukünftig werden die Gemeinden den Ledignamen auf der Stimmkarte weglassen.*

### Technologischer Datenschutz

Wir wurden kurz vor Ende des Berichtsjahres von den Medien angefragt, wie die **Erstellung von Verkehrsflussanalysen** der Telecom Liechtenstein AG (TLI) im Zusammenhang mit der **Auswertung der Standortdaten von Mobiltelefonbesitzern** im Zusammenhang mit dem Schutz der Privatsphäre der Betroffenen zu bewerten sei. Konkret sollte mit einer Analyse aufgezeigt werden, wie viele Liechtensteiner Mobiltelefonbesitzer im Grenzgebiet von Österreich einkaufen. Aufgrund des sensiblen Kontextes und des allgemeinen Medieninteresses haben wir uns entschieden, den Sachverhalt zu prüfen. *Aus Sicht des Datenschutzes kommt es gegenständlich vor allem auf die Anonymisierung der ausgewerteten Daten an.* Wir haben die TLI bei einem Erstgespräch insbesondere auf eine Richtlinie hingewiesen, welche wir im April 2014 veröffentlich haben.[11]

6 Art. 11 Abs. 1 und 2 DSG.
7 Art. 1 Abs. 1 DSV.
8 Art. 12 Abs. 6 DSGVO.
9 Vgl. Erwägungsgrund 57 DSGVO.
10 Art. 17 Abs. 1 Bst. b) VRG.
11 Richtlinie über die Anwendung der Anonymisierung/Pseudonymisierung, https://www.llv.li/files/dss/pdf-llv-dss-richtlinie-anonymisierung-pseudonymisierung.pdf.

## Polizei, Sicherheit und Justiz

Anlässlich von Versteigerungen werden in der Regel **Gerichtsedikte** auf der **Internetseite des Gerichts publiziert.** Eine betroffene Person fragte an, ob eine Publikation bzw. ein bestimmtes Edikt, welches Name, Geburtsdatum, Staatsbürgerschaft, Zivilstand und Adresse umfasste, durch das Landgericht von deren Internetseite genommen werden könne. *Nachdem wir diese Angelegenheit mit dem Landgericht erörtert haben, ist diese Publikationsform umgehend dahingehend abgeändert worden, als dass künftig bei Gerichtsedikten keine persönlichen Daten mehr aufscheinen.*[12]

Ein Betroffener erkundigte sich, ob es rechtens sei, wenn die **Motorfahrzeugkontrolle (MFK) Daten** wegen Falschparkens in Feldkirch **an Privatpersonen in Österreich** bekannt gibt. Die hier massgebliche Rechtsgrundlage ist das Strassenverkehrsgesetz (SVG). Demnach muss die MFK einer Person, die ein zureichendes Interesse glaubhaft machen kann, die Namen von Fahrzeughaltern und deren Versicherer bekannt geben.[13] Dabei obliegt es der Prüfung der MFK, ob ein zureichendes Interesse vorliegt.[14] *Da die MFK die Fahrzeug- und Fahrzeughalterregister führt, und sie gemäss Gesetz die Auskunftspflicht trifft, erfolgte in der konkreten Konstellation die Auskunft der Motorfahrzeugkontrolle zu Recht.*

Wir wurden angefragt, wie **Videoüberwachungen in Gastwirtebereichen** zu beurteilen seien.[15] An diesen Orten halten sich Menschen hauptsächlich zur Erholung und zum Konsum von Speisen sowie Getränken auf. Im Allgemeinen wird in einem solchen Kontext wesentlich lockerer miteinander umgegangen, als dies etwa bei beruflichen Tätigkeiten oder privaten Besorgungen der Fall ist. Aus diesem Grund haben die Personen hier ein besonders schutzwürdiges Interesse daran, dass ihr Verhalten während ihres Aufenthalts in einem Gastbetrieb nicht permanent aufgezeichnet und nachfolgend für eine unbestimmte Zeit vorgehalten wird. Die Interessen der Besucher sind in diesen Fällen grundsätzlich höher zu bewerten als das Interesse des Betreibers einer Videoüberwachung. *Das heisst, dass in der Regel eine Videoüberwachung in Gaststätten, Restaurants oder einer Cafeteria nicht zulässig ist.*[16]

12 Vgl. Tätigkeitsbericht 2010, 1.9.
13 Art. 99b Abs. 4 SVG.
14 Vgl. Tätigkeitsbericht 2009, 1.9.
15 Art. 6a DSG.
16 Vgl. Tätigkeitsbericht 2009, 1.5.

## Wirtschaft und Finanzen

Wir wurden von der **Steuerverwaltung** (STV) angefragt, inwieweit beim **Informationsaustausch mit ausländischen Behörden** die klassische E-Mail-Kommunikation mit der Datensicherheit vereinbar sei. Grundsätzlich werden sämtliche Dokumente zwischen den Steuerbehörden über speziell dafür eingerichtete sichere Systeme (z. B. FATCA[17]) oder auf postalischem Weg ausgetauscht. Die STV wurde von zwei ausländischen Behörden angefragt, ob für gelegentliche Korrespondenzen und in bestimmten Fällen auch E-Mail genutzt werden könne. *Wir wiesen darauf hin, dass bei regelmässigem Informationsaustausch mit einer bestimmten (ausländischen) Behörde ein sicherer Kanal einzurichten sei.* Eine verschlüsselte E-Mail-Kommunikation ist eine Möglichkeit für einen solchen sicheren Kanal. Es sollte jedoch darauf geachtet werden, dass das System so konfiguriert wird, dass der Inhalt der Nachrichten vor dem Versand automatisch verschlüsselt wird, und ein manuelles Zutun des Nutzers nur in Ausnahmefällen notwendig ist.

Ein Dienstleistungsbetrieb aus dem Finanzbereich fragte uns an, ob gemäss DSG eine **Meldung von Verletzungen des Schutzes personenbezogener Daten** an die Datenschutzstelle erfolgen müsse. *Aufgrund der geltenden Gesetzeslage ist eine derartige Meldung (Data Breach Notification) noch nicht erforderlich.* Wir nutzten die konkrete Anfrage jedoch, um darauf hinzuweisen, dass mit der DSGVO – welche für den Anfrager ab Ende Mai 2018 relevant ist – eine Meldepflicht eingeführt wird. Nach der DSGVO hat der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen (Datenschutz-) Aufsichtsbehörde zu melden.[18]

## Arbeitsbereich

Wir wurden angefragt, ob es zulässig sei, von **Stellenbewerbern Strafregisterauszüge** zu verlangen. Unternehmen haben ein berechtigtes Interesse daran, nur Mitarbeitende zu beschäftigen, von denen keine Gefahr für die Sicherheit ausgeht. Gerade in Branchen wie dem Bankenwesen, dem Rechtsanwalts- und Treuhandbereich oder der Spitzentechnologie, in denen Angestellte Zugang zu sensiblen Einrichtungen und Daten erhalten, besteht das Bedürfnis, Strafregisterauszüge über Stellenbewerber anzufordern. Der Strafregisterauszug enthält besonders

17 Tätigkeitsbericht 2016, 3.
18 Art. 33 DSGVO.

schützenswerte Daten.[19] *Strafregisterauszüge dürfen von Stellenbewerbern nur in jenen Fällen verlangt werden, in denen diese zur Abklärung der Eignung des Bewerbers für eine bestimmte Stelle notwendig sind.* Hierbei ist auf den konkreten Einzelfall abzustellen. So ist es beispielsweise bei einem Chauffeur zulässig, sich nach Vorstrafen im Zusammenhang mit dem Strassenverkehr zu erkundigen. Ebenso sind bei einem Bewerber für Anlageberatungen bei einem Finanzintermediär Fragen nach Vorstrafen im Vermögensbereich zulässig. Über laufende Strafverfahren, welche voraussichtlich einen Einfluss auf die Arbeitsplatzeignung oder Vertragsdurchführung haben werden, darf sich ein potenzieller Arbeitgeber ebenfalls erkundigen. Zu ergänzen ist, dass der Bewerber die aus dem Strafregister gelöschten Vorstrafen verschweigen darf.

**Bildung**

Bereits 2014 wurden wir vom Schulamt angefragt, ob die Verwendung des Cloud-Dienstes Office 365 von Microsoft aus datenschutzrechtlicher Sicht zulässig sei. Im Ergebnis stellten wir fest, dass durch die Möglichkeit, die Lizenz für Office 365 über den Schweizer «educa.ch»-Rahmenvertrag zu erwerben, eine datenschutzkonforme Nutzung grundsätzlich gewährleistet ist.[20] Zu diesem Zeitpunkt ging es um die klassischen Office-Produkte wie Textverarbeitung, Tabellenkalkulation usw. Das Schulamt fragte nun ergänzend, ob das **Verschieben der Mail-Konten der Schüler in die Cloud von Microsoft** ebenfalls zulässig sei. Unsere Prüfung ergab, dass der sogenannte Exchange-Service in Office 365 vom oben erwähnten bestehenden Rahmenvertrag umfasst wird. Aus diesem Grund kann der Service unter denselben Bedingungen und Einschränkungen in die Cloud verschoben werden, wie dies bei den anderen von den Schulen genutzten Produkten von Microsoft der Fall ist. Wir wiesen erneut darauf hin, dass auch wenn einer Nutzung von Office 365 im Bildungsbereich nichts entgegensteht, darauf geachtet werden muss, welche Daten in der Cloud bearbeitet werden bzw. Cloud-tauglich sind. Als Grundsatz muss gelten, dass die Zurückhaltung der Nutzung des Cloud-Dienstes mit der Sensitivität der bearbeiteten Daten steigt. So ist weiter darauf zu achten, dass europäische Datacenter genutzt werden und eine Verschlüsselung von besonders schützenswerten Personendaten erfolgt. *Bei Einhaltung der zuvor genannten Bedingungen gibt es aus datenschutzrechtlichen Überlegungen keine Einwände gegen die Verwendung von Exchange in der Cloud für die Schülerkonten an Liechtensteiner Schulen.*

**Datenbekanntgabe im Inland**

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** dürften.[21] Das Unternehmen soll im Auftrag von Gemeinden die Energieverbrauchsdaten so aufbereiten, dass sie im Gemeinde-Geo-Informationssystem (GIS) hinterlegt werden können und beim jeweiligen Anklicken von Parzellen abrufbar sind. Bei der Prüfung der Rechtslage stellte sich heraus, dass für die Datenweitergabe *keine gesetzliche Grundlage* besteht. Es wurde daher angeregt, eine solche zu schaffen. Die Regierung nahm diese Anregung zur Kenntnis und prüfte die Anpassung der entsprechenden Spezialgesetze bzw. Schaffung neuer Gesetze. Sie entschied sich für die *Schaffung eines neuen Gesetzes, nämlich des Energiekatastergesetzes.* Dieses Gesetz regelt die Übermittlung diesbezüglich massgebender Daten zur Erstellung des Energiekatasters von verschiedensten Stellen an die Gemeinden.

## 2.2 Stellungnahmen zu Vorlagen und Erlassen

Die Rechtsordnung als Gesamtheit der Rechtsvorschriften regelt die Grundprinzipien der Gesellschaft und zielt auf ein geordnetes Zusammenleben der Gemeinschaft ab. Von diesen Rechtsvorschriften sind häufig auch Personendaten oder besonders schützenswerte Personendaten betroffen. Aus diesem Grund werden der Datenschutzstelle alle Vernehmlassungsvorlagen zur Information oder auch zur direkten Stellungnahme zugestellt. Nachdem die Bearbeitung der Vorlagen teils sehr zeitintensiv sein kann, müssen wir jeden Einzelfall prüfen und uns auf die Rechtssetzungsprojekte beschränken, welche den grössten Einfluss auf die Privatsphäre betroffener Personen haben.[22]

So haben wir unter anderem eine Stellungnahme zum **Gesetz auf Abänderung des Entsendegesetzes,** mit dem eine Gleichbehandlung von Schweizer und Liechtensteinischen Betrieben im Bereich der grenzüberschreitenden Dienstleistung (GDL)

19 Art. 3 Abs. 1 Bst. e) dd) DSG.
20 Tätigkeitsbericht 2014, 2.1.
21 Tätigkeitsbericht 2016, 2.1.
22 Unsere Stellungnahmen sind zum Teil abrufbar unter http://www.llv.li/#/12458/externe-stellungnahmen-zu-vernehmlassungsberichten.

erreicht werden sollte, abgegeben. Die bisher in Liechtenstein geltenden Rechtsvorschriften des Entsendegesetzes, die von jenen der Schweiz vor allem im Bereich des Vollzugs abweichen, führten zu unterschiedlichen Bedingungen der Marktteilnehmer und dadurch verbundener Ungleichbehandlung. Die Teilrevision des Entsendegesetzes in Kombination mit weiteren Massnahmen im Bereich der Behördenpraxis soll in Zukunft «gleich lange Spiesse» für die Marktteilnehmer schaffen. Aus datenschutzrechtlicher Sicht für das Entsendegesetz relevant sind insbesondere zwei Artikel des DSG. Art. 21 DSG bestimmt, dass Behörden Personendaten nur bearbeiten dürfen, wenn dafür eine gesetzliche Grundlage vorhanden ist. Art. 23 DSG wiederum legt fest, dass auch die Bekanntgabe von Personendaten durch die Behörden einer Rechtsgrundlage im Sinne von Art. 21 DSG bedarf. *Wir regten an, dass diese im Entsendegesetz noch fehlenden Bestimmungen in das zu revidierende Entsendegesetz Eingang finden sollten.* Diese Anregung floss in das Gesetz vom 5. Oktober 2017 über die Abänderung des Entsendegesetz ein.

Mit dem **Zahlungsdienstegesetz** (ZDG) wird die Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt (PSD 2) umgesetzt und die Vorgängerrichtlinie PSD 1 ersetzt. Mit PSD 2 – wie schon zuvor mit der PSD 1 – soll ein funktionierender Binnenmarkt für Zahlungsdienste erreicht werden. Gegenüber PSD 1 hat PSD 2 einerseits eine Erhöhung der zivilrechtlichen Verhaltenspflichten von Zahlungsdienstleistern zum Ziel. Zum anderen soll mit PSD 2 eine Erhöhung des Konsumentenschutzes, der Transparenz der im EWR erbrachten Zahlungsdienste und eine Verbesserung der Wettbewerbsbedingungen für Zahlungsdienstleister erreicht werden. Wir wiesen bei unserer Stellungnahme vor allem darauf hin, *dass sich die datenschutzrelevanten Begriffsbestimmungen im ZDG nicht mit jenen des DSG decken.* Insbesondere problematisch schien hier der im ZDG verwendete Begriff «sensible Zahlungsdaten»[23] im Vergleich zu «besonders schützenswerten Daten» gemäss DSG. Das DSG differenziert zwischen Personendaten[24] einerseits und besonders schützenswerten Personendaten[25] andererseits. Bei sensiblen Zahlungsdaten handelt es sich im Vergleich mit den Personendaten gemäss DSG um eine Mischbestimmung. So sind sensible Zahlungsdaten im Sinne der PSD 2 und des ZDG Daten, die genutzt werden, um einen Kunden zu identifizieren und zu authentifizieren (beispielsweise beim Login oder bei der Ausführung von Internetzahlungen). Hierzu zählen gemäss PSD 2 insbesondere ein PIN, ein Identifikationscode oder der Fingerabdruck, nicht aber Name oder Kontonummer. Bei Name oder Kontonummer handelt es sich zwar um personenbezogene Daten nach dem DSG, nicht jedoch um sensible Zahlungsdaten im Sinne des ZDG und der diesem zugrundeliegenden PSD 2. *Zusammenfassend bedeutet dies, dass die Begriffsbestimmung nach PSD 2 zu «sensiblen Zahlungsdaten» nicht mit den Begriffsbestimmungen des DSG korrespondiert, was jedoch im Sinne des Schutzes der Privatsphäre und Anwendbarkeit des Rechts wesentlich wäre.*

Im Zuge der Einführung des **Bedrohungsmanagements** wurden unsere Anregungen anlässlich der ersten Lesung im Landtag beachtet und diskutiert. Die Regierung hat in Aussicht gestellt, dass sie dies für die Ausarbeitung ihrer Stellungnahme erneut prüfen würde.[26] Ein zeitlicher Fahrplan für die zweite Lesung bzw. für die Erstellung der Stellungnahme der Regierung wurde noch nicht fixiert, weshalb uns eine Beurteilung noch nicht möglich war.

Weiter gaben wir eine Stellungnahme betreffend die Abänderung des **Gesetzes über die Landespolizei** (Polizeigesetz; POLG) ab. Unter anderem sollen mit der Gesetzesänderung neue Befugnisse im Zusammenhang mit der Verhinderung und Bekämpfung von Terrorismus und Verbrechenstatbeständen eingeführt werden. In diesem Zusammenhang können wir die Notwendigkeit der Gesetzesänderung bzw. Anpassung – beispielsweise in Bezug auf die verdeckte und gezielte Kontrolle – durchaus nachvollziehen. *Dennoch haben wir darauf hingewiesen, dass die neu hinzukommende Möglichkeit der «gezielten Kontrolle» im Bericht und Antrag jedenfalls näher erläutert bzw. ausgeführt werden sollte.* Dies vor allem, weil zum einen die unbestimmten Rechtsbegriffe, wie «schwere Straftaten», «konkrete Anhaltspunkte», «Gesamtbeurteilung einer Person» und «erwarten lässt» zu wenig differenziert sind, was zu einer unterschiedlichen Auslegung führen könnte.

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

Das Gesetz sieht vor, dass wir in hängigen Verfahren auf Ersuchen von entscheidenden Organen oder

23 Art. 4 Ziff. 33 ZDG.
24 Art. 3 Abs. 1 Bst. a) DSG.
25 Art. 3 Abs. 1 Bst. e) DSG.

26 Landtagsprotokoll vom 4. November 2016, Traktandum 26, Replik Thomas Zwiefelhofer, S. 14, 31 und 35.

Rechtsmittelbehörden Stellungnahmen zu Datenschutzfragen einreichen können. Von dieser Bestimmung wurde schon in den Vorjahren kaum Gebrauch gemacht. Das Berichtsjahr 2017 verlief in Bezug auf strittige Datenschutzfragen insofern positiv, als weder auf behördlicher noch auf privater Seite ungelöste Fälle bzw. strittige Verfahren gegeben waren. Die Möglichkeit, einen aktiven Beitrag zur Rechtsprechung in Sachen Datenschutz abgeben zu können, begrüssen wir ausdrücklich.

## 2.4 Auslandsdatentransfer und Empfehlungen bei Auslandsdatentransfer

Im Bereich Auslandsdatentransfer erreichten uns auch Anfragen zum **EU-US Privacy Shield.** Seit dem 1. August 2016 können sich Unternehmen bei Übermittlung von Daten in die USA auf den sogenannten EU-US Privacy Shield als eine der möglichen Rechtsgrundlagen für Datentransfers in die USA stützen. Dieser löste die bis 6. Oktober 2015 gültige Safe-Harbor-Entscheidung der Europäischen Kommission (2000/520/EG) ab, die vom EuGH im sogenannten Schrems-Urteil am 6. Oktober 2015 aufgehoben wurde. In ihrer Entscheidung (2016/1250) vom 12. Juli 2016 hat die Europäische Kommission festgestellt, dass die Einhaltung der im EU-US Privacy Shield verankerten Datenschutzprinzipien durch die beteiligten US-Unternehmen ein angemessenes Datenschutzniveau gewährleistet. Die unter dem EU-US Privacy Shield zertifizierten Unternehmen müssen sich jährlich neu zertifizieren. *Liechtensteinische Unternehmen können sich bei einem Datentransfer an zertifizierte US-amerikanische Unternehmen aktuell auf den EU-US Privacy Shield als Rechtsgrundlage des Datentransfers stützen.*[27]

## 2.5 Projektbegleitung

Im Rahmen der Schaffung einer gesetzlichen Grundlage von **eHealth** konnten wir weiter mitarbeiten.[28] Konkret wurden wir zu einer Produktpräsentation eingeladen, bei der bereits spezifische technische Ausgestaltungen sowie mögliche Datenflüsse diskutiert wurden. *Eine für uns zentrale Frage war und ist jene des Datenstandorts. Wir würden eine sichere Datenspeicherung in Rechenzentren in Liechtenstein begrüssen.* Wir werden das Thema jedenfalls weiter aktiv verfolgen, denn nur ein datenschutzkonformes und sicheres eHealth wird das notwendige Vertrauen der Bevölkerung geniessen können.

Seit dem 01. Juli 2016 können in allen 28 EU-Mitgliedsstaaten sowie im EWR Vertrauensdienste nach der **eIDAS-Verordnung**[29] angeboten werden. Die Verordnung enthält verbindliche europaweit geltende Regelungen in den Bereichen «Elektronische Identifizierung» und «Elektronische Vertrauensdienste». Mit der Verordnung werden einheitliche Rahmenbedingungen für die grenzüberschreitende Nutzung elektronischer Identifizierungsmittel und Vertrauensdienste geschaffen. In Liechtenstein sind Technologien und Infrastruktur zwar vorhanden,[30] jedoch ist die mehrheitlich von externen Partnern betriebene und verwendete Technologie bzw. der Service in die Jahre gekommen. Die genannte Verordnung lässt Spielraum für verschiedene Umsetzungsvarianten. *Wir wurden seitens der Projektleitung zu verschiedenen Besprechungen eingeladen und hatten so die Gelegenheit, vor allem in Bezug auf die Datensicherheit zu sensibilisieren.*

Wie im letzten Tätigkeitsbericht erwähnt, begleiten wir die Stabsstelle Financial Intelligence Unit (SFIU) bei der ordnungsgemässen **Löschung von Daten.**[31] Für das konkrete Projekt wurde festgelegt, dass eine Löschung im Zuge der Migration bestehender Datenbestände in ein neues System erfolgen soll. Die Beschaffung der neuen Softwarelösung hat sich bei der SFIU jedoch verzögert. *Da es uns auf den konkreten Prozess in der Praxis ankommt und der gesetzlich geforderte Löschzeitpunkt noch nicht erreicht ist, werden wir hier die SFIU weiter begleiten und die Löschung voraussichtlich 2018 final überprüfen.* Zwischenzeitlich haben wir die SFIU auf unsere aktuelle Richtlinie betreffend die Vernichtung von Personendaten[32] und den Umgang mit Personendaten im Testbetrieb bzw. bei der Einführung einer neuen Softwarelösung hingewiesen.

Ende 2016 wurde eine erste Publikation zur **Volkszählung 2015** veröffentlicht.[33] Wir schätzen die bisherige gute Zusammenarbeit mit dem Amt für Statistik (AS) und werden diese auch künftig fortsetzen. Hier gilt unser Augenmerk vor allem der **Vernichtung bzw. Anonymisierung** sogenannter **«Hilfsdaten»,** die während der Auswertung und der Erstellung der Publikation generiert werden. *Aus Ressourcengründen waren wir gezwungen unsere geplante Kontrolle zu verschieben. Wir sind jedoch bestrebt, diese im folgenden Jahr nachzuholen.*

27 EU-US Privacy Shield, siehe Kapitel 6.1.
28 Tätigkeitsbericht 2011, 1.4, sowie Tätigkeitsbericht 2016, 2.5.

29 Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.
30 https://www.llv.li/#/113513/elektronische-identitat.
31 Tätigkeitsbericht 2016, 2.5.
32 Siehe Kapitel 4.3.
33 Download unter http://www.as.llv.li/ oder direkt unter http://www.llv.li/files/as/vz2015-erste-ergebnisse.pdf.

Das **Zentrale Personenregister (ZPR)** wurde Ende der Neunzigerjahre erstellt und wird seither laufend ausgebaut. Die zentral geführte Datenbank wird von zahlreichen Amtsstellen genutzt und enthält unter anderem Daten sämtlicher Einwohner Liechtensteins und Daten von im Ausland wohnhaften Personen, die mit der Landesverwaltung in Kontakt getreten sind. Sie stellt ein besonders wichtiges Arbeitsinstrument in der Landesverwaltung dar. Neben technologischen und funktionalen Weiterentwicklungen wurden in den letzten Jahren zahlreiche Nachbesserungen betreffend die datenschutzkonforme Ausgestaltung vorgenommen. So werden beispielsweise seit 2013 sämtliche Lesezugriffe protokolliert, was der Überprüfung der rechtmässigen Nutzung des ZPR dient.[34] Seit dem Inkrafttreten des ZPRG 2012[35] konnten zwar viele Fortschritte den Datenschutz betreffend erzielt werden, doch sind *nach wie vor zahlreiche Punkte offen*.[36] Diese werden nun seitens der Regierung im Zuge der Modernisierung des ZPR angegangen. Wir wurden in das Projekt von Beginn an eingebunden, was wir sehr begrüssen.

34 Art. 7 Abs. 3 ZPRG.
35 Tätigkeitsbericht 2012, 1.8.
36 Tätigkeitsbericht 2015, 2.5.

# 3. AUFSICHT

2016 untersuchten wir die **Datensicherheit der elektronischen Steuererklärung (eTax).**[37] Als Ergebnis stellten wir fest, dass der Passwortschutz der eTax-Applikation für das Steuerjahr 2015 nicht dem Stand der Technik entsprach und einfach umgangen werden konnte. Dem Nutzer gegenüber wurde der Eindruck erweckt, dass ausreichende Schutzmechanismen vorhanden seien, obwohl diese in der Praxis einem Angriff nicht standgehalten hätten. Es standen in weiterer Folge mehrere Möglichkeiten zur Auswahl, die Situation im Sinne der Betroffenen zu korrigieren. Wir sprachen uns gegen die Entfernung und für die Implementierung eines sicheren Passwortschutzes der einzelnen Dateien der Steuererklärungen aus. Die Steuerverwaltung teilte unsere Ansicht nicht, sondern kündigte an, den Passwortschutz zu entfernen und die Nutzer entsprechend darüber zu informieren. *Beim ersten Programmstart der elektronischen Steuererklärung 2016*[38] *wurde der Nutzer darüber informiert, dass der Passwortschutz entfernt wurde.* Wir raten Nutzern bei der Verwendung der elektronischen Steuererklärung eTax daher insbesondere darauf zu achten, dass die Software nur auf einem geschützten Computer (Betriebssystem-Updates eingespielt, Nutzerpasswort vergeben, Festplatte bei Notebooks verschlüsselt usw.) verwendet wird.[39] Die Dateien der Steuererklärung sollten nicht in einer öffentlichen Cloud oder einer anderen externen Ablage gespeichert werden, wo Unbefugte möglicherweise Zugriff darauf haben.

Das Land und die Gemeinden setzen eine technische Lösung für den **Austausch von Meldedaten** zwischen einzelnen elektronischen Einwohnerregistern in den Gemeinden und dem Zentralen Personenregister (ZPR) ein. Uns wurde mitgeteilt, dass neben den Meldedaten auch andere Daten aus dem ZPR mit den Gemeinden ausgetauscht wurden – so auch für kurze Zeit sämtliche Ereignisse des Zivilstandsamts (ZSA).[40] Bereits im Projektstadium der Konzeption der genannten Lösung wiesen wir darauf hin, dass beim Datenaustausch die Verhältnismässigkeit in Bezug auf die zu synchronisierenden Daten zu beachten sei.[41] Für den Datenaustausch bedürfe es zudem einer Bewilligung der ZPR-Kommission. Diese wird in jenen Fällen erteilt, in denen die Daten zur Erfüllung einer gesetzlichen Aufgabe der Behörde (gegenständlich der Gemeinden) erforderlich ist, der Austausch im Sinne des DSG verhältnismässig ist und keine technischen oder rechtlichen Hindernisse entgegenstehen.[42] Durch das im ZPRG explizit vorgesehene abgestufte Berechtigungsverfahren sollen einer Behörde nur jene Daten zugänglich gemacht bzw. übermittelt werden, die sie für ihren gesetzlichen Auftrag benötigt. *Wir erachten die Übermittlung sämtlicher Ereignisse des ZSA an die Gemeinden mit den einschlägigen gesetzlichen Regelungen als nicht vereinbar.* Von Gesetzes wegen dürfen nur jene Ereignisse bekannt gegeben werden, welche die Gemeinden gemäss gesetzlichem Auftrag für ihre Arbeit benötigen. Es liegt daher an den Gemeinden entsprechend zu begründen, weshalb sie bestimmte Daten aus dem ZPR zur Erfüllung ihrer gesetzlichen Aufgaben benötigen.

Bei einem im **Bereich E-Marketing** tätigen Unternehmen führten wir eine Sachverhaltsabklärung in Folge mehrerer bei uns eingegangener Beschwerden durch. Insbesondere stellte sich für uns die Frage, ob bei den zum Kundenstamm dieses Unternehmens gehörenden Personen jeweils eine Einwilligungserklärung zur Bearbeitung ihrer Daten vorlag, die auch das Einverständnis zur Weitergabe der entsprechenden Kundendaten an sogenannte Sponsoren[43] umfasste. Eine Einwilligung nach dem DSG ist jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass Daten, die sie betreffen, bearbeitet werden.[44] Gemäss DSG ist eine Einwilligung in der Regel überdies erst dann gültig, wenn sie nach angemessener Information freiwillig erfolgt.[45] *Einzig im Zusammenhang mit der regelmässigen Prüfung der Notwendigkeit der Aufbewahrung von Daten über die Gewinnspielteilnehmer war eine Empfehlung auszusprechen. Das Unternehmen teilte uns mit, dass es dieser vollumfänglich nachkommen wird.*

Die BENDURA BANK AG (vormals Valartis Bank (Liechtenstein) AG) veröffentlichte am 17. November 2016 eine Pressemitteilung, in der sie die Öffentlichkeit darüber informierte, dass sie Ziel eines **Hacker-**

37 Tätigkeitsbericht 2016, 3.
38 http://www.llv.li/#/110926/etax-herunterladen.
39 Informationen zum das Thema IT-Sicherheit unter https://www.bsi-fuer-buerger.de/.
40 Ereignisse wie Geburt, Heirat, Scheidung, Einbürgerung usw.
41 Tätigkeitsbericht 2014, 2.5.
42 Art. 9 ZPRG.
43 Im konkreten Fall erhalten Sponsoren, meist Unternehmen, die sich finanziell an einer Marketing-Aktion beteiligen, die Angaben von Teilnehmern (z. B. eines Gewinnspiels) zur weiteren Verwendung für Marktforschung oder für weitere Werbeangebote.
44 Art. 3 Abs. 1 Bst. m) DSG.
45 Art. 4 Abs. 4 DSG.

**angriffs** geworden sei. Da durch diesen Angriff die Möglichkeit einer Verletzung der Persönlichkeitsrechte nicht ausgeschlossen werden konnte, nahmen wir dies zum Anlass, eine entsprechende Sachverhaltsabklärung durchzuführen. Diese ergab, dass die zum Zeitpunkt der Entwendung der Daten von der Bank verwendete Software zwischenzeitlich ersetzt bzw. aktualisiert wurde. *Die verwendeten Systeme wurden zusätzlich gehärtet und lassen einen Datendiebstahl, wie er in der Pressemitteilung beschrieben wurde, nicht mehr zu. Wir sahen aus diesem Grund keine Notwendigkeit, Empfehlungen auszusprechen oder weitere Massnahmen zu setzen.*

Wir stehen nach wie vor hinter der Idee des **«Datenstandorts Liechtenstein».** In diesem Zusammenhang haben wir speziell im Hinblick auf den Datentransfer ins Ausland einige ausgewählte Unternehmen auf Einhaltung des Datenschutzgesetzes (DSG) untersucht. Dabei stützten wir uns auf Vorarbeiten des Bayerischen Landesamts für Datenschutzaufsicht.[46] Diese Datenschutzbehörde hatte einen spezifischen Fragebogen erarbeitet, der verschiedenste Aspekte des Auslandsdatentransfers abdeckte.[47] Dieser Fragebogen sollte insbesondere darüber Aufschluss geben, wo es bei den Unternehmen Schwachstellen im Auslandsdatentransfer gibt und in welchen Punkten möglicherweise gesetzlichen Verpflichtungen nicht oder nicht vollständig nachgekommen wird. *Die Auswertung der von den Unternehmen retournierten Fragebögen ergab, dass bei einigen Unternehmen durchaus Anpassungsbedarf bestand.* Dies insbesondere im Zusammenhang mit den Melde- und Bewilligungspflichten bei Verwendung von Standardvertragsklauseln als Rechtsgrundlage des Auslandsdatentransfers.

46 https://www.lda.bayern.de/de/index.html.
47 https://www.lda.bayern.de/de/international_audit.html.

# 4. INFORMATION UND SENSIBILISIERUNG DER ÖFFENTLICHKEIT

## 4.1 Veranstaltungen

Der **Datenschutztag** stand in diesem Jahr unter dem Motto «Maschinen statt Gefühle – wer trifft die besseren Entscheidungen?». Navigationsgeräte oder Handys und andere digitale Assistenten unterstützen uns ständig und machen uns Vorschläge. Wollen wir diese überhaupt? Es ging um das Spannungsverhältnis zwischen den unbestrittenen Vorteilen der Nutzung von digitalen Assistenten – wie mehr Komfort oder Effizienz – und dem schmalen Grat zum Verlust der Entscheidungsautonomie jedes Einzelnen. Datenschutz wird oft auch als das «Recht auf informationelle Selbstbestimmung» bezeichnet. Bestimmen wir noch selbst über uns, wenn wir ständig von digitalen Assistenten unterstützt werden? Oder treffen wir (un-)bewusst die Entscheidung, Verantwortung an diese Assistenten abgeben? Was bedeutet es für die Gesellschaft, wenn wir nicht mehr selbst entscheiden? Wird es dazu kommen, dass Maschinen zukünftig eigenständig für uns Entscheidungen treffen? Diese schwierigen und hochaktuellen Fragen wurden an der Veranstaltung diskutiert. Dabei ging es auch um die Frage, wie weit die Forschung und der Fortschritt gehen sollten. Als Beispiel sei das selbstfahrende Auto genannt: Bei einem unvermeidbaren Unfall trifft heute noch der Mensch die spontane Entscheidung, wie er den Schaden zu minimieren versucht. Bei selbstfahrenden Autos entscheidet aber das Auto selbst. Sollen dabei die Passagiere oder die Passanten geschützt werden? Dies ist eine Frage nach Werten und Ethik in der Gesellschaft, die den Datenschutz betrifft, aber auch weit darüber hinausgeht. Auf unserer Internetseite ist ein Interview zu diesem Thema mit Dr. Philipp Mittelberger abrufbar.[48]

In Kooperation mit der Universität Liechtenstein nahmen wir an einer **Diskussionsveranstaltung mit dem Titel «Update: Vorratsdatenspeicherung»** teil. Der Europäische Gerichtshof (EuGH) äusserte sich in zwei Urteilen zur Vorratsdatenspeicherung.[49] Während das erste Urteil die auch von Liechtenstein umgesetzte Richtlinie zur Vorratsdatenspeicherung aufgehoben hatte, setzte sich das zweite Urteil mit nationalen Regelungen auseinander. Gemein ist beiden Entscheidungen die klare Betonung des EuGH, dass eine unterschiedslose Speicherung von Daten der ganzen europäischen Bevölkerung nicht verhältnismässig ist.[50] Die Veranstaltung bot Gelegenheit, über die Rechtmässigkeit der geltenden Rechtslage zu diskutieren und sich über die Implikationen der Entscheidung des EuGH für Liechtenstein auszutauschen. Wir wiesen in der Diskussion auch darauf hin, dass der Bericht und Antrag der Regierung zur Zukunft der Vorratsdatenspeicherung zu diesem Zeitpunkt kürzlich verabschiedet worden war und dem Landtag vorgelegt werden sollte.[51]

Am alle zwei Jahre stattfindenden **Zertifikatslehrgang Compliance Officer** der Universität hatten wir wieder die Möglichkeit, detailliert über den Datenschutz und die dortigen aktuellen Entwicklungen zu informieren. Dabei ging es um folgende Themenblöcke: Grundsätze des Datenschutzes und Tätigkeiten der Datenschutzstelle, die DSGVO als ein entscheidender Meilenstein im Datenschutz, Datensicherheit sowie Werkzeuge und Methoden für Compliance im Datenschutz. Wir aktualisierten die bereits seit dem letzten Lehrgang vorhandenen Informationen und reicherten diese vor allem mit aktueller Rechtsprechung sowie Entwicklungen betreffend die DSGVO an. Dieser Lehrgang soll weiterhin alle zwei Jahre durchgeführt werden, wodurch wir ein regelmässiges Forum bekommen. Dies ist sehr zu begrüssen.

**Datenschutz-Grundverordnung**

Wir haben unsere «Weckrufe» an von der DSGVO betroffene Unternehmen fortgesetzt. Unser Ziel war es vor allem zu gewährleisten, dass sie sich zeitgerecht auf die neuen Regelungen vorbereiten können. Denn die DSGVO gilt ab dem 25. Mai 2018 nicht nur für EU-Länder. Die Verordnung ist auch für Unternehmen aus EWR- oder anderen Ländern massgebend, wenn sie Waren oder Dienstleistungen in der EU anbieten oder das Verhalten von Personen beobachten, die sich in der EU aufhalten.[52]

48 http://www.llv.li/files/dss/wirtschaftregional-20170121.pdf.

49 Urteil des EuGH vom 8. April 2014 (http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=DE), vgl. Tätigkeitsbericht 2014, 4.3, und Urteil des EuGH vom 21. Dezember 2016 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&doclang=DE), vgl. Tätigkeitsbericht 2016, 4.3.

50 So betont er in Randnummer 106: «Eine solche [unterschiedslose] Regelung verlangt keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit. Insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen könnten (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 59)».

51 Siehe Kapitel 7.

52 Vgl. dazu das extraterritoriale Prinzip nach Art. 3 DSGVO.

In diesem Zusammenhang haben wir mehrere Veranstaltungen durchgeführt. So organisierten wir beispielsweise speziell für die **betrieblichen Datenschutzverantwortlichen einen Kurs über die Grundlagen des Datenschutzes** mit Betonung der DSGVO, wobei die Grundlagen auch mit Technikbezug erklärt wurden. Die Veranstaltung war mit 30 Teilnehmern sehr gut besucht. Es fand eine rege Diskussion statt, die dem Erfahrungsaustausch diente.

Auf unsere Initiative hin fand an der Universität Liechtenstein eine ganztägige **Veranstaltung zur DSGVO** statt. Der erste Teil der Veranstaltung richtete den Fokus auf die neuen Vorgaben, die mit der DSGVO einzuhalten sind. Unser Beitrag hatte den Titel *«Von der Bedeutung(slosigkeit) der Datenschutzstelle in der künftigen Aufsicht über liechtensteinische Unternehmen»* und beschäftigte sich mit der Wichtigkeit einer rechtzeitigen Übernahme der DSGVO in den EWR. Diese ist aus unserer Sicht für die heimischen Unternehmen wichtig, da sie sonst zukünftig Vorgaben zweier Rechtsräume erfüllen müssten. Ausserdem können wir als Datenschutzbehörde nur in diesem Fall im Aufsichtsmechanismus auf EU-Ebene mitwirken. Im zweiten Teil erhielten die Teilnehmenden wichtige Tipps zur Vorbereitung der Umsetzung. Vor allem wurde aufgezeigt, welche Instrumentarien und Prozesse Unternehmen bei der Umsetzung implementieren müssen. Im Rahmen zweier Podiumsdiskussionen zu den jeweiligen Themen brachten die Teilnehmenden Fragen aus der Praxis ein.

Im September luden wir zum bereits siebten **Jahrestreffen der betrieblichen Datenschutzverantwortlichen** ein, um über aktuelle Entwicklungen im Datenschutzbereich im Allgemeinen sowie über die kommende DSGVO im Besonderen zu informieren. Die Teilnehmerzahl ist im Vergleich zu den Vorjahren weiter gestiegen. Das rege Interesse zeigt, dass der Bedarf an Aufklärung und Austausch zum Thema Datenschutz und vor allem zur DSGVO sehr gross ist. Im Rahmen dieses Jahrestreffens waren die Datenschutzverantwortlichen aufgerufen, ihre Erfahrungen im Zusammenhang mit der Implementierung der DSGVO in ihren Unternehmen vorzustellen. Eine Vertreterin einer Versicherung stellte umfassend die in ihrem Unternehmen unternommenen Anstrengungen und verwirklichten Massnahmen als Vorbereitung auf die DSGVO vor. *Dabei wurde der grosse Anpassungsbedarf und der nicht zu unterschätzende Zeitbedarf und Zeitrahmen bei der Umsetzung der DSGVO in die betriebliche Praxis in aller Deutlichkeit für alle Beteiligten der Veranstaltung sichtbar.*

## 4.2 Veröffentlichungen in den Medien

Dem Liechtensteiner Vaterland gaben wir ein Interview zu **Darknets,** in dem es auch um die Überwachung im Allgemeinen ging.[53] Uns war es wichtig darzulegen, dass Internet und Privatsphäre sowohl rechtlich als auch technisch durchaus miteinander vereinbar sind. So sind der Überwachung im Internet Grenzen gesetzt. Beispielsweise hat der EuGH Wege zur Ausgestaltung der Vorratsdatenspeicherung aufgezeigt, die in Liechtenstein neu geregelt wurden.[54] Ebenso tummeln sich nicht nur Kriminelle im so genannten dunklen Teil des Internets. Die Technologien werden auch zum Schutz der Privatsphäre und Identität für das reguläre Surfen im Internet genutzt. *Nutzer verwenden diese Techniken zur Verschleierung ihrer Identität in jenen Fällen, in denen sie sich frei und geschützt vor Datensammlern, Tracking, Profiling und dergleichen im Internet bewegen möchten.* Dabei nehmen sie bewusst die mit der Sicherheit einhergehenden Einschränkungen, wie vor allem die verminderte Nutzerfreundlichkeit, in Kauf.

Im Zusammenhang mit der **DSGVO** gaben wir mehrere Interviews in den Liechtensteinischen Tageszeitungen. Anlässlich der Halbzeit in der zweijährigen Vorbereitungsphase im Mai 2017[55] erläuterten wir umfassend, dass die DSGVO zahlreiche Änderungen für die Datenbearbeiter bzw. nach der DSGVO für die Verantwortlichen mit sich bringt. Die Änderungen betreffen vor allem die Transparenz und Nachweisbarkeit der gesetzeskonformen Datenbearbeitung. *Wir wiesen ebenfalls darauf hin, dass Unternehmen sich frühzeitig mit der DSGVO beschäftigen und den nicht unerheblichen Aufwand – zumindest für die interne Evaluation, ob und in welcher Form ein Unternehmen überhaupt von der DSGVO betroffen ist – nicht unterschätzen sollten.*

In einem weiteren Medienbericht betonten wir, dass wir die DSGVO vor allem als Chance für den **«Datenstandort Liechtenstein»** sehen. Daten sollen im EWR möglichst ohne Hindernisse fliessen. Das war auch bisher schon der Fall. Unternehmen ausserhalb des EWR, vor allem in den USA oder auch der Schweiz, werden dagegen stärker in die Pflicht genommen. Als EWR-Mitglied hat Liechtenstein die Möglichkeit, am freien Datenverkehr teilzunehmen und hat nun die *Chance, vor allem von den Vorteilen zu profitieren.*

53 https://ligital.li/2017/11/ein-bisschen-darknet-fuer-alle/.
54 Tätigkeitsbericht 2014, 4.3 und Kapitel 7.
55 Die DSGVO wurde am 04. Mai 2016 im Amtsblatt der Europäisches Union veröffentlicht (http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L:2016:119:TOC) und trat somit gem. Art. 99 Abs. 1 DSGVO am 25. Mai 2016 in Kraft. Anwendbar ist sie ab dem 25. Mai 2018; Art. 99 Abs. 2 DSGVO.

Die Landesverwaltung publiziert seit 2015 vier Mal jährlich eine Mitarbeiterzeitung, die an sämtliche Mitarbeiter verteilt wird. In zwei Ausgaben hatten wir die Möglichkeit, die Leser mit kurzen Sicherheitstipps betreffend den Schutz der Privatsphäre zu sensibilisieren. Im ersten Beitrag wiesen wir darauf hin, dass Nutzer von Smartphones bei zahlreichen Apps selbst festlegen können, welche Daten über ihre Person oder auch über die Nutzung der jeweiligen App an den Hersteller oder an Dritte weitergegeben werden. Die Grundeinstellungen sind in vielen Fällen nicht sehr datenschutzfreundlich. So lohnt es sich, die Einstellungsmöglichkeiten direkt nach der Installation einer App zu kontrollieren. Im zweiten Beitrag wiesen wir auf die Gefahren hin, die mit digitalen Weihnachtskarten verbunden sind. Gerade zur Weihnachtszeit klicken Empfänger zu leichtfertig und sorglos auf die Anhänge eingehender Mails oder folgen den in den E-Mails enthaltenen Links. Doch oftmals tarnen sich Phishing-Mails als saisonale Glückwunschkarten, die es Angreifern ermöglichen, an vertrauliche und persönliche Daten zu gelangen.

## 4.3 Internetseite

Im Rahmen der Revision des Sorgfaltspflichtsgesetzes (SPG) war die Löschung ein spezielles Thema. Wir hatten angekündigt, *eine spezifische Empfehlung dazu zu publizieren.*[56] Dieser Ankündigung sind wir nachgekommen und haben eine **Empfehlung zur Vernichtung von Personendaten** veröffentlicht.[57] Ziel der Empfehlung ist es, den Inhabern von Datensammlungen *Hilfestellung bei der Einhaltung ihrer Verpflichtung zur Vernichtung personenbezogener Daten zu geben.* Das Vernichten von Personendaten stellt eine Konkretisierung des im DSG normierten Verhältnismässigkeitsprinzips dar. Der Inhaber einer Datensammlung darf nur diejenigen Daten bearbeiten, die für die Erfüllung einer jeweils konkreten Aufgabe (Zweckerreichung) unbedingt notwendig und geeignet sind. Im Zeitalter des Datensammelns und der vernetzten Systeme ist die praktische Umsetzung zur Einhaltung der Bestimmungen an eine angemessene Vernichtung in vielen Fällen nicht einfach. Die erwähnte Empfehlung erklärt die wesentlichen Merkmale sowie begriffliche und technische Abgrenzungen und stellt abschliessend mögliche Vorgehensweisen für die datenschutzkonforme Vernichtung vor. Das Löschrecht wird im Rahmen der DSGVO gestärkt. Wo es zweckmässig und sinnvoll ist, wird deshalb bereits auf die DSGVO hingewiesen. Die Empfehlung umfasst jedoch keine detaillierten Ausführungen zu spezifischen Bestimmungen der DSGVO, wie beispielsweise das Recht auf Löschung («Recht auf Vergessenwerden») oder das Verfahren betreffend die Informationspflicht in Bezug auf die Löschung aller Links zu Personendaten oder Kopien oder Replikationen dieser Daten aus öffentlich zugänglichen Kommunikationsdiensten. Hierzu wird der Europäische Datenschutzausschuss *(engl. Data Protection Board)*[58] entsprechende Leitlinien und Empfehlungen bereitstellen.

Zudem stand die **DSGVO** auch in diesem Jahr im Mittelpunkt der Veröffentlichungen auf unserer Internetseite.[59] Regelmässig informierten wir auch über aktuelle Entwicklungen der Artikel-29-Datenschutzgruppe und verlinkten deren Stellungnahmen.

56 Bericht und Antrag Nr. 159/2016, Seite 111.
57 Empfehlung zur Vernichtung von Personendaten, https://www.llv.li/files/dss/pdf-llv-dss-empfehlung-vernichtung-von-daten.pdf.
58 Art. 68 DSGVO.
59 Auf der Internetseite der DSS (www.dss.llv.li) unter Datenschutz-Grundverordnung (DSGVO).

# 5. WEITERE AUFGABEN

Gemäss Zustellgesetz hat die Liechtensteinische Post AG («Post») als Betreiber des **elektronischen Zustelldienstes (eZD) jährlich den Nachweis über die Gewährleistung des Datenschutzes** im Sinne der Datenschutzgesetzgebung und der Datensicherheit zu erbringen.[60] Wir führten in diesem Zusammenhang mit Unterstützung des Amtes für Informatik als Vertreter der Landesverwaltung eine Sachverhaltsabklärung durch, welche den durch die Landesverwaltung als Dateninhaber ausgelagerten Betrieb des eZD an die Post und an die beteiligten Auftragsdatenbearbeiter umfasste. Zusammengefasst haben wir festgestellt, dass die Bearbeitung von Personendaten durch die Post im Kern datenschutzkonform erfolgt. Insgesamt ist die Haltung der Post gegenüber dem Datenschutz und dem Schutz der Persönlichkeit der Betroffenen, namentlich den Empfängern von Behördenbriefen, sowie gegenüber der Datensicherheit als positiv hervorzuheben.

Ebenfalls positiv zu erwähnen sind die Zusammenarbeit und das Umfeld während der Sachverhaltsabklärung. Der eZD wird bisher wenig genutzt. Die Post als Betreiber ist aus diesem Grund bestrebt, die laufenden Kosten des Dienstes vor allem aufgrund der geringen Nutzerzahl niedrig zu halten. Nichtsdestotrotz sind die Datenschutzgesetzgebung und die Datensicherheit einzuhalten. *Im Rahmen der gegenständlichen Sachverhaltsabklärung haben wir in verschiedenen Punkten einen Änderungsbedarf festgestellt und entsprechende Empfehlungen und Bemerkungen ausgesprochen.* Diese betrafen vor allem die Informationspflichten gegenüber den Empfängern von Behördenbriefen sowie Nachbesserungen bei der Protokollierung und dem aktiven Monitoring zwecks Erkennung von Bedrohungen beispielsweise durch Schadsoftware und/oder anderen Angriffen auf die bearbeiteten Daten.

60 Art. 3b Abs. 4 Zustellverordnung (ZustV).

# 6. INTERNATIONALE ZUSAMMENARBEIT

## 6.1 Artikel-29-Datenschutzgruppe

Auch bei der Artikel-29-Datenschutzgruppe stand, wie schon im letzten Jahr, die DSGVO im Mittelpunkt. Wir hatten über die europäische Datenschutzreform bereits berichtet.[61] So wurden im laufenden Berichtsjahr eine Reihe weiterer Leitlinien verabschiedet oder bereits existierende Stellungnahmen im Hinblick auf die Erfordernisse der Bestimmungen der DSGVO angepasst.

Zu folgenden Themen der Grundverordnung wurden Dokumente verabschiedet, die alle auf unserer Internetseite verlinkt sind:[62]

Die Datenschutzgruppe hatte Ende des letzten Jahres drei **Leitlinien** veröffentlicht: **«Recht auf Datenübertragbarkeit», «Datenschutzbeauftragter»** und die **«Federführende Behörde».** In einer anschliessenden sechswöchigen Konsultationsphase konnten Interessierte Stellungnahmen und Kommentare zu den genannten Leitlinien an die Artikel-29-Datenschutzgruppe senden. Die eingegangenen Stellungnahmen wurden geprüft und entsprechend in eine finale Fassung eingepflegt. Die wesentlichen Punkte haben wir schon im letztjährigen Tätigkeitsbericht erwähnt.[63]

Ferner wurden von der Artikel-29-Datenschutzgruppe **Leitlinien zur Datenschutz-Folgenabschätzung** (DSFA) erstellt. Auch hier wurde nach dem zuvor erwähnten zweistufigen Verfahren (öffentliche Konsultation) und finaler Verabschiedung vorgegangen. So wird mit der DSGVO den für die Datenverarbeitung Verantwortlichen kein konkretes DSFA-Verfahren vorgeschrieben, sondern vielmehr die Möglichkeit gegeben, eigene Rahmenbestimmungen in Ergänzung der bestehenden Arbeitsmethoden einzuführen. Voraussetzung ist jedoch, dass die in Art. 35 DSGVO beschriebenen Komponenten darin Berücksichtigung finden. Solche Rahmenbestimmungen können speziell auf den für die Datenverarbeitung Verantwortlichen zugeschnitten sein oder für eine gesamte Branche gelten.[64] Datenschutz-Folgenabschätzungen können als eine Weiterentwicklung der Vorabkontrollen nach der Datenschutzrichtlinie gesehen werden.[65] So sind Unternehmen unter bestimmten Umständen von der Erstellung einer solchen Abschätzung befreit, z. B. in jenen Fällen, in denen die Bearbeitung auf einer nationalen Rechtsgrundlage, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften die konkrete Datenbearbeitung regelt sowie bereits mit dem Erlass dieser Rechtsgrundlage eine entsprechende Folgenabschätzung erfolgte (Vorabkontrolle).[66] Für Unternehmen in Liechtenstein ist hier vor allem zu berücksichtigen, dass sie sich in der Regel nicht auf diese Ausnahmen stützen können, da die Vorabkontrolle im DSG nicht vorgesehen ist.[67]

Einwilligung und Transparenz sind grundlegende Prinzipien des Datenschutzes. Eine Einwilligung nach der DSGVO setzt sich aus mehreren Elementen zusammen. Gemäss Legaldefinition[68] ist eine **Einwilligung** der betroffenen Person dann gegeben, wenn sie erstens freiwillig, zweitens für den bestimmten Fall, drittens in informierter Weise, viertens unmissverständlich und fünftens in einer eindeutigen erklärenden und aktiven Handlung gegeben wird. Von der Artikel-29-Datenschutzgruppe wird jedes der erwähnten Elemente analysiert und einer differenzierten Betrachtung unterzogen. Das Element «Freiwilligkeit» sieht die Datenschutzgruppe beispielsweise dann in Gefahr, wenn ein Machtungleichgewicht zwischen Datenbearbeiter und betroffener Person besteht. Sie nennt hier als Beispiel die Beziehung zwischen Arbeitgeber und Arbeitnehmer. Abgrenzungsfragen ergeben sich auch bezüglich der anderen Tatbestandsmerkmale an eine wirksam erteilte Einwilligung. Eine vertiefte Analyse und differenzierende Betrachtung unter Aufzeigung der jeweils gegebenen neuralgischen Punkte nimmt die Artikel-29-Datenschutzgruppe auch bei den anderen Tatbestandsmerkmalen an eine wirksame Einwilligung vor. Fazit: *Für eine wirksame Einwilligung muss jedes Element geprüft werden und auch erfüllt sein.* Eine bestehende Einwilligung setzt laut Artikel-29-Datenschutzgruppe voraus, dass diese daraufhin überprüft werden muss, ob sie den Anforderungen an eine wirksame Einwilligung gemäss DSGVO genügt. Das Ergebnis kann durchaus dazu führen, dass die Einholung einer neuerlichen Einwilligung notwendig ist.

61 Tätigkeitsbericht 2016, 6.1.
62 https://www.llv.li/#/118188/artikel--datenschutzgruppe.
63 Tätigkeitsbericht 2016, 6.1.
64 https://www.llv.li/files/dss/leitlinien-folgenabschatzung.pdf.
65 Art. 20 RL 95/46/EG.
66 Vgl. Art. 35 Abs. 10 DSGVO.
67 Vgl. dazu den Art. 20 der RL 95/46/EG, der in Liechtenstein nicht in nationales Recht umgesetzt wurde.
68 Art. 4 Ziff. 11 DSGVO.

Der Grundsatz der **Transparenz** ist eng verzahnt mit dem Grundsatz der Einwilligung. Gemäss dem Grundsatz der Transparenz sind einer betroffenen Person die über sie verarbeiteten Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache mitzuteilen.[69] Der Grundsatz der Transparenz soll vor allem sicherstellen, dass eine betroffene Person einerseits ihre Betroffenenrechte, andererseits aber auch ihr Recht, über die eigenen Daten zu verfügen, wahrnehmen kann. In Art. 12 DSGVO wird der Grundsatz der Transparenz zum Beispiel durch Informationspflichten bei der Erhebung von personenbezogenen Daten sowie durch das Auskunftsrecht der betroffenen Personen näher ausgestaltet. Der Grundsatz der Transparenz ist somit im Datenschutz zentral. *Dies bedeutet für die Verantwortlichen, dass die Datenverarbeitung und die Prozesse auf die diesbezüglich in der DSGVO niedergelegten Erfordernisse abzustimmen sind, um den festgelegten Bedingungen zu entsprechen.*

Die Artikel-29-Datenschutzgruppe veröffentlichte Leitlinien betreffend die **Meldung von Verletzungen des Schutzes personenbezogener Daten.**[70] Darin wird vor allem ausgeführt, was unter einer Verletzung des Schutzes personenbezogener Daten zu verstehen ist, und welche Verpflichtungen in Bezug auf die Meldung an die Aufsichtsbehörde oder die Betroffenen zu beachten sind.[71] Erwähnenswert ist hier, dass nicht nur Verletzungen der Vertraulichkeit – z. B. durch eine unbefugte oder versehentliche Offenlegung personenbezogener Daten – eine Meldepflicht begründen können. Ebenso ist bei unbefugter oder versehentlicher Änderung personenbezogener Daten (Verletzung der Integrität) oder bei versehentlichem oder unbefugtem Verlust des Zugriffs auf oder der Vernichtung von personenbezogenen Daten (Verletzung der Verfügbarkeit) eine mögliche Meldepflicht zu prüfen. Ferner finden sich in den Leitlinien Ausführungen zur fristgerechten Meldung an die Aufsichtsbehörde. Die DSGVO verlangt im Falle einer meldepflichtigen Verletzung (die Verletzung führt zu einem Risiko für die Rechte und Freiheiten natürlicher Personen), dass der Verantwortliche diese unverzüglich und möglichst binnen 72 Stunden, nachdem ihm *die Verletzung bekannt wurde*, der zuständigen Aufsichtsbehörde meldet. Die Artikel-29-Datenschutzgruppe ist hier der Auffassung, dass eine Verletzung einem Verantwortlichen als bekannt angesehen werden kann, wenn dieser eine angemessene Gewissheit darüber hat, dass ein Sicherheitsvorfall eingetreten ist, und dieser dazu geführt hat, dass personenbezogene Daten kompromittiert wurden. In den Leitlinien finden sich zahlreiche erläuternde Beispiele.

Die Artikel-29-Datenschutzgruppe veröffentlichte ferner Leitlinien betreffend **Automatisierte Entscheidungen im Einzelfall einschliesslich Profiling.**[72] Das *Profiling* ist in der DSGVO legal definiert.[73] Die DSGVO bestimmt, dass eine betroffene Person nur unter ganz bestimmten Einschränkungen einer ausschliesslich auf einer automatisierten Verarbeitung – einschliesslich Profiling – beruhenden Entscheidung, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, unterworfen werden darf.[74] Die Leitlinien der Artikel-29-Datenschutzgruppe umfassen Definitionen zur Profilerstellung und der automatisierten Entscheidungsfindung sowie allgemeine und spezifische Ausführungen zu Bestimmungen über die Profilerstellung und automatisierte Entscheidungsfindung. In den Anhängen finden sich abschliessend Best-Practice-Empfehlungen, die auf den Erfahrungen der EU-Mitgliedstaaten aufbauen.

Mit dem Ziel, dass nationale Aufsichtsbehörden Verstösse gegen Bestimmungen der DSGVO homogen ahnden und um ihnen Sicherheit bei der Ausübung ihrer durch die DSGVO übertragenen Aufgabe der **Sanktionierung von Datenschutzverstössen** zu geben, hat die Artikel-29-Datenschutzgruppe entsprechende Leitlinien erlassen.[75] Die zu verhängenden Massnahmen bzw. Geldbussen sind gemäss DSGVO abhängig von der Art, Schwere und Dauer des Verstosses unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung, der Anzahl betroffener Personen, dem Grad des Verschuldens, Vorliegen früherer Verstösse und einer Reihe weiterer zu berücksichtigender Faktoren. Die gegenständlichen Leitlinien gehen in differenzierender Form auf die einzelnen Faktoren ein und sollen die Aufsichtsbehörden bei ihrer Aufgabe der Sanktionierung von Verstössen massgeblich unterstützen.

69 Erwägungsgrund 42 DSGVO.
70 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47741.
71 Art. 33 und 34 DSGVO.
72 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963.
73 *«Profiling» bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;* (Art. 4 Ziff. 4 DSGVO).
74 Art. 22 DSGVO.
75 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889.

Seit dem 1. August 2016 können sich Unternehmen bei Übermittlung von Daten in die USA auf den **EU-US Privacy Shield** als eine der möglichen Rechtsgrundlagen für Datentransfers in die USA stützen. Wichtiger Teil des Privacy Shields ist aber auch die Übereinkunft zwischen den Vertragsparteien, dass nach Ablauf eines Jahres nach dessen Implementierung, die Angemessenheit der Datenschutzprinzipien durch die europäische Seite erneut geprüft wird. Diese erste Prüfung hat im Berichtsjahr stattgefunden. Dabei nahmen neben Repräsentanten der Kommission acht Repräsentanten der Artikel-29-Datenschutzgruppe teil. Das Ergebnis der Überprüfung aus Sicht der Datenschutzgruppe wurde in einem Bericht zusammengefasst und zwischenzeitlich in einer Pressemitteilung auf der Internetseite der Artikel-29-Datenschutzgruppe veröffentlicht.[76] Bei dieser ersten Prüfung wurden verschiedene signifikante Schwachstellen identifiziert, die ein angemessenes Datenschutzniveau aus Sicht der Artikel-29-Datenschutzgruppe in Frage stellen. Handlungsbedarf wird insbesondere dahingehend geäussert, dass prioritär eine unabhängige Ombudsperson (Ombudsmechanismus) ernannt sowie die Geschäftsordnung weiter erläutert werden müssen. Die zentralen Kritikpunkte sind laut Artikel-29-Datenschutzgruppe bis 25. Mai 2018 zu beseitigen, weniger kritische bis zur nächsten jährlichen Überprüfung. Wir verfolgen hier die Entwicklungen weiter.

## 6.2 Europarat

Der Konventionsausschuss beschäftigte sich neben unterschiedlichen Themen wie dem Schutz von Gesundheitsdaten oder dem Schutz personenbezogener Daten im Polizeibereich vor allem mit der Revision der Datenschutzkonvention 108. Das letzte Treffen des Konsultativkomitees zur Konvention 108 fand im September 2017 statt. Sobald das Ministerkomitee des Europarates die revidierte Konvention angenommen hat, haben die Vertragsparteien zwei Jahre Zeit für die Ratifizierung der modernisierten Konvention. Wir nahmen im Berichtsjahr aus Ressourcengründen an keiner Sitzung teil.

## 6.3 Weitere internationale Zusammenarbeit

Seit Dezember 2011 ist Liechtenstein Mitglied des Schengen-Raums. Im Kern des Abkommens von **Schengen** steht das Schengener Informationssystem der zweiten Generation (SIS II). Im Zusammenhang mit der Schengen-Mitgliedschaft finden seither regelmässig Evaluationen im Bereich Datenschutz statt. Nach 2011 wurden wir zuletzt 2015 evaluiert. Der **Evaluationsbericht** wurde uns im Berichtsjahr, also etwa zwei Jahre nach der Evaluation, **zugestellt.** Darin wurde festgehalten, dass wir in der Datenschutzstelle zusätzliche Ressourcen benötigen würden, um den vielzähligen Aufgaben, wie insbesondere den regelmässigen Kontrollen des Schengener Informationssystems (SIS) und des Visa Informationssystems (VIS), nachkommen zu können. Unsere personellen Ressourcen sind jedoch seit dem Schengen-Beitritt 2011 unverändert geblieben. *Aufgrund notwendiger Verlagerungen unserer bestehenden Ressourcen auf für Liechtenstein zentrale Themen, wie beispielsweise den Finanz- und Gesundheitsbereich sowie die DSGVO, nahmen wir auch im aktuellen Berichtsjahr an keinen Schengen-Sitzungen teil.*

76 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48781.

# 7. IN EIGENER SACHE

Die Datenschutzverordnung (DSV) wurde 2014 um eine **Gebührenpflicht** für Gutachten auf Stellungnahmen erweitert.[77] Doch der *Datenschutz darf nicht zu einem Luxusgut werden.* Dieser Meinung war auch ein Landtagsabgeordneter bei der Diskussion unseres Tätigkeitsberichts 2016. Wir haben immer darauf hingewiesen, dass sich eine Gebührenpflicht als kontraproduktiv erweisen könnte.[78] Unser Ziel war und ist es, Hürden abzubauen und diejenigen zu unterstützen, die den Schutz der Privatsphäre ernst nehmen. Deshalb *sprechen wir uns für eine Abschaffung der Gebührenpflicht aus.* Diese findet seine Grundlage zwar in der DSV, jedoch nicht im Gesetz. Aufgrund der fehlenden Deckung im DSG haben wir uns entschlossen, die Verhängung von Gebühren vorerst auszusetzen und die daraus resultierenden Auswirkungen auf die Anfragen zu evaluieren.

Im Rahmen der Vernehmlassung zur Änderung des DSG hatten wir vorgeschlagen, die **Bewilligungspflicht für Anlagen zur Videoüberwachung** im öffentlichen Raum abzuschaffen.[79] Die Praxis zeigt, dass dem kaum nachgekommen wird. Dies liegt nicht zuletzt daran, dass es an entsprechenden Sanktionsmöglichkeiten fehlt. In Einzelfällen erhalten wir Anträge von pflichtbewussten Unternehmen und Privatpersonen, was jedoch unsere knappen Ressourcen zusätzlich bindet.

Die **Vorratsdatenspeicherung** ist seit langem ein Thema. Nach zwei Urteilen des EuGH entfiel bekanntermassen die europarechtliche Grundlage für die Speicherung von Kommunikationsdaten auf Vorrat.[80] Das Ergebnis einer von der Regierung im Jahr 2015 einberufenen Arbeitsgruppe zur Analyse der möglichen Folgen für die Gesetzeslage in Liechtenstein, in welcher wir einen aktiven Beitrag leisteten,[81] floss nun direkt in die Revision des Kommunikationsgesetzes (KomG) sowie weiterer die Vorratsdatenspeicherung betreffender Rechtsnormen ein. Die Bestimmungen über den Datenschutz finden sowohl Anwendung auf die Überwachung als auch die Speicherung von Daten auf Vorrat. Bereits in der Vergangenheit hat sich bei den diesbezüglichen Kontrollen gezeigt, dass diese sehr zeit- und ressourcenintensiv sind.[82] Aufgrund der Erweiterung der datenschutzrechtlichen und insbesondere datensicherheitsrelevanten Bestimmungen wird sich der Prüfungsumfang bei Kontrollen vergrössern. Künftig wird es speziell zu berücksichtigende Aspekte geben: getrennte Speicherung bzw. logische Unterscheidung zwischen Betriebsdaten und Vorratsdaten; Verschlüsselung; Zugriff auf Vorratsdaten nur durch besonders ermächtigte Mitarbeiter unter Nutzung eines Vier-Augen-Prinzips; Verwendung eines einheitlichen Formblatts für die Übermittlung der Daten; revisionssichere Protokollierung und die Pflicht zur Erstellung interner Richtlinien sowie die unwiederbringliche Löschung der Vorratsdaten. Zudem sind Nachkontrollen durchzuführen, um feststellen zu können, ob unsere Empfehlungen umgesetzt wurden oder nicht. Die Regierung hat den Mehraufwand, der mit der Revision des KomG verbunden ist, im Bericht und Antrag an den Landtag entsprechend ausgeführt.[83] Das heute bestehende Datenschutzniveau muss aus Sicht der Regierung unbedingt aufrechterhalten bleiben.[84] *Mit anderen Worten macht eine gesetzliche Pflicht zur Datenschutzkontrolle, wie vom EuGH gefordert, nur Sinn, wenn bei uns die dafür notwendigen Ressourcen vorhanden sind.*

Die Erwartungshaltung und Wichtigkeit des Themas DSGVO für die heimische Wirtschaft wurde mehrfach in den regionalen Medien thematisiert. Im Mai-Landtag wurden zwei und im Oktober-Landtag eine kleine Anfrage zur **DSGVO** gestellt.[85] In der Beantwortung dieser Anfragen hat die Regierung die **Wichtigkeit des Themas für Liechtenstein** bestätigt. Es war sogar von einer Vorabumsetzung der DSGVO in Liechtenstein die Rede. Entsprechend dieser Bedeutung setzten wir unsere Anstrengungen fort, uns als Organisation mit den bestehenden personellen Ressourcen auf die kommenden Anforderungen vorzubereiten. Gleichzeitig nahmen wir im Zusammenhang mit dem Budgetprozess einen ersten Anlauf zur Aufstockung unseres Personals. Dabei sind wird jedoch gescheitert. Dies liegt wohl letztlich am Verfahren, welchem wir hierbei unterliegen. So sieht die aktuelle Gesetzeslage vor, dass wir unseren Budgetantrag bei zwei verschiedenen Stellen einreichen müssen: Während die Geschäftsprüfungskommission (GPK) nach Art. 28c DSG für den Voranschlag zuständig ist, liegt die Zuständigkeit für die personellen Ressourcen beim Landtagsprä-

77 Art. 33 Abs. 1 DSV.
78 Tätigkeitsbericht 2016, 7.
79 Tätigkeitsbericht 2015, 7.
80 Tätigkeitsbericht 2014, 4.3, und Tätigkeitsbericht 2016, 4.3.
81 Tätigkeitsbericht 2015, 2.5.
82 Tätigkeitsbericht 2013, 4.

83 BuA 88/2017, S. 14f.
84 BuA 88/2017, S. 15.
85 http://www.landtag.li/kleineanfragenprint.aspx?id=150532 und http://www.landtag.li/kleineanfragenprint.aspx?id=150559.

sidium. Dieses Verfahren ist unserer Ansicht nach sehr problematisch. Es gibt keine andere Behörde in Liechtenstein, die einem solch umständlichen Verfahren unterliegt. Wir hatten dies in der Vergangenheit bemängelt und obwohl eine diesbezügliche Vernehmlassung bereits im Sommer 2015 ablief, wurde das DSG noch immer nicht angepasst.

## 7.1 Datenschutz-Grundverordnung

Die DSGVO war im abgelaufenen Jahr einer unserer Schwerpunkte. Als kleine Amtsstelle sind wir gehalten, früh auf wichtige Entwicklungen zu reagieren. Die DSGVO ist nicht nur EU-, sondern auch EWR-relevant und wird bedeutende Änderungen – auch für uns als Aufsichtsbehörde – mit sich bringen. Die DSGVO hat uns daher in verschiedenen Belangen beschäftigt.

Es ist aus unserer Sicht und insbesondere für Liechtensteinische Unternehmen besonders wichtig, darauf zu achten, dass die DSGVO möglichst zeitnah in den EWR übernommen wird. Denn erst nach der Übernahme der DSGVO in das EWR-Abkommen können wir als Aufsichtsbehörde für **Unternehmen mit Hauptsitz in Liechtenstein** als **federführende Behörde** tätig werden. Die diesbezüglich notwendigen Vorbereitungen laufen. Wir haben hier bei den zuständigen Stellen unsere Unterstützung und Mitarbeit angeboten und werden dies auch weiterhin tun. Eine unserer gesetzlichen Aufgaben war und ist die Aufsicht über Unternehmen, auch in grenzüberschreitenden Fällen. Gerade dabei ist es von Bedeutung, dass wir als nationale Datenschutzbehörde federführende Behörde für Unternehmen mit Hauptsitz in Liechtenstein sein können.

Die DSGVO sieht die **Datenschutzbehörden als Aufsichtsbehörden,** deren zentrale Aufgabe eben *die Aufsicht* ist. In grenzüberschreitenden Fällen sieht der sogenannte One-Stop-Shop[86] eine obligatorische Zusammenarbeit der betroffenen Aufsichtsbehörden vor.[87] Somit wird die alleinige Entscheidungsbefugnis der nationalen Datenschutzbehörden – und somit auch unsere – auf jene Fälle reduziert, die einen reinen Inlandbezug aufweisen. Für Unternehmen in Liechtenstein bedeutet dies in der Praxis, dass vor allem jene, die Waren oder Dienstleistungen in der EU anbieten und/oder wenn Betroffene (z. B. Kunden) ihre Rechte diesen gegenüber wahrnehmen wollen, mit Aufsichtsverfahren aus Mitgliedsländern der EU konfrontiert sein können. Wie unsere konkrete Rolle aussehen wird, ist noch offen, da die EWR-Übernahme noch nicht abgeschlossen ist.

Um einen Eindruck darüber zu vermitteln, wie ein **Aufsichtsverfahren ab dem 25. Mai 2018** aussehen könnte, haben wir an **zufällig ausgewählte Unternehmen einen fiktiven Prüffragebogen**[88] versandt. Dieser Fragebogen diente den Unternehmen als Selbstkontrolle, wie weit sie auf dem Weg die Anforderungen der DSGVO erfüllen zu können, schon gediehen sind. Eine Beantwortung und Rücksendung des Fragebogens war nicht zwingend erforderlich, lediglich gewünscht.

Für eine Standortbestimmung in der heimischen Wirtschaft haben wir zu Beginn des Berichtsjahres eine **anonyme Umfrage an 103 Unternehmen** versendet, die uns gegenüber einen Datenschutzverantwortlichen bezeichnet haben. Wir fragten, inwieweit sich die Unternehmen von der DSGVO betroffen sehen und ob bzw. wie sie sich auf die DSGVO vorbereiten würden. Letztlich interessierte uns auch, wie sich die betroffenen Unternehmen die Unterstützung durch staatliche Stellen und/oder die Verbände vorstellen. Insgesamt gingen 50 Rückmeldungen bei uns ein. *Interessant für uns waren vor allem die Antworten auf die Frage, wie der Staat die Unternehmen unterstützen sollte, damit wir unsere begrenzten Ressourcen so effizient wie möglich – und vor allem auch mit dem grössten Mehrwert für die Unternehmen – einsetzen können.* So gaben 94 Prozent der teilnehmenden Unternehmen an, dass eine staatliche Unterstützung durch amtliche Informationen, wie z. B. auf unserer Internetseite, wünschenswert sei.[89] Ferner gaben 86 Prozent an, dass der Staat eine Arbeitsgruppe zur Analyse von Praxisfragen der DSGVO einsetzen sollte. Häufig genannt wurde auch, dass von staatlicher Seite aktiv durch Schulungen, Workshops oder Veranstaltungen die Bestimmungen der DSGVO erläutern und über deren Anwendung in der Praxis informiert werden sollte. Unterstützung auch in Form von Mustervorlagen, Handbüchern oder Handlungsempfehlungen würde man begrüssen.[90] Wir haben *all diese Anregungen aufgenommen und wo möglich entsprechend berücksichtigt.*

86 Bei grenzüberschreitenden Verarbeitungen ist die sogenannte federführende Aufsichtsbehörde alleiniger Ansprechpartner des Verantwortlichen bzw. des Auftragsverarbeiters; Art. 56 Abs. 6 DSGVO.

87 Art. 60 DSGVO.

88 Verwendung des Fragebogens in Absprache mit dem Bayrischen Landesamt für Datenschutz, https://www.lda.bayern.de/.

89 http://www.llv.li/#/117565/datenschutz-grundverordnung-dsgvo-.

90 Analyse und Auswertung der Umfrage unter http://www.llv.li/#/117872/umfrageauswertung.

# 8. AUSBLICK

Kurz vor Jahresende wurde das Vernehmlassungsverfahren der Regierung betreffend die **Totalrevision des Datenschutzgesetzes** sowie die Abänderung weiterer Gesetze eröffnet. Mit der Totalrevision des DSG werden die in der DSGVO enthaltenen Öffnungsklauseln konkretisiert, welche es dem nationalen Gesetzgeber ermöglichen, nationale Datenschutzbestimmungen beizubehalten oder zu erlassen. Die Öffnungsklauseln betreffen Bereiche ausserhalb des Kerns des gemeinsamen (digitalen) Binnenmarkts, sodass es vertretbar erscheint, dass hier in Europa national unterschiedliche Datenschutzbestimmungen gelten. Wir werden eine Stellungnahme zur Vernehmlassung abgeben sowie die weiteren Entwicklungen hinsichtlich der Anpassung der Datenschutzbestimmungen in den Spezialgesetzen beobachten und bei Fragen zur Verfügung stehen.

Wie sich im Berichtsjahr bereits klar abgezeichnet hat, wird die DSGVO auch im Jahr 2018 unsere Tätigkeiten massgeblich bestimmen, denn die neue Gesetzgebung weist den Datenschutzbehörden eine **zentrale Rolle für die einheitliche Durchsetzung des neuen Datenschutzrechts** in der Europäischen Union und im Europäischen Wirtschaftsraum zu. Ihnen obliegt es, dafür Sorge zu tragen, dass das Ziel eines wirksamen gelebten Datenschutzrechts erreicht werden kann.

Ein erster zentraler Bestandteil der Aufgabenerfüllung muss es daher sein, alle Kanäle der **Informationsvermittlung** zu nützen, um datenverarbeitende Stellen wie auch Bürger auf die Risiken und Schutzmassnahmen, Vorschriften, Garantien, Rechte und Verpflichtungen im Zusammenhang mit der Verarbeitung personenbezogener Daten hinzuweisen und sie in Bezug auf ihre spezifischen Fragen zu beraten. Ein besonderes Augenmerk wird dabei der Webseite gelten, deren Vollständigkeit und Aktualität sowie einfache und übersichtliche Navigation oberste Priorität haben.

In Bezug auf die Adressaten der Kommunikation haben wir uns im Berichtsjahr vermehrt auf Unternehmen und den Privatbereich fokussiert. Doch wollen wir die Behörden und im Speziellen die Landesverwaltung nicht völlig ausser Acht lassen. Denn die Verpflichtungen der DSGVO gelten ebenso für Behörden. Ungeachtet möglicher Geldbussen bei Verstössen haben gerade Behörden eine besondere Pflicht, die Privatsphäre der Betroffenen zu schützen. Hier wird ein Fokus auf der Weiterentwicklung der **Schutzbedarfsanalysen**[91] und der **Rechtsgrundlagenanalysen beim Projektmanagement der Landesverwaltung** liegen.

Die neue erweiterte Rolle bedingt auch **interne Änderungen und Anpassungen.** Die Ausrichtung der **Strategie und der internen Prozesse** auf die DSGVO wird eine weitere Priorität im Jahr 2018 sein. Eine Anpassung verlangen sowohl die Verfahren und Prozesse betreffend die Aufsicht und Kontrolle im eigenen Land als auch die Zusammenarbeit auf europäischer Ebene. Art. 57 Abs. 1 DSGVO überträgt den Aufsichtsbehörden eine Vielzahl an Aufgaben, die sich dadurch auszeichnen, dass sie ein Ziel definieren, das die Aufsichtsbehörde erreichen muss, oder einen Problembereich benennen, für den sie eine Lösung finden sollen. Dabei obliegt der Behörde die Entscheidung, ob sie im konkreten Fall tätig werden soll, und welche der in Art. 58 DSGVO genannten Befugnisse sie zur Erfüllung der Aufgabe nutzen will. Diese Konkretisierung werden wir mittels einer internen Strategie vornehmen.

Mit der Übernahme der Aufgaben der Zusammenarbeit in der Union gemäss Art. 60 ff. DSGVO betreten wir vollkommenes Neuland und müssen diese organisatorisch und personell aufbauen. Wir können im Rahmen einer grenzüberschreitenden Datenverarbeitung zur federführenden oder betroffenen Aufsichtsbehörde werden und dabei in ein Verfahren der Zusammenarbeit nach Art. 60 DSGVO involviert werden. Diese Verfahren sind komplex, mit knappen Fristen verbunden und können bei Uneinigkeit zwischen den beteiligten Aufsichtsbehörden zu schwierigen und langwierigen Kontroversen führen. In welchem Umfang wir damit tatsächlich befasst sein werden, bleibt abzuwarten. Eine gewisse Vorbereitung und Ausarbeitung eines Konzeptes sind aber nichtdestotrotz unumgänglich.

Wir werden des Weiteren die Entwicklungen innerhalb der Artikel-29-Datenschutzgruppe bzw. des künftigen Europäischen Datenschutzausschusses genau beobachten, die Interessen Liechtensteins in diesen Gremien einbringen und die ausgearbeiteten Leitlinien und Empfehlungen auf der Internetseite zugänglich machen.

91 Tätigkeitsbericht 2016, 3.

Mit der europäischen Neuregulierung des Datenschutzes soll das informationelle Selbstbestimmungsrecht der Bürger gestärkt werden und Europa die Chance bekommen, seine digitale Souveränität wieder herzustellen. In diesem neuen Gefüge möchten wir, die Datenschutzstelle, auch 2018 als kompetenter und zuverlässiger Ansprechpartner den Bürgern, Unternehmen und Institutionen in Liechtenstein zur Verfügung stehen und mittels Beratung, Kontrolle und Aufsicht einen Beitrag zu einem wirksamen gelebten Datenschutzrecht leisten.

# 9. ANHANG

## 9.1 Anfragestatistik

Die Beratung privater Personen und Behörden ist eine unserer Kernaufgaben. Im Berichtsjahr erhielten wir insgesamt 542 Anfragen. Gegenüber den Vorjahren bedeutet dies quantitativ einen leichten Rückgang. Dem gegenüber hat sich allerdings der qualitative Umfang der Anfragen merklich erhöht. Den erwähnten Rückgang erklären wir uns wie folgt: **Das Thema DSGVO ist bei den Unternehmen angekommen** und andere Datenschutzfragen werden von den Datenbearbeitern zurückgestellt. Diese These wird durch mehrere Feststellungen gestützt.

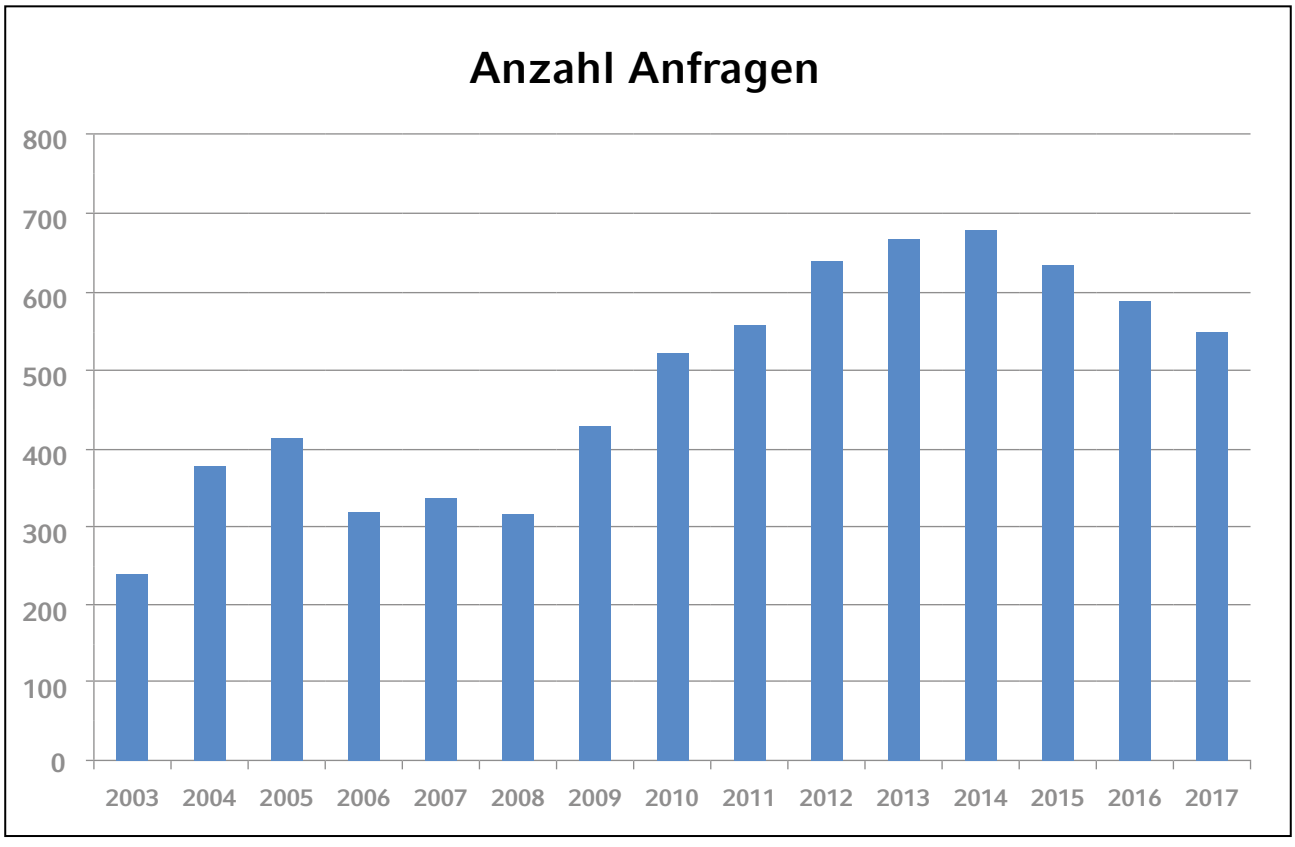
So hatten vor allem in der zweiten Jahreshälfte **über ein Drittel der Anfragen einen direkten oder indirekten Bezug zur DSGVO.**

Seit dem Beginn der Aufzeichnungen stammen die meisten Anfragen von der Landesverwaltung oder anderen Behörden. Doch 2017 war dies anders. Erstmalig erhielten wir beinahe **30 Prozent mehr Anfragen von Unternehmen (Industrie, Gewerbe und Dienstleistungsbereich) als von der Landesverwaltung oder anderen Behörden.**

Die meisten Anfragen sind nach wie vor genereller Natur, wo sich die Anzahl mehr als verdoppelte. Insgesamt verzeichneten wir in sämtlichen – mit Ausnahme von vier Sachgebieten – einen quantitativen Rückgang der Anfragen. **Drei der vier Sachgebiete, in denen die Anzahl der Anfragen zunahmen,** haben entweder einen **direkten oder indirekten Bezug zur DSGVO:** Erstens «Allgemeine Anfragen», welche speziell jene betreffend die DSGVO mit umfassen; zweitens «Umsetzung/Anwendung europäischen Rechts»; und drittens «Anfragen und Stellungnahmen zu Gesetzesvorhaben». Ebenfalls nahm die Zahl der Anfragen zum technologischen Datenschutz leicht zu.

**Anzahl Anfragen im Vergleich zu den Vorjahren**

Die nachfolgende Abbildung zeigt die Entwicklung der Anzahl der Anfragen über die vergangenen 15 Jahre:



## Anzahl Anfragen pro Personengruppe und Sachgebiet

Die folgende Tabelle gibt detailliert Auskunft über die Anzahl an Anfragen pro Personengruppe und Sachgebiet:

| | Anwaltsbüros | Gemeinden | Industrie, Gewerbe, Dienstleistung | Internationales | Landesverwaltung, Behörden | Medien | Privatpersonen | Vereine, Verbände |
|---|---|---|---|---|---|---|---|---|
| Datenschutz allgemein | 44 | 9 | 44 | 5 | 31 | 58 | 30 | 3 |
| Arbeitsbereich | 1 | | 1 | | 2 | | 4 | 1 |
| Datenbekanntgabe Inland | 1 | 3 | 2 | | 3 | | 4 | |
| Datenbekanntgabe Auslandsbezug | 9 | | 16 | 14 | 3 | | | 9 |
| Geltendmachung gesetzlicher Rechte | 1 | 1 | 17 | 1 | 4 | 2 | 9 | 1 |
| Gesetzesvorhaben | | | | | 18 | | | |
| Gesundheit/Soziales | 2 | | 2 | | 3 | | | |
| Keine Zuständigkeit DSS | | | 5 | | 2 | | 2 | |
| Polizei/Sicherheit | | | | 14 | | | | |
| Register der Datensammlungen | 1 | | 15 | | 1 | | | |
| Schengen/Dublin | | | | 3 | | | | |
| Technologischer Datenschutz | | | 12 | | 11 | 16 | 11 | 3 |
| Umsetzung/Anwendung europäischen Rechts | 4 | | 22 | 1 | 4 | 1 | | |
| Vernehmlassungen ohne Stellungnahme | | | | | 17 | | | |
| Videoüberwachung | | 1 | 9 | | 4 | 3 | 10 | 2 |
| **Gesamtergebnis** | **65** | **14** | **148** | **38** | **108** | **80** | **70** | **19** |

## 9.2 Newsletter

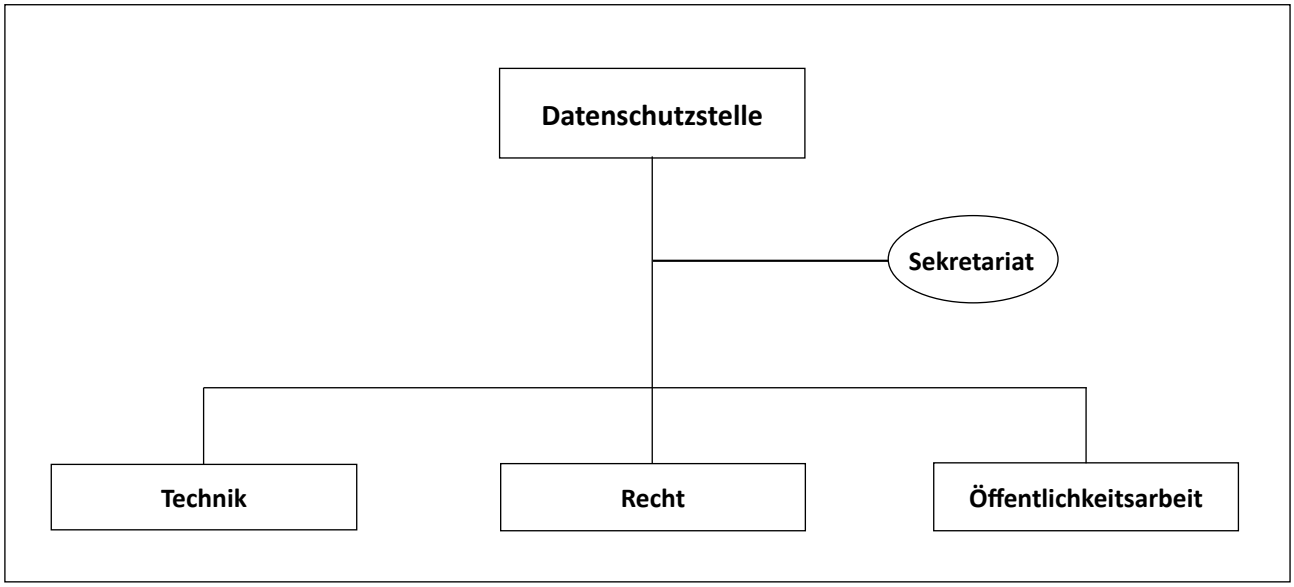
In unserem E-Mail-Newsletter informieren wir laufend über aktuelle Entwicklungen zum Datenschutz.[92] Im Jahr 2017 haben wir 14 Newsletter versendet, in erster Linie zum Thema DSGVO. Wir erreichten damit im Januar 568 Abonnenten und konnten die Anzahl bis Dezember auf 612 Abonnenten steigern.

## 9.3 Veröffentlichte Publikationen

Folgende Publikationen wurden erstellt oder überarbeitet:

- Empfehlung zur Vernichtung von Personendaten, September 2017.[93]

## 9.4 Organigramm




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

93 Empfehlung zur Vernichtung von Personendaten, https://www.llv.li/files/dss/pdf-llv-dss-empfehlung-vernichtung-von-daten.pdf.

DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Postfach 684
FL-9490 Vaduz

Telefon +423 236 60 90

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