DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Tätigkeitsbericht 2012

Datenschutzstelle des Fürstentums Liechtenstein

INHALTSVERZEICHNIS

VORWORT

Auch im vergangenen Jahr bestätigte sich der Trend der zunehmenden Anfragen. Mit 640 **Anfragen** konnte wiederum ein neuer Höchststand verzeichnet werden. Einige davon werden im Bericht ausführlich dargestellt, da sie aus unserer Sicht für die breite Öffentlichkeit von Interesse sind.

Darunter gab es auch einige **Beschwerden** von Privatpersonen. Diese betrafen verschiedene Bereiche. Zwei Beschwerden in Bezug auf den Arbeitsplatz führten nicht zum gewünschten Erfolg. Dabei spielte die schwächere Stellung im Arbeitsverhältnis wohl eine entscheidende Rolle (siehe 1.1.).

Ausser den Anfragen war unsere Arbeit von folgenden Schwerpunkten gekennzeichnet:

Aus Anlass des zehnjährigen Bestehens des Datenschutzgesetzes gaben wir eine **repräsentative Umfrage** in Auftrag. Dabei wurden 500 Personen im Land zu verschiedenen Themen befragt. Die Ergebnisse zeigen, dass die *Behörden des Landes* grundsätzlich ein *grosses Vertrauen* der Bevölkerung geniessen. Andererseits waren aber 70 % der Befragten der Meinung, nur wenig über den Datenschutz zu wissen. Dies bedeutet aus unserer Sicht, dass die *Bevölkerung besser sensibilisiert* werden sollte. Das ist jedoch nicht nur unsere Aufgabe, sondern eine, bei der *Synergien* geschaffen werden sollten. Synergien sind in einem kleinen Land wie Liechtenstein sehr wichtig (siehe 2.1.).

Im Sinne der Sensibilisierung organisierten wir wiederum eine öffentliche Veranstaltung aus Anlass des **Europäischen Datenschutztages** in Zusammenarbeit mit dem Institut für Wirtschaftsinformatik der Universität Liechtenstein. Das Thema lautete *„Was weiss das Internet über mich?" – Meine Daten als Handelsware!* Ausserdem luden wir zur Schaffung der erwähnten Synergien wiederum die **Datenschutzverantwortlichen** zu einem Gedankenaustausch ein. Dabei fanden zwei Veranstaltungen statt: eine für die Verantwortlichen des öffentlichen und eine für diejenigen des privaten Bereichs (siehe 2.1.).

Man hört immer wieder, dass Daten anonymisiert oder pseudonymisiert werden. Da diese Begriffe aber nicht immer verstanden oder gar verwechselt werden, entschieden wir, eine **„Richtlinie über die Anwendung der Anonymisierung/Pseudonymisierung"** zu erstellen (siehe 2.2.).

Wir konnten erste Kontrollen abschliessen (siehe 4.).

Im Rahmen unserer **internationalen Zusammenarbeit** wurden verschiedene wichtige Dokumente geschaffen: Unter anderem je ein Arbeitspapier zu *Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes, zur Gesichtserkennung bei Online- und Mobilfunkdiensten*, zu Entwicklungen im Bereich *biometrischer Technologien* oder die von der irischen Datenschutzbehörde durchgeführte Kontrolle von *Facebook* (siehe 5.).

Im Januar 2012 stellte die Europäische Kommission die **Revision des Datenschutzes in Europa** vor. Dabei ist vorgesehen, die Rechte der Bürger und die Befugnisse der Datenschutzbehörden zu stärken und die Dateninhaber mehr in die Pflicht zu nehmen. Das Ganze soll in einer Verordnung geregelt werden. Für uns bedeutet dies zwar eine erhebliche Zunahme der Aufgaben. Andererseits werden wir uns aber verstärkt auf Rechtsansichten insbesondere aus Deutschland oder Österreich stützen können, da dort keine rechtlichen Unterschiede mehr bestehen werden. Insgesamt kann von einem Quantensprung beim Schutz der Privatsphäre in Europa gesprochen werden, da z.B. bei Datenschutzverstössen Bussen bis zur Höhe von 2 % des Jahresumsatzes vorgesehen sind. Noch ist die Revision nicht abgeschlossen, eine Verabschiedung der Verordnung ist aber für Ende 2013 geplant (siehe 3. und 5.1. und 5.5.).

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

Vaduz, im April 2013

Dr. Philipp Mittelberger
Datenschutzbeauftragter

BERICHTERSTATTUNG 2012

Die Zahl der Anfragen, die an uns gerichtet werden, nimmt weiterhin zu. Im vergangenen Jahr wurden *so viele Anfragen wie noch nie* an uns gestellt,[1] insgesamt 640 Anfragen. Dies bedeutet gegenüber dem Vorjahr eine Zunahme um 81 Anfragen. Die Anzahl der Zugriffe auf unsere Internetseite betrug im Berichtsjahr 60'729.

Es würde den Rahmen dieses Berichts sprengen, alle Anfragen darzustellen. Immerhin sollen aber einige Fragen und deren Beantwortung dargestellt werden, die für die Öffentlichkeit interessant sein dürften.

1. Fälle aus unserer Beratungspraxis

1.1. Wahrnehmung gesetzlicher Rechte/Beschwerden

Das Auskunftsrecht ist das zentrale Recht. Denn nur wer weiss, wer wann und wie Daten über ihn bearbeitet, kann seine Rechte auf Berichtigung, Sperrung oder Löschung geltend machen.[2] Um die Geltendmachung der erwähnten Rechte ging es in folgenden Fällen:

Eine Person wandte sich an uns, da sie den Verdacht hatte, dass die Einhaltung ihrer Arbeitszeit durch den *Arbeitgeber per Video heimlich überwacht* wird. Eine Videoüberwachung am Arbeitsplatz kann unter gewissen Umständen erlaubt sein. Der Arbeitgeber muss gewisse Kontrollmöglichkeiten haben, um sicher zu sein, dass der Arbeitnehmer seinen Pflichten am Arbeitsplatz nachkommt.[3] Solche Möglichkeiten müssen aber dem Arbeitnehmer im Voraus angekündigt werden und sich in einem gewissen Rahmen bewegen. Eine heimliche Überwachung ist nicht erlaubt. Dieser Fall zeigt, wie heikel Datenschutzprobleme am Arbeitsplatz sein können. Die betroffene Person mag zwar in Bezug auf diesen Fall im Recht sein. Sie fürchtete jedoch Repressionen nach der Lösung des Falles, da sie weiterhin demselben Arbeitgeber unterstellt ist. Deshalb bat sie uns, (vorerst) nichts zu unternehmen.

Ähnlich gelagert war folgender Fall: Die in Frage stehende Person wusste, dass strittige Informationen über sie beim Arbeitgeber vorhanden sind und wollte im Minimum einen Vermerk über die Bestreitung der Richtigkeit der Angaben bewirken.[4] Das Antwortschreiben des Arbeitgebers auf das Auskunftsbegehren war offenbar sehr allgemein gehalten (und somit nicht vollständig im Sinne des DSG). Zudem war in diesem Schreiben eine versteckte Drohung enthalten, die dieser Person ihre Abhängigkeit im Arbeitsverhältnis vor Augen führte. Aufgrund drohender Sanktionen bat sie uns ebenfalls, nicht zu intervenieren.

Eine andere Beschwerde betraf einen Fall einer *Lohnexekution*. Dabei sandte ein Rechtsanwalt einen Fax an ein Unternehmen und bat um Auskunft, ob ein Schuldner dort arbeitet. Der Fax wurde unangekündigt an die allgemeine Fax-Nummer geschickt und konnte somit dort von jedermann gelesen werden. Die betroffene Person machte geltend, dass der Fax von unbeteiligten Dritten im Unternehmen gelesen wurde. Wir forderten den Anwalt zur Stellungnahme auf. Dabei wurde geltend gemacht, dass es sich um eine „unbürokratische und kostengünstigere Variante" handle. Dem mag so sein. Doch ist das Senden eines unangekündigten Faxes an eine allgemeine Nummer in einem solchen Fall sicher nicht als verhältnismässig einzustufen. Der Anwalt sicherte uns zu, von dieser Praxis Abstand zu nehmen.

Die Dritte Geldwäscherei-Richtlinie regelt die Behandlung von *Politically Exposed Persons (PEPs)*.[5] Neben dem eigentlichen PEP sind auch dessen Ehepartner, Eltern und Kinder sowie deren Ehepartner als „Risikogruppe" einzustufen. Bestimmte Stellen, wie insbesondere Banken, Versicherungen und andere Finanzdienstleister, sind verpflichtet, spezifizierte Geschäfte oder „verdächtige Transaktionen" zu melden, die PEPs und ihre Familienmitglieder tätigen wollen. Es kann vorkommen, dass eine Bank beispielsweise die interne Weisung erstellt, dass PEPs kein Konto eröffnen dürfen. Einige Personen wandten sich an uns und machten darauf aufmerksam, dass sie in Liechtenstein zwar eine Funktion

1 2010 waren es 559; vgl. dazu Details im Anhang.
2 Vgl. Tätigkeitsbericht 2003, 3.1.2.; Tätigkeitsbericht 2007, 4.1., 6.; Tätigkeitsbericht 2009, 1.1.1., 1.5.; Tätigkeitsbericht 2010, 1.1.
3 Siehe unsere Richtlinie zum Datenschutz am Arbeitsplatz: http://www.llv.li/amtsstellen/llv-dss-richtlinien/llv-dss-ueberwachung-arbeitnehmer.htm.
4 Vgl. Art. 37 Abs. 2 und Art. 38 Abs. 3 Bst. b DSG.
5 Im Rahmen der Prüfung der Geldwäscherei war festgestellt worden, dass Potentaten illegal Gelder ins Ausland geschafft hatten. Dies galt es zu verhindern. Deshalb wurden in der Richtlinie Vorschriften zur Prüfung von Angaben über solche Personen eingeführt.

in einem öffentlichen Gremium innehatten; dies jedoch ehrenamtlich. Eine Qualifizierung als PEP sei absurd. Sie wollten von der PEP-Liste gestrichen werden, wussten jedoch nicht, wie sie das *Löschrecht* ausüben können. Wir konnten bei der Stabsstelle Financial Intelligence Unit (SFIU), die Zugriff auf die entsprechenden Datenbanken hat, feststellen, dass diese Personen in einer Datenbank erwähnt wurden.[6] Diese Datenbank wird in Grossbritannien geführt, weshalb wir an unsere britischen Kollegen gelangten, die uns die nötigen Kontaktangaben sendeten. Dies ermöglichte die Löschung der entsprechenden Daten. Bei der Vorführung der Datenbank durch die SFIU konnte festgestellt werden, dass in Liechtenstein gut 700 Personen und Firmen als PEPs verzeichnet sind.

Beim *Kauf einer Eintrittskarte am Schalter* für eine Veranstaltung wurden Käufer aufgefordert, ihre *Adresse bekanntzugeben*, dies offenbar ohne Begründung. Wir forderten das in Frage stehende Unternehmen zur Stellungnahme auf. Wir bekamen die Antwort, dies diene dem Schutz der Kunden, insbesondere bei Verlust der Eintrittskarte. Die Daten würden aber nach Durchführung der Veranstaltung gelöscht. Wir wiesen das Unternehmen darauf hin, dass die Angabe von nicht notwendigen Daten, wie einer Adresse beim Kauf an einem Schalter, nur mit der Einwilligung der betroffenen Person erfolgen kann. Um die Einwilligung zu bekommen, muss objektiv und umfassend vorinformiert werden.[7] Offenbar war überhaupt nicht informiert worden. Wir wiesen das Unternehmen auf die fehlenden Einwilligungen hin. Dementsprechend informierte es die Kunden nachträglich und bestätigte uns die Löschung von Adressen bei fehlender Einwilligung.

Zwei Internetnutzer hatten festgestellt, dass ihre Fotos mit Namen auf einer Internetseite auftauchten. Die Seite legt es ganz bewusst auf die *Blossstellung* der Betroffenen an. In einem Kontaktformular wird auf eine Bearbeitungsgebühr für die Beantwortung von Anfragen hingewiesen, welche mittels Kreditkarte bezahlt werden muss. Möchte man also nicht blossgestellt werden, sollte man dafür bezahlen und auch seine Kreditkartennummer angeben! Unsere Nachforschungen ergaben, dass die Seite international verflochten ist, so dass eine Durchsetzung des Löschrechts sehr schwierig, wenn nicht gar unmöglich ist. Deshalb sollte man besonders darauf achten, ob und welche Fotos im Internet veröffentlicht werden sollen. Das konkrete Beispiel zeigt, dass auch „normale" Fotos durch unseriöse Internetseitenbetreiber kopiert und für andere Zwecke missbraucht werden.[8] Es muss nicht immer um die vielzitierten peinlichen Fotos gehen, die vor allem auf Facebook veröffentlicht werden.

In einem weiteren Fall wurde geltend gemacht, dass eine Person eine Berufszulassung nicht erhalten hatte, da das entsprechende Amt falsche Informationen an den Prüfungsexperten gegeben hatte. Wir informierten dahingehend, dass diese falsche Information belegt sein müsse. Je nach dem kann daraus ein *Amtshaftungsfall* entstehen.

Wie schon vor zwei Jahren erhielten wir wieder eine Beschwerde in Bezug auf eine *Datenerhebung durch das Schulamt*.[9] Es ging im Wesentlichen darum, dass vor allem die Kinder des 3. und 5. Schuljahres Fragen wie „Wie viele Personen leben bei dir zu Hause?" oder „Wie viele Bücher gibt es bei dir zu Hause?" in der Schule beantworten mussten. Zwar waren die Eltern auf diesen Umstand in einem Rundschreiben hingewiesen worden. Sie hatten jedoch nicht die Möglichkeit, auf die Beantwortung der Fragen einen direkten Einfluss zu nehmen. Diese Fragen betreffen nicht nur die Kinder selbst, sondern eben das Umfeld daheim. Wir wiesen das Schulamt darauf hin, dass der minimale Aufwand des Verteilens und Einsammelns der Fragebogen in den Klassen kein Argument darstellt, das der Abwicklung zu Hause entgegensteht. Ein weiteres Problem bestand in einer teils missverständlichen Formulierung des Schreibens, was womöglich auch zu Widerstand führte. Wir waren dem Schulamt bei der Verfassung eines neuen Schreibens behilflich. Zudem wurde uns zugesagt, dass in Zukunft solche Fragen daheim, unter Einbezug der Eltern, beantwortet werden.

6 Dabei wird häufig auf die Anbieter von kommerziellen Datenbanken (z.B. World-Check, Factiva, World-Compliance) zurückgegriffen. Diese privaten Datenbanken führen globale Listen von Personen, die von der Definition von PEPs erfasst sein können. Bei jeder Person kann in der Datenbank nachvollzogen werden, warum sie eingetragen ist. Die Einträge stützen sich meist auf veröffentlichte Meldungen durch Behörden oder die Presse.

7 Vgl. Art. 5 DSG.

8 Zum Löschen von Internetinhalten vgl. Tätigkeitsbericht 2009, 1.1.2.

9 Tätigkeitsbericht 2010, 1.8.

Um die Einwilligung ging es auch in der folgenden Beschwerde: Im Rahmen der Kurse, die der Arbeitsmarktservice den Stellensuchenden anbietet, soll auch die *Darstellung des Lebenslaufes* optimiert werden. Hierzu werden die Lebensläufe aller Teilnehmer während des Kurses offengelegt und diskutiert. Dabei war im Vorfeld vereinbart worden, dass alles, was im Rahmen des Kurses bekannt und besprochen wird, absolut vertraulich zu behandeln und hierüber Stillschweigen zu wahren ist. In einem Fall war die betroffene Person nicht damit einverstanden. Somit stellte sich die Frage, ob es für die Offenlegung des Lebenslaufes eine (gesetzliche) Pflicht gibt oder ob eine Offenlegung nur nach entsprechender Einwilligungserklärung des betroffenen Kursteilnehmers zulässig ist. Wir kamen zum Schluss, dass es keine solche gesetzliche Pflicht gibt, wodurch eine Offenlegung des Lebenslaufes nur bei Vorliegen einer Einverständniserklärung der betroffenen Kursteilnehmer zulässig ist.[10] Verweigert ein Kursteilnehmer eine Offenlegung, ist dies zu respektieren.

1.2. Technologischer Datenschutz

Das Zustellgesetz sieht vor, dass Zustellungen an Personen unter bestimmten Voraussetzungen durch Veröffentlichung auf der Internetseite der Behörde vorgenommen werden können.[11] Diese Veröffentlichung ermöglicht eine Indexierung in (Personen-) Suchmaschinen. Dadurch können die Daten für unbestimmte Zeit im Internet aufgefunden werden. Somit ist eine Verletzung der Privatsphäre von betroffenen Personen möglich. Im Sinne der Verhältnismässigkeit sollten Gegenmassnahmen geprüft werden. Wir haben in diesem Zusammenhang verfügbare technische Mittel angeschaut, die den Webseitenbetreibern zur Verfügung stehen, um Suchmaschinen von der Indexierung ihrer Internetauftritte abzuhalten. Neben der klassischen *robots.txt*[12] scheinen *HTML-Meta-Tags*[13] eine gute Alternative darzustellen. Mit den Meta-Tags kann der Seitenbetreiber festlegen, dass auf seinen Internetseiten gespeicherte Personendaten nicht in den Index (und somit in die Suchtrefferlisten von Suchmaschinen) aufgenommen werden sollen.[14] Falls jedoch festgestellt wird, dass der Schutz der betroffenen Person höher wiegt als das Interesse der Behörde an der Zustellung eines Schriftstücks, sollte von der Veröffentlichung der Personendaten im Internet abgesehen werden; z.B. verzichtet das Ausländer- und Passamt im Zusammenhang mit Asylverfahren darauf.

Wir unterstützten wieder verschiedene Ämter bei der Erstellung von **Bearbeitungsreglementen**.[15] Verantwortlich für die Erstellung ist der Inhaber der jeweiligen Datensammlung. In der Praxis wird das Reglement häufig in jenen Organisationseinheiten erstellt und gepflegt, in denen die Personendaten konkret bearbeitet werden.[16] Die *„Empfehlung zur Datensicherheit sowie zu den technischen und organisatorischen Massnahmen des Datenschutzes"*[17] enthält eine Checkliste der notwendigen Inhalte sowie weitere Erläuterungen zum Thema.

Die AHV/IV/FAK-Anstalten (AHV) führen mit Revisoren bei den Gemeinden regelmässig **Prüfungen von Steuererklärungen** durch. Zur Optimierung der Abläufe ersuchte die AHV das Amt für Informatik (AI) um Bekanntgabe und Übermittlung einer Einwohnerliste, damit erforderliche Abklärungen unmittelbar vor Ort auf den Notebooks der Mitarbeiter der AHV durchgeführt werden können. Unsere Prüfung ergab, dass die bestehende Rechtsgrundlage für die Bearbeitung der angefragten Daten ausreicht, jedoch waren weitere Sicherheitsmassnahmen auf den Notebooks der Revisoren notwendig: Neben der Einrichtung einer entsprechenden *Festplattenverschlüsselung* auf sämtlichen verwendeten Notebooks waren für die Datenübermittlung der Einwohnerliste vom AI an die AHV weitere Massnahmen zur *Transportkontrolle*[18] zu berücksichtigen. Weiters wurde festgestellt, dass bis zu diesem Zeitpunkt kein *Nutzungsreglement* spezi-

10 Art. 23 Abs. 1 Bst. b DSG.
11 Art. 28 Abs. 1 ZustG.
12 http://www.robotstxt.org. In der auf dem Server des Seitenbetreibers gespeicherten robots.txt-Datei kann dieser Codezeilen einfügen, mithilfe derer die Suchmaschinen erkennen können, dass die entsprechenden Webseiten nicht indexiert werden sollen.
13 http://support.google.com/webmasters/bin/answer.py?hl=de&answer=93710.
14 Die grössten Internet-Suchmaschinen berücksichtigen Meta-Tags.
15 Art. 12 Abs. 2 Satz 1 DSV bzw. Art. 20 Abs. 2 Satz 1 DSV. Diese sind für bestimmte Datenbearbeitungen Pflicht. Ein Bearbeitungsreglement dokumentiert insbesondere die Datenbearbeitungs- und Kontrollverfahren.
16 Dies sind häufig die zuständige Informatikabteilung bzw. die dortigen Systemadministratoren der Datensammlungen, die bei der Erstellung und Pflege, insbesondere der technischen Inhalte, unterstützen.
17 http://www.llv.li/amtsstellen/llv-dss-richtlinien/llv-dss-empfehlung-tom.htm.
18 Art. 10 Abs. 1 Bst. c DSV. – Vgl. Abschnitt 2.4.3, S. 16, in Empfehlung zur Datensicherheit sowie zu den technischen und organisatorischen Massnahmen des Datenschutzes, http://www.llv.li/amtsstellen/llv-dss-richtlinien/llv-dss-empfehlung-tom.htm.

ell für den Umgang mit mobilen Datenträgern oder mobilen Arbeitsgeräten bei der AHV existierte. Die AHV wurde auf unsere Checkliste zur Prüfung von Nutzungsreglementen hingewiesen.[19]

1.3. Telekommunikation

Das Kommunikationsgesetz sieht vor, dass wir die Anwendung der Bestimmungen betreffend Datenschutz und Datensicherheit in Bezug auf Daten, die zum Zwecke der Mitwirkung bei einer Überwachung bearbeitet werden, zu kontrollieren haben.[20] Um die jährlich geforderte Statistik[21] erstellen zu können, müssen die Anbieter jede Anfrage und jede Mitwirkung bei einer Überwachung eines öffentlichen Kommunikationsnetzes dokumentieren. Die Protokolldaten sind uns auf Ersuchen zu übermitteln. Damit die Protokollierung und die grundsätzlichen Abläufe beim Datenaustausch im Sinne des Datenschutzes einheitlich erfolgen, erarbeiteten wir einen **„Datenschutzrechtlichen Leitfaden für den Austausch von Personendaten zwischen Telekommunikationsanbietern und Behörden anlässlich von Überwachungsmassnahmen der elektronischen Kommunikation gem. Art. 52ff. KomG"**. Dieser Leitfaden wurde der Landespolizei zugestellt.

Zudem trat eine Amtsstelle mit ihren Überlegungen an uns heran, die ein- und ausgehenden **Telefonate aufzuzeichnen und zu speichern**, was unseres Wissens nach ein Novum innerhalb der Landesverwaltung wäre.[22] Als Zweck dieser Aufzeichnung wurde die Verbesserung und Sicherung der Qualität sowie die Beweissicherung bei möglichen verbalen Angriffen und Attacken genannt. Eine ausdrückliche gesetzliche Grundlage für Telefonaufzeichnungen bei Behörden gibt es bislang nicht.[23] Gibt es keine hinreichende gesetzliche Grundlage, können Personendaten ausnahmsweise mit der Einwilligung der betroffenen Personen bearbeitet werden.

1.4. Gesundheit und Soziales

Wir wurden seitens des Amtes für Gesundheit im Rahmen einer Revision der Krankenversicherungsverordnung (KVV)[24] um Prüfung eines sogenannten **Vormerksystems** ersucht. Dabei handelt es sich um einen Vermerk über die Nichtbezahlung von Prämien sowie Kostenbeteiligungen auf der Krankenversicherungskarte. Kann die Kasse die ausstehenden Prämien oder Kostenbeteiligungen nicht einbringlich machen, hat sie die Möglichkeit, die Übernahme der Kosten für weitere Leistungen bis zur Bezahlung der Prämien aufzuschieben.[25] Wir haben das Amt für Gesundheit vor allem dahingehend beraten, in der KVV Informationspflichten der Kasse gegenüber den Versicherten aufzunehmen. Diese Informationen betreffen bei einer Eintragung in das Vormerksystem Art, Umfang, Zweck und Folgen dieser Eintragung sowie das dem Versicherten zustehenden Auskunftsrecht. Dies wurde so in den Gesetzesänderungsentwurf aufgenommen, welcher jedoch noch nicht in Kraft getreten ist.

1.5. Polizei, Sicherheit und Justiz

Liechtenstein beteiligt sich am sogenannten Visa Waiver Program (VWP) der USA. Damit können Liechtensteiner in die USA einreisen, ohne einer Visumspflicht zu unterstehen. Nach den Anschlägen des 11. September 2001 wurde die Frage der Einreise mit Sicherheitsaspekten verknüpft: Nach dem Austausch von Passdaten kam es 2010 zwischen den USA und Liechtenstein zum Abschluss des Terrorist Information Sharing Agreements (TISA). Danach entstand die Forderung des Abschlusses eines **Agreement on enhancing cooperation in preventing and combating serious crime (PCSC)**.[26] Das PCSC stellt ein Rahmenabkommen zum Datenaustausch zur Bekämpfung schwerer Kriminalität dar. Das Abkommen wird auch als sogenanntes „Prüm-like"

19 Checkliste für Benutzungsreglemente betreffend mobile Geräte, http://www.llv.li/pdf-llv-dss-checkliste_mobile_geraete.pdf.
20 Art. 52b KomG.
21 Statistik gem. Art. 52 KomG/Art. 54b VKND. Die entsprechende Richtlinie 2006/24/EG wurde bis heute nicht in den EWR übernommen. Somit besteht auch noch keine Pflicht zur Berichterstattung über die Statistik.
22 Vgl. hierzu auch Tätigkeitsbericht 2009, 1.7.; Tätigkeitsbericht 2010, 1.3.
23 Das Gesetz über den strafrechtlichen Schutz des persönlichen Geheimbereichs regelt nicht die grundsätzliche Zulässigkeit des Aufzeichnens durch Behörden, sondern bestimmt lediglich, wann das Aufzeichnen und Abhören von Telefonaten strafbar ist. Es kann daher nicht als ausreichende Rechtsgrundlage im Sinne von Art. 21 Abs. 1 DSG herangezogen werden.
24 Verordnung vom 14. März 2000 zum Gesetz über die Krankenversicherung (LR 832.101).
25 Art. 36 der Verordnung zum Gesetz über die Krankenversicherung (KVV). Vom Aufschub ausgenommen ist die Übernahme von Kosten für medizinisch notwendige Leistungen oder Leistungen bei Mutterschaft.
26 Vgl. 3.

Abkommen bezeichnet und orientiert sich am Prümer Vertrag. Der liechtensteinische Entwurf für ein solches Agreement orientierte sich am Abkommen zwischen den USA und Österreich, da es aus Datenschutzsicht als sehr streng galt.[27] Gegenstand ist der *Austausch von Fingerabdrücken und DNA-Angaben*. Liechtenstein verfügt über eine gemeinsame Fingerabdruck- und DNA-Datenbank mit der Schweiz, was im Abkommen berücksichtigt wurde. Obwohl wir nicht zuständig sind für die Aushandlung von Staatsverträgen, nahmen wir angesichts der Wichtigkeit der Sache für Liechtenstein ausnahmsweise an den Verhandlungen zur Schaffung des Abkommens teil. Dies sollte jedoch ein Ausnahmefall bleiben. Denn nach dem DSG sind wir für die Anwendung des Datenschutzes, und nicht für legislative Aufgaben, zuständig.

Anlässlich von Kontrollen nach Art. 52 KomG kam unter anderem zur Sprache, dass die Provider den zur Anordnung einer Überwachungsmassnahme elektronischer Kommunikation erforderlichen gerichtlichen Beschluss *vollständig und ungeschwärzt* übermittelt erhalten. Durch diese Vorgehensweise werden ihnen zum Teil äusserst sensible und möglicherweise auch dem Amtsgeheimnis unterfallende Informationen mitgeteilt, die diese zur Umsetzung der Überwachungsmassnahme nicht benötigen. Das kann zu einer Verletzung des Rechts auf Achtung der Privatsphäre der in dem Beschluss namentlich genannten Personen führen. In der österreichischen Strafprozessordnung, die für die liechtensteinische als Rezeptionsvorlage diente, wird dieser Interessenskonflikt dadurch gelöst, dass explizit eine gesonderte, d.h. gekürzte *Betreiberausfertigung* vorgesehen ist, in der nur *die für eine Durchführung* der angeordneten Überwachungsmassnahme *erforderlichen* Angaben aufzuführen sind.[28] Mit Vorsehen einer solchen gesonderten Betreiberausfertigung in der ö-StPO wurde nach unserer Ansicht eine Ausgestaltung gefunden, die den Interessen und Rechten aller Beteiligten gleichermassen dient. Dieser Teil der Bestimmung wurde (noch) nicht in die liechtensteinische StPO übernommen, wodurch sich nunmehr diese datenschutzrechtlich problematische **Regelungslücke im Rahmen von § 103 StPO** ergibt. Wir haben demzufolge das Ressort Justiz um Prüfung einer Ergänzung von § 103 StPO mit einer zu § 138 Abs. 3 ö-StPO vergleichbaren Regelung gebeten.

Eine weitere Frage zur Datenbekanntgabe betraf die Pflicht zur Auskunft über (Auszüge von) Akten, wenn einer Behörde ein Verdacht auf eine Straftat vorliegt. Bei Offizialdelikten sieht § 53 StPO eine Anzeigepflicht für Behörden vor. Diese Anzeigepflicht umfasst in der Regel auch eine entsprechende umfassende Akteneinsicht, da die Anzeigepflicht ansonsten ins Leere laufen würde.[29] D.h. in einem solchen Fall ist die Behörde dazu verpflichtet, die für die Ermittlungen erforderlichen Informationen an die zuständige Ermittlungsbehörde bekanntzugeben. Ein Verstoss gegen das Amtsgeheimnis liegt in diesem Falle nicht vor.[30]

1.6. Wirtschaft und Finanzen

Mit der vorletzten Revision des DSG im Jahr 2009 wurde der **Vorbehalt bzgl. des Sorgfaltspflichtgesetzes (SPG)** ersatzlos gestrichen.[31] Das SPG selbst kennt in der jetzigen Fassung jedoch keine speziellen Datenschutzbestimmungen. Das hat zur Folge, dass bei der Bearbeitung von Personendaten im Rahmen des SPG das DSG voll, und nicht nur subsidiär, zur Anwendung kommt. Dies führt aufgrund der sensiblen Thematik zu Spannungsfeldern, die auch auf europäischer und internationaler Ebene intensiv diskutiert werden.[32] Dem Verhältnismässigkeitsgrundsatz des DSG, wonach nur die zwingend erforderlichen Daten zu erheben und zu bearbeiten sind, steht im Besonderen der „risk based approach" des SPG entgegen, wonach möglichst viele Informationen gesammelt werden müssen. Da die Aufhebung des

27 Das PCSC funktioniert als „hit/no hit-System" durch die automatische Abfrage von Fingerabdrücken. Es kommt daher grundsätzlich zu keinem unmittelbaren Datenaustausch, ebenso werden keine Untersuchungsakten übermittelt. Durch die automatische Abfrage von Fingerabdrücken kann eine Identifikation herbeigeführt werden. Erst nach einem „hit" (Treffer) erfolgt im Wege der Amtshilfe ein Austausch personenbezogener Daten. Das Abkommen sieht die Einrichtung von Kontaktstellen vor. Im Falle eines Treffers kommt es zu einer Kontaktaufnahme mit der jeweils zuständigen Kontaktstelle. Die Amtshilfe erfolgt im Rahmen der Polizeizusammenarbeit mittels einer Rechtshilfeanfrage (Mutual Legal Assistance, MLA-Request). Kommt es zu keinem Treffer („no hit"), erfolgt eine sofortige Löschung der Fingerabdrücke.

28 § 138 Abs. 3 der österreichischen Strafprozessordnung (ö-StPO).

29 Vgl. Fabrizy, Kurzkommentar zur österreichischen Strafprozessordnung, 11. Auflage, Wien 2011, RN 12 zu § 78 ö-StPO.

30 Vgl. Art. 38 Abs. 2 StPG. Im Falle des Art. 38 Abs. 3 StPG in Verbindung mit Art. 31 StPV ist jedoch eine gesonderte Befreiung vom Amtsgeheimnis erforderlich.

31 Vgl. Tätigkeitsbericht 2009, 1.6.

32 Vgl. Dokument der Europäischen Kommission COM(2012) 168 final.

SPG-Vorbehaltes im DSG nicht durch eine entsprechende Revision des SPG begleitet wurde, herrscht nun Unklarheit in der Rechtsanwendung. Dies sollte der Gesetzgeber dringend nachholen.

1.7. Arbeitsbereich

Hier sei daran erinnert, dass wir einige Beschwerden zum Datenschutz am Arbeitsplatz erhielten.[33]

Die neuen Reglemente für die Landesverwaltung zur Regelung von **Mobbing und sexueller Belästigung am Arbeitsplatz** sehen u.a. vor, dass das Amt für Personal und Organisation (APO) die Erfahrungen der medizinischen Anlaufstellen jährlich und in anonymisierter Form den Vorgesetzten in der entsprechenden Behörde zur Verfügung stellt. Zu diesem Zweck wurde durch die Landesverwaltung ein Dokument zur „Falldokumentation" ausgearbeitet, das die Anlaufstellen jeweils ausfüllen und dem APO zuschicken sollen. Die statistischen Erhebungen sollen es dem APO ermöglichen, hierauf basierend die Notwendigkeit und Effektivität der Vorgehensweise besser einschätzen und die Prozesse stetig im Interesse aller Beteiligten optimieren zu können. Entscheidend beim Ausfüllen dieser Falldokumentation ist die Anonymität.[34] Ansonsten bestünde die Gefahr, dass das Arztgeheimnis bzw. die Verschwiegenheitspflicht nach dem Gesundheitsgesetz widerrechtlich verletzt wird. Dies könnte strafrechtliche Folgen nach sich ziehen.[35] Die erste Vorlage dieser Falldokumentation konnte die Anonymität nicht gewährleisten. Wir machten auf diesen Missstand aufmerksam.

In einer Anfrage ging es um die **Geltung des Briefgeheimnisses am Arbeitsplatz**. Hier konnten wir zur Beantwortung auf unsere *Richtlinien über Internet- und E-Mail-Überwachung am Arbeitsplatz für öffentliche Verwaltungen und Privatwirtschaft* verweisen.[36] Danach ist die private Post[37] am Arbeitsplatz zu schützen und ungeöffnet an die adressierte Person weiterzuleiten. Wird private Post durch Drittpersonen trotzdem geöffnet, so kann eine widerrechtliche Persönlichkeitsverletzung vorliegen, die rechtliche Konsequenzen nach sich ziehen kann. Ähnlich wie bei der schriftlichen Post darf der Arbeitgeber aufgrund des Persönlichkeitsschutzes keine Einsicht in den Inhalt **privater E-Mails** des Arbeitnehmers haben. Eine automatisierte Unterscheidung zwischen privaten und geschäftlichen E-Mails ist kaum möglich. Private E-Mails sind vom Absender demzufolge durch eine Vermerkoption „privat" zu kennzeichnen. Wenn kein Unterscheidungsvermerk zwischen privaten und beruflichen E-Mails besteht und die private Natur eines E-Mails aufgrund der Adressierungselemente nicht erkennbar und nicht anzunehmen ist, darf der Arbeitgeber – analog den klassischen Postsendungen – davon ausgehen, dass das E-Mail beruflich ist. Bestehen Zweifel über die Natur eines E-Mails, ist sie mit dem Angestellten zu klären. Ein Entpacken und weiteres Bearbeiten (z.B. Sichern, Weiterleiten, Scannen) von E-Mails, welche als „privat" gekennzeichnet bzw. erkennbar sind, bleibt dem Arbeitgeber somit verwehrt. Eine Möglichkeit, den Inhalt von privaten E-Mails zu schützen, besteht darin, einen internetbasierten, vom geschäftlichen getrennten und wenn möglich verschlüsselten E-Mail-Dienst zu gebrauchen.[38]

1.8. Datenbekanntgabe im Inland

Mit dem Gesetz über das **Zentrale Personenregister** wurde einer alten Forderung nachgekommen. Bereits 2003 hatten wir darauf hingewiesen, dass eine zentral geführte Datenbank, in der Angaben vor allem der gesamten ständigen Bevölkerung mit bis

33 Vgl. 1.1.

34 Zu den Voraussetzungen an eine Anonymisierung siehe unten, 2.3.; Richtlinie über die Anwendung der Anonymisierung/Pseudonymisierung, http://www.llv.li/pdf-llv-dss-richtlinie-anonymisierung-pseudonymisierung.pdf.

35 § 121 StGB.

36 Vgl. Richtlinien über Internet- und E-Mail-Überwachung am Arbeitsplatz für öffentliche Verwaltungen und Privatwirtschaft, S. 22ff.; http://www.llv.li/richtlinien_ueber_internet-_und_e-mail-ueberwachung_am_arbeitsplatz.

37 Als Privatpost gilt eine Sendung, bei der erkennbar ist, dass sie einem Arbeitnehmer nicht in beruflicher Eigenschaft, sondern als Privatperson zugestellt worden ist. Anhaltspunkte für Privatpost sind besondere Vermerke wie „privat" oder „vertraulich". Massgebend ist auch die Art der Sendung (Todesanzeige, adressierte Zeitung oder Zeitschrift) oder äussere Merkmale (Kleinformate, farbiges Papier). Die Anschrift „Herr X, Amtsstelle Y" lässt somit erst dann auf den persönlichen Inhalt schliessen, wenn dies durch einen Zusatz („privat" usw.) zum Ausdruck gebracht wird. In diesen Fällen dürfen Drittpersonen die so gekennzeichnete Post nicht öffnen.

38 Die Verschlüsselung kann bspw. durch Benutzung von PGP-Software (Pretty Good Privacy) oder webbasierter E-Mail-Dienste wie Hushmail.com gewährleistet werden, wobei ein vollständiger Schutz nur erreicht wird, wenn sowohl Absender wie auch Empfänger einen verschlüsselten E-Mail-Dienst benutzen.

zu 51 Datenfeldern gespeichert sind, auf die wiederum (damals) 24 Amtsstellen zugreifen können, eine rechtliche Grundlage benötigt.[39] Das Gesetz trat am 1. Januar 2012 in Kraft und sieht u.a. eine ZPR-Kommission vor, in der wir vertreten sind.[40] In der Anfangsphase ging es darum zu definieren, welche Behörden in der Kommission vertreten sind. Das Gesetz ist hierzu nicht ganz klar. Daneben wurde nach den Übergangsbestimmungen des Gesetzes im ersten Jahr die *Geschäftsordnung* der Kommission geschaffen.[41] Ebenso war ein *Bearbeitungsreglement* zu schaffen. Dieses konnte basierend auf einem älteren Entwurf rechtzeitig fertiggestellt werden. Im Sinne der Transparenz wurde beschlossen, dieses im Intranet für sämtliche Mitarbeiter abrufbar zu machen. Schliesslich sahen die Übergangsbestimmungen vor, dass die Kommission bis Jahresende zu prüfen hatte, ob Behörden, die im Zeitpunkt des Inkrafttretens dieses Gesetzes Daten bearbeiten oder abfragen dürfen, die *gesetzlichen Voraussetzungen* dafür erfüllen. Ist dies nicht der Fall, so hat die ZPR-Kommission der betroffenen Behörde die Datenbearbeitung oder Datenabfrage zu untersagen.[42] Dieser Prüfung der bereits bestehenden Bearbeitungs- und Abfragemöglichkeiten der Ämter wurde – trotz unseres Hinweises auf diese gesetzliche Übergangsbestimmung – in der vorgegebenen Frist nicht nachgekommen. Daneben sehen die Gesetzesmaterialien verschiedene weitere Massnahmen vor, die zur Gewährleistung des Rechts auf Achtung der Privatsphäre notwendig sind.[43] Hier ist insbesondere die *Schaffung der Verhältnismässigkeit* zu nennen: Damit muss sichergestellt sein, dass einem Sachbearbeiter lediglich jene Informationen durch das ZPR zugänglich sind, welche er zur Erfüllung seiner Aufgabe benötigt. Weitere notwendige Anpassungen betreffen die Einschränkung des Zugriffs auf *Vergangenheitsdaten*, die Implementierung des gesetzlich vorgesehenen *Sperrrechts* sowie die *Anonymisierung von Testdaten*. Seit dem Inkrafttreten des ZPRG konnten Fortschritte in der Umsetzung der oben genannten Forderungen erzielt werden. So wurde beispielsweise die Leseprotokollierung[44] technisch vorbereitet als auch entsprechende Werkzeuge und Hilfsmittel für die Administration des ZPR geschaffen, welche in weiterer Folge die Umsetzung der Verhältnismässigkeit erleichtern sollten. Doch sind zahlreiche Punkte nach wie vor offen.

Im Rahmen von Verfassungsinitiativen werden bekanntlich Unterschriften in der Bevölkerung gesammelt und am Schluss der Regierungskanzlei zur Prüfung abgegeben. Bei der **Initiative „Ja, damit deine Stimme zählt"** wurden wir angefragt, ob die Listen der Personen, welche die Initiative unterschrieben hatten, geheim gehalten werden. Hintergrund der Anfrage waren offenbar Befürchtungen, dass diesen Personen bei einer möglichen Bekanntgabe von Namen an eine dritte Stelle Nachteile entstehen könnten. Die Regierungskanzlei teilte uns auf Anfrage mit, dass keine Namen an Dritte bekanntgegeben werden.

Demgegenüber wurden vereinzelt Aussagen in Bezug auf diese Initiative, die auf *Facebook* gemacht worden waren, in den Zeitungen unter Namensnennung wiedergegeben. Wir wurden angefragt, was davon zu halten ist. Facebook ist eine Plattform, die dem Informationsaustausch dient. Zwar ist diese Internetseite nicht ganz öffentlich zugänglich, doch sind die Registrierungshürden minimal. Jedermann kann Mitglied von Facebook werden und danach Beiträge lesen. Wenn jemand einen Beitrag in einem öffentlichen Forum schreibt, tut er dies, um seine Meinung der Allgemeinheit bzw. den Facebook-Nutzern bekanntzugeben. Zwar wird keine Einwilligung erteilt, damit diese Meinung danach in einer Zeitung zitiert werden darf. Dies ist unserer Ansicht nach auch nicht nötig. Das DSG erwähnt, dass eine Bearbeitung von allgemein zugänglichen Daten erlaubt ist.[45] Angaben auf Facebook sind nach unserer Auffassung aufgrund der minimalen Registrierungsbedingungen *quasi* öffentlich. Damit steht einer Wiedergabe in den Zeitungen aus Datenschutzsicht nichts entgegen.

Eine Gemeinde fragte uns an, in welchen Fällen Daten auf Anfrage bekanntgegeben werden dürfen. Wir

39 Tätigkeitsbericht 2003, 4.1.2.
40 Art. 16 Abs. 1 Bst. b ZPRG.
41 Art. 16 Abs. 5 iVm Art. 21 Abs. 2 ZPRG. Sie ist auf dem Internet abrufbar: http://www.llv.li/amtsstellen/llv-ai-zpr.htm.
42 Art. 21 Abs. 1 ZPRG.
43 Die einzelnen Massnahmen werden im letzten Tätigkeitsbericht aufgelistet: vgl. Tätigkeitsbericht 2011, 7., Fussnote 127., Vgl. dazu Bericht und Antrag betreffend die Schaffung eines Gesetzes über das Zentrale Personenregister (ZPRG), Nr. 67/2011, Pkt. 3.2, sowie Prof. Dr. Dietmar Jahnel in „Zentrale Personenverwaltung in Liechtenstein - Datenschutzrechtliches Gutachten", Februar 2008, http://www.llv.li/pdf-llv-dss-zpv-gutachten-jahnel.pdf.
44 Vgl. Art. 7 Abs. 3 ZPRG.
45 Art. 17 Abs. 2 Bst. f DSG.

wiesen auf unsere Antworten aus dem Jahr 2004[46] hin und informierten ergänzend, dass inzwischen eine spezielle Bestimmung in der Datenschutzverordnung geschaffen worden war.[47] In vielen Fällen besteht ein Ermessensspielraum zur Datenbekanntgabe. Somit entscheidet die Gemeinde selbst, in welchen Fällen Daten bekanntgegeben werden dürfen. Das DSG sieht keine Sanktionen bei einem Missbrauch vor. Deshalb regten wir an, bei Missbrauchsfällen künftig keine Daten mehr bekanntzugeben.

Immer wieder erhalten wir Anfragen, die mit der *Wahrnehmung der Rechte* nach dem DSG zu tun haben. Wenn nun eine Person Auskunft über ihre Daten möchte oder sie berichtigen bzw. löschen möchte, sollte sie sich *entsprechend ausweisen*, wenn sie der entsprechenden Behörde nicht bekannt ist. In dem Sinne sollte eine telefonische Auskunft nur gegeben werden, wenn klar ist, dass es sich bei der anfragenden Person wirklich um die betroffene Person handelt. Zwar wurde schon in unseren *Richtlinien zur Bekanntgabe von Personendaten durch Behörden* darauf hingewiesen.[48] Offenbar wird dies aber nicht immer beachtet. Deshalb sei noch einmal darauf hingewiesen.

Ein anderer Fall betraf die **Bekanntgabe von Lebensbescheinigungen bzw. Mutationsmeldungen** der AHV-Anstalten an Träger sozialer Einrichtungen.[49] Anstoss hierzu hatte die Jahresversammlung des liechtensteinischen Pensionskassenverbandes gegeben, an der u.a. der Austausch von Rentenbezüger-Daten mit der liechtensteinischen AHV problematisiert worden war.[50] Diese Unterscheidung von im Inland und im Ausland lebenden Rentenbezügern ist keine Frage des Datenschutzes, wurde aber offenbar so verstanden.[51] Dies ist übrigens nicht der erste Fall, in dem eine Unmöglichkeit zu Unrecht dem Datenschutz aufgebürdet wird.[52] Ausgehend von der bisherigen Praxis zur Einholung von Lebensbescheinigungen konnte hier zusammen mit Vertretern der AHV und des Pensionskassenverbandes ein gemeinsames Konzept für einen Datenaustausch im Rahmen der gesetzlichen Vorgaben gefunden werden, das im Interesse aller Beteiligten liegt. Die Installierung eines neuen IT-Systems bei der AHV sowie entsprechend angepasste Formulare haben hierbei deutlich zu einer effizienten und datenschutzkonformen Durchführung beigetragen.

1.9. Datenbekanntgabe mit Auslandsbezug

Anfragen zur Zulässigkeit einer grenzüberschreitenden Datenbekanntgabe waren primär aus dem Finanz- und Versicherungsbereich zu verzeichnen. Hier standen vor allem Fragen zur **grenzüberschreitenden Auftragsdatenbearbeitung** (Outsourcing)[53] sowie zu diesbezüglichen Regelungen von Geheimhaltungspflichten[54] im Fokus. Klärungsbedarf besteht oftmals hinsichtlich der *Frage des anwendbaren Rechts*.[55]

Das **Projekt „lebenszyklusorientierte Grund- und Alterssicherung"** orientiert sich am Leitbild einer möglichst transparenten und einfachen Besteuerung der Bürger, bei der das erzielte Einkommen über den Lebenszyklus möglichst nur einmal belastet werden soll. Damit verbunden ist eine umfassende

46 Vgl. Tätigkeitsbericht 2004, 4.1.
47 Art. 18a DSV.
48 Vgl. Seite 11: http://www.llv.li/pdf-llv-dss-richtlinie-datenbekanntgabe-durch-behoerden.pdf. Dementsprechend enthalten unsere Musterschreiben zur Geltendmachung der Rechte einen Hinweis, dass die Identität nachgewiesen werden sollte: http://www.llv.li/form-llv-dss-musterschreiben
49 Vgl. Tätigkeitsbericht 2010, 1.4.
50 Vgl. Vaterland vom 25. April 2012: „Während für die ausländischen Rentenbezüger eine Lösung mit der AHV habe erzielt werden können, gebe sie [AHV] die Daten der einheimischen Bezüger aufgrund des Datenschutzes nicht [an die Träger der beruflichen Vorsorge] weiter. Unsere Aufgabe ist es nun, mit dem Datenschützer eine Einigung zu finden, die mit der Lösung für die ausländischen Bezüger vergleichbar ist."
51 Generell darf die AHV an Organe, die mit der Durchführung sowie der Kontrolle anderer Gesetze im Bereich der sozialen Kontrolle betraut sind, die hierfür erforderlichen Daten bekanntgeben (Art. 19ter Abs. 1 Bst. b AHVG). Eine Differenzierung bezüglich des Wohnorts ist nicht vorgesehen. Mit anderen Worten bedeutet diese Bestimmung für den konkreten Fall, dass die AHV im Einzelfall berechtigt ist, gegenüber den Pensionskassen Mutationsmeldungen (Mutationsmeldungen beinhalten in der Regel Mitteilungen über Adressänderungen, Leistungsänderungen oder -einstellungen) zu erstellen, egal ob der betroffene Rentenbezüger in Liechtenstein oder im Ausland wohnt. Dies kann im Zweifel auch die Mitteilung über eine Leistungseinstellung in Folge eines Todesfalls des Berechtigten beinhalten.
52 Vgl. Pressemitteilung zum Tätigkeitsbericht 2011: http://www.llv.li/pdf-llv-dss-pressemitteilung_tb2011.pdf
53 Art. 19 DSG. Vgl. Tätigkeitsbericht 2011, 2.2.; http://www.llv.li/amtsstellen/llv-dss-spezialthemen/llv-dss-spezialthemen-datenbearbeitung.htm.
54 Zum Beispiel das Versicherungsgeheimnis, von dem nach Art. 44 VersAG entbunden werden kann, vgl. hierzu ausführlich Tätigkeitsbericht 2011, 3. mit weiteren Verweisen.
55 Art. 2 Abs. 2 DSG; vgl. hierzu die Stellungnahme der Artikel-29-Datenschutzgruppe zum anwendbaren Recht (WP 179), abzurufen unter: http://ec.europa.eu/justice/data-protection/article-29/index_de.htm.

„Wohlstandsberichterstattung", welche die Einkommens- und Vermögenssituation sowie die jeweiligen sozialen Lagen möglichst erschöpfend beschreiben kann. Eine solche Berichterstattung setzt voraus, dass auf der Ebene der Einzelpersonen möglichst flächendeckend alle persönlichen Charakteristika erfasst werden. Dies bedeutet, dass für alle Einwohner Liechtensteins Einzeldaten bereitzustellen sind betreffend Alter, Geschlecht, Zivilstand, Ausbildung, Erwerbstätigkeit und Einkünfte (Arbeits- und Vermögenseinkommen, AHV-Renten, Pensionszahlungen, Arbeitslosengeld, Ausbildungsbeihilfen, Unterhaltszahlungen, Sozialhilfe, Wohnbauförderung etc.). Diese und weitere Einzeldaten sollten rückwirkend bis zum Jahr 2000 sowie zukünftig jährlich erhoben und zusammengeführt werden. Zudem waren verschiedene Haushaltsdaten vorgesehen, die jedoch in der Landesverwaltung nicht erfasst werden, wie Bankguthaben, Haushaltsausgaben usw. Wir hielten fest, dass aus Sicht der Privatsphäre jegliche staatliche Massnahme eine gesetzliche Grundlage benötigt. Demgemäss ist zuerst eine gesetzliche Grundlage für die Beschaffung und Bearbeitung sämtlicher Einzeldaten notwendig. Sodann ist die Bestimmung über eine zentrale Führung der Daten bzw. eine Zusammenführung derselben nötig. Schliesslich wäre die Bekanntgabe der gesammelten Daten jedenfalls nur über eine explizite rechtliche Grundlage nötig. Die Daten sollten zu Forschungszwecken bekanntgegeben werden. Bei einer allfälligen Bekanntgabe wäre auch die Sicherstellung einer Datenlöschung nach Erfüllung des erreichten Zwecks notwendig. Zwar sehen Einzelgesetze bzw. Spezialgesetze Aspekte vor, jedoch fehlt es an rechtlichen Grundlagen in dieser Dichte. Wir beurteilten das Vorhaben kritisch. Als besonders problematisch sahen wir bei diesem Vorhaben, dass die gesammelten Daten an eine Person im Ausland gegeben werden sollten. Eine Datenbekanntgabe in einer bisher noch unbekannten Dichte an eine Person im Ausland kann unter Umständen auch trotz einer entsprechenden Vertraulichkeitsregelung zu Problemen führen.

2. Öffentlichkeitsarbeit

2.1. Allgemeines

Aus Anlass des zehnjährigen Bestehens des Datenschutzgesetzes gaben wir eine **repräsentative Umfrage** in Auftrag. Die Umfrage hatte zum Zweck, den Stand der Sensibilisierung der Bevölkerung zum Datenschutz zu testen. Basis war eine Umfrage, die 2008 EU-weit durchgeführt worden war. 500 Personen wurden folgende Fragen gestellt:

1. Wie sehr machen Sie sich Gedanken über den Schutz persönlicher Daten?

   Die Antwort zeigte, dass sich 14 % gar keine, 24 % nicht sehr viel, 36 % ein bisschen und 26 % sehr viele Gedanken machen.

2. Wie gross ist das Vertrauen in Institutionen, wenn es um persönliche Daten geht?

   Am meisten Vertrauen geniessen die Steuerbehörden (93 %), die Polizei (90 %), die Sozialversicherungen (89 %), die Ärzte und Arbeitgeber (je 87 %). Am wenigsten wird Versandhäusern (19 %), Kreditauskunfteien (37 %) und Reiseunternehmen (41 %) vertraut. Insgesamt geniessen die öffentlichen Institutionen sehr grosses Vertrauen.

3. Was denken Sie über den Datenschutz?

   79 % gaben an, dass die eigenen Daten korrekt geschützt werden, 70 %, dass die Bevölkerung wenig über den Schutz von persönlichen Daten weiss, 62 % beunruhigt es, persönliche Daten im Internet anzugeben und 46 % sind der Meinung, dass die Gesetzgebung gut mit der wachsenden Menge persönlicher Daten im Internet umgehen kann.

4. Was wissen Sie über Ihre Rechte zu persönlichen Daten?

   83 % kennen das Recht, eine Verwendung zu verbieten, 91 % das Recht, in gewissen Fällen eine Zustimmung geben zu können, 72 % das Lösch- oder Berichtigungsrecht, 70 % wissen, dass sie einen Zugang zu gerichtlichen Instanzen haben, 51 % wissen, dass sie ein Recht auf Auskunft haben, wenn Dritte Daten über sie speichern und 40 % kennen das Recht auf Schadenersatz.

5. Ist die Übermittlung persönlicher Daten im Internet sicher?

   Diese Frage wurde von 19 % bejaht, von 69 % verneint, 11 % gaben an, das Internet nicht zu nutzen oder keinen Computer zu haben. 1 % hat mit „weiss nicht" geantwortet.

6. Schützen Sie Ihre persönlichen Daten?

   76 % haben aktuelle Schutzprogramme auf dem Computer installiert, 75 % geben nur notwendige Daten an, 58 % tun dies nur bei Firmen, die sie kennen, 55 % tun dies nur auf sicheren Seiten und 53 % achten auf richtige Sicherheitseinstellungen beim Browser.

7. Wie viel Überwachung soll erlaubt sein?

   8 % sind für eine Überwachung des Internets in jedem Fall, 43 % nur bei einem konkreten Verdacht, 35 % sind für eine beaufsichtigte Überwachung bei einem konkreten Verdacht und 12 % meinen, das Internet soll in keinem Fall überwacht werden. 5 % sind für eine Überwachung der Kreditkartennutzung in jedem Fall, 19 % sind in jedem Fall dagegen, 40 % sind für eine Überwachung nur bei Verdacht und 35 % für eine beaufsichtigte Überwachung. 3 % sind für eine Überwachung von Telefongesprächen in jedem Fall, 13 % sind dagegen, 36 % nur bei einem konkreten Verdacht und 46 % sind für eine beaufsichtigte Überwachung.

8. Ist Ihnen eine unabhängige Behörde und deren Aufgaben bekannt?

   71 % der Befragten ist nicht bekannt, dass es eine unabhängige Datenschutzbehörde gibt, 28 % wissen davon und 1 % hat mit „weiss nicht" geantwortet. Von diesen 28 %, die von der Existenz einer unabhängigen Behörde wissen, haben 85 % noch nie Kontakt mit ihr aufgenommen; 84 % sind der Ansicht, dass sie bei Verstössen einschreiten sollte und 82 % meinen, sie sollte Beschwerden entgegennehmen.

Die Einzelheiten der Umfrage können in Anhang 2 eingesehen werden.

Folgende Schlussfolgerungen können aus dieser Umfrage gezogen werden:

Es ist positiv, dass ein grosses Vertrauen gegenüber vor allem öffentlichen Institutionen und der Gesetzgebung gegeben ist. Dies wird allerdings dadurch relativiert, dass 70 % der Bevölkerung der Meinung ist, nur wenig über den Datenschutz zu wissen.

Aus unserer Sicht zeigt die Umfrage, dass die *Bevölkerung besser sensibilisiert* werden sollte. Dies ist jedoch nicht nur unsere Aufgabe, sondern eine, bei der *Synergien* geschaffen werden sollten. Synergien sind in einem so kleinen Land wie Liechtenstein sehr wichtig. Die Umfrage zeigt zudem – nicht überraschend – dass Jugendliche nur wenig sensibilisiert sind. Dies sollte geändert werden. So wäre es z.B. aus unserer Sicht sinnvoll, wenn die Eltern, Schulen, aber auch Medien oder eben wir und auch der Jugendschutzbeauftragte, mit dem wir sehr gut zusammenarbeiten, selbst einen Teil dazu beitragen würden, dieser wichtigen Aufgabe nachzukommen. Dies gilt aber nicht nur beim Themenbereich „Sensibilisierung für neue Medien", sondern allgemein bei allen Themen mit Bezug zum Datenschutz, wie z.B. im Gesundheitswesen.[56]

Die Umfrage zeigt auch, dass sich die Bevölkerung zwar ihrer Rechte bewusst ist. Die Anzahl Personen, die über das *Auskunftsrecht* Bescheid wussten, war jedoch im Vergleich zum Lösch- oder Berichtigungsrecht geringer. Dies ist eigentlich paradox, kann doch ein Löschanspruch erst dann wahrgenommen werden, wenn man weiss, was für Daten bearbeitet werden. Und eben dies erfährt man über das Auskunftsrecht. Am auffälligsten war aus unserer Sicht, dass nur 40 % wussten, dass es einen grundsätzlichen *Schadenersatzanspruch* gibt; 42 % verneinten dies. Die allgemeine Datenschutzrichtlinie 95/46/EG sieht einen solchen Anspruch vor, der in Liechtenstein nicht explizit ins DSG übernommen wurde, aber dennoch gilt.[57] Schliesslich gaben rund 28 % an, von einer *unabhängigen Datenschutzbehörde* zu wissen. Von diesen 28 % gaben nur 15 % an, mit

56 Zum Thema „Neue Medien" wurde inzwischen eine Arbeitsgruppe geschaffen, in der wir auch vertreten sind.

57 Vgl. Art. 23 der Richtlinie. Schadenersatzansprüche können im Privatrechtsbereich aufgrund von § 1328a ABGB oder im öffentlichen Bereich aufgrund des Amtshaftungsgesetzes gestellt werden.

uns je Kontakt gehabt zu haben. Dies kann darin begründet sein, dass aufgrund des erwähnten hohen Vertrauens kein Grund zu einer Kontaktaufnahme bestand; ein anderer Grund kann darin bestehen, dass die Sensibilisierung eben zu niedrig ist und ein mögliches Problem nicht erkannt wurde; ein dritter möglicher Grund kann im Nichtwissen über eine Schadenersatzmöglichkeit gegeben sein.

Das interregionale Jugendschutzprojekt **„Gateway – Abenteuer Neue Medien"** bot eine willkommene Gelegenheit zur Sensibilisierung,[58] indem wir wiederum an der LIHGA präsent waren. Dabei gab es interessante *Diskussionen* zum Thema *Internet*. Viele Eltern sind sich bewusst, dass sie ihr Kind nicht unbeaufsichtigt lassen sollten. Während einige sich mit dem Thema nicht gut auskennen und so den Kindern praktisch freie Hand lassen, klären andere ihre Kinder aktiv auf und waren an den Broschüren, die wir verteilten,[59] sehr interessiert. Eltern können sich bei diesem Thema überfordert fühlen. Deshalb sehen wir uns darin bestätigt, dass das Thema „Neue Medien" systematisch angegangen werden sollte. An der LIHGA informierten wir zu folgenden Themen:

Anhand eines praktischen Beispiels zur *Personensuche auf dem Internet* zeigten wir, wie aufgrund von öffentlich zugänglichen Informationen in Kombination mit Informationen, die eine Person selbst ins Internet stellt, praktisch ein Persönlichkeitsprofil entsteht.[60] Man hört immer wieder das Argument: „Ich habe nichts zu verbergen." Die Kombination von Informationen, die man selbst ins Internet gestellt hat mit sonst öffentlich zugänglichen Informationen führt dann doch teils zu Erstaunen. Eine Person beschwerte sich bei uns, dass auf einer sogenannten „naming and shaming" Internetseite[61] ein Foto auftauchte, auf dem sie abgebildet war. Das Foto stammte aus dem Facebook-Profil der betroffenen Person. Eine Löschung dieses Fotos war auf dieser Internetseite nur gegen Bezahlung vorgesehen. Dies entspricht nicht dem europäischen Datenschutzrecht. Unsere Nachforschungen ergaben, dass die Seite international verflochten ist, so dass eine Durchsetzung des Löschrechts sehr schwierig, wenn nicht gar unmöglich ist. Natürlich sollte man darauf achten, welche Fotos man im Internet veröffentlicht. Dieses Beispiel zeigt aber auch, dass „normale" Fotos zu unangenehmen Situationen führen können. Dies war eine unserer Kernaussagen an der LIHGA. Eine andere unangenehme Situation kann entstehen, wenn man auf einem Foto auf Facebook markiert wurde. Nicht davon zu reden, wenn man zu Unrecht an den „Pranger" gestellt oder gar gemobbt wurde.

Zudem informierten wir zum Datenschutz bei *Social-Games*[62]. Betreiber von Social-Games sind verpflichtet, ihre Datenbearbeitung auf die für die Dienstererbringung erforderlichen Daten zu beschränken und es muss für jede Datenerhebung vorab auch ein definierter Zweck vorliegen, über den die Spieler auch zu informieren sind. Nur wenige Datenschutzerklärungen sind so verfasst, dass sie dem Grundsatz der sowohl umfassenden als auch verständlichen Aufklärung entsprechen. Gerade bei der tiefen Verknüpfung in soziale Netzwerke ist nicht immer differenzierbar, welche Daten zu welchem Zweck dem Spiele-Betreiber durch das Soziale Netzwerk zur Verfügung gestellt werden. Anhand von Beispielen wurden die Besucher diesbezüglich sensibilisiert.

Schliesslich machten wir auch auf den Datenschutz auf *Smartphones*[63] oder in sozialen Netzwerken aufmerksam.

Im Landtag war die Anregung entstanden, dass wir uns regelmässig in den Medien äussern und infor-

58 Interessant ist dabei insbesondere eine Broschüre – der sogenannte „Facebook-Check" – die speziell für Jugendliche zur Problematik der Privatsphäre bei Facebook erstellt worden war. Sie ist in Schulen an Jugendliche direkt abgegeben und an Elternabenden verteilt worden.
Siehe auch Massnahmenkatalog zum Familienleitbild 2012 der Regierung, Seite 27: http://www.familienportal.li/fileadmin/user/Dokumente/20120611__Massnahmenkatalog.pdf

59 Die meisten Broschüren stammen von www.klicksafe.de.

60 Wir nutzten für die Internet Recherche insbesondere soziale Netzwerke (Facebook, LinkedIn, Xing), Online-Telefonbücher, (Personen-)Suchmaschinen wie www.123people.com oder www.yasni.com, www.eautoindex.ch, Online Firmen- und Personenregister (z.B. www.moneyhouse.ch), Ahnenforscherdatenbanken sowie Onlineauftritte von Gemeinden und anderen öffentlichen Stellen. Hilfreich für die Erstellung von Personenprofilen waren auch öffentlich abrufbare Vereins- und Gemeindeprotokolle, wo teilweise konkrete Wortmeldungen nachgelesen werden können. Siehe auch z.B. die Babyliste des Landesspitals: http://landesspital.li/Services/Babyliste/tabid/1153/Default.aspx

61 Die Internetseite jerk.com funktioniert, wie der Name schon sagt (jerk bedeutet „Dummkopf" oder „Trottel"), nach dem Prinzip der Blossstellung, vgl. dazu 1.1.

62 Spiele, die insbesondere in sozialen Netzwerken mit „Freunden" gespielt werden (z.B. FarmVille).

63 http://www.bitkom.org/de/themen/50792_71151.aspx.

mieren.[64] Dazu bekamen wir im dreimal jährlich erscheinenden **PeCe-Magazin** Gelegenheit. Folgendes wurde thematisiert:

Online-Werbung, und dabei speziell die *nutzerbasierte Online-Werbung*, stellt eine wesentliche Einnahmequelle für kostenlose Dienste im Internet dar. Uns ist bewusst, dass Werbeinhalte, welche an die Interessen der Nutzer angepasst sind, durchaus einen Mehrwert für Internetnutzer haben können und diese Form der Werbung häufig positiv empfunden wird. Dazu fehlt aber bisher die nötige Transparenz den Nutzern gegenüber.[65] Als Grundlage für die nutzerbasierte Online-Werbung dienen Interessenprofile der Internetnutzer, deren Erzeugung und Speicherung auf den ersten Blick harmlos erscheinen mag. Ein einmal erstelltes Profil eines Studenten kann jedoch zu einem späteren Zeitpunkt kompromittierend sein: Zum Beispiel wenn dieser zuvor für eine Studienarbeit über einen längeren Zeitraum intensiv über Rechtsradikalismus oder andere gesellschaftskritische oder gar strafrechtlich relevante Themen im Internet recherchiert hat. Gefordert sind in einem ersten Schritt insbesondere die Betreiber von Internetseiten, die sich direkt für eine datenschutzkonforme Ausgestaltung verantwortlich zeichnen und für die Privatsphäre ihrer Besucher die Verantwortung tragen.

Im zweiten Magazin hatten wir die Gelegenheit, Datenschutzaspekte im Zusammenhang mit der nächsten Generation *Internet-Protokoll (IPv6)* anzusprechen. Durch den damit zur Verfügung stehenden, beinahe unbegrenzten Adressraum können zukünftig sämtliche Geräte wie Computer, Smartphones, Multimedia-Geräte wie TV und Radio, Navigationsgeräte usw. mit einer statischen IP-Adresse direkt mit dem Internet verbunden werden: das „*Internet der Dinge*". Mit den praktischen Vorteilen sind jedoch Risiken für die Privatsphäre verbunden, z.B. die einfache Identifizierung der Nutzer und deren Geräte im Internet aufgrund statisch vergebener IP-Adressen. In Stellungnahmen von Datenschutzbehörden werden verschiedene Anforderungen an den Einsatz von IPv6 gestellt.[66] Beispielsweise wird gefordert, dass u.a. die dynamische Zuweisung von IP-Adressen durch den Internet-Service-Provider (ISP) auch künftig möglich sein soll. Die ISPs sollten zudem Internetnutzer mit Anonymisierungsdiensten dabei unterstützen, eine dauerhafte Identifizierung über deren IP-Adresse zu verhindern oder wenigstens zu erschweren. Gerade hier sind insbesondere auch die Gerätehersteller aufgefordert, bei der Entwicklung von Produkten *(„privacy by design")* sowie bei den jeweiligen Standard-Konfigurationen *(„privacy by default")* die entsprechenden Datenschutzaspekte zu berücksichtigen. Eine grosse Herausforderung für den Datenschutz ist es, die Voraussetzungen dafür zu schaffen, dass gerade bei zukünftigen Entwicklungen die Privatsphäre der Betroffenen über sämtliche Bereiche hinweg, vom Transportprotokoll bis zur Applikationsebene, berücksichtigt und zusätzlich ein Wettbewerbsvorteil für vorbildliche Unternehmen generiert wird.

Das dritte Magazin hatte die *Sicherheit im Unternehmen* zum Gegenstand, ein wichtiges Thema für die Wirtschaft. Angesprochen waren Methoden von Zutrittskontrollen und Passwortschutz über das Dokumentenmanagement bis zum Outsourcing. Wir wiesen darauf hin, dass hier, wie so oft, die Interessen der Betroffenen (Unternehmen, Kunden, Angestellte) gegeneinander abzuwägen sind. Aufgrund einer Risikoanalyse der zu bearbeitenden Daten ist das Sicherheitsniveau zu bestimmen. So sind bei einem Bäcker und bei einer Bank nicht dieselben Voraussetzungen gegeben. Aber auch innerhalb einer Bank gibt es sensiblere Bereiche, die besser zu schützen sind als andere. Biometrische Zutrittssysteme kommen immer mehr in Mode. Bei der Wahl eines solchen Systems ist aber zu berücksichtigen, dass biometrische Daten höchstpersönlich und in der Regel

64 Vgl. Tätigkeitsbericht 2011, 6.

65 Dies wird sich mit der Umsetzung der Richtlinie 2009/136 ändern. Art. 5 Abs. 3 der Richtlinie 2002/58 wird danach wie folgt geändert: „Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäss der Richtlinie 95/46/EG u.a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat …"

66 Artikel-29-Datenschutzgruppe, Stellungnahme über die Verwendung eindeutiger Kennungen bei Telekommunikationsendeinrichtungen: das Beispiel IPv6, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp58_de.pdf; IWGDPT, Arbeitspapier zur Nutzung eindeutiger Identifikatoren in Telekommunikationsendgeräten: das Beispiel IPv6, http://www.datenschutz-berlin.de/attachments/206/wpipv6_de.pdf; Orientierungshilfe – Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft, http://www.bfdi.bund.de/DE/Themen/TechnologischerDatenschutz/TechnologischeOrientierungshilfen/Artikel/Orientierungshilfen_IPv6.html.

unveränderbar sind. Deshalb sollte nur bei einem hohen Sicherheitsanspruch auf *biometrische Daten* zurückgegriffen werden.[67] Zum Thema Zugriffsschutz verwiesen wir auf die Anforderungen eines starken Passworts.[68] Auch beim Thema *Outsourcing* bzw. beim Spezialfall *Cloud Computing* ist es wichtig, für die Sicherheit in einem Unternehmen zu sorgen. Dies allein schon aus Haftungsfragen. Zentral ist, dass die gesetzlichen Bestimmungen eingehalten werden und eine Datenbearbeitung im Auftrag (Outsourcing) überhaupt erlaubt ist.[69]

2.2. Veranstaltungen

Anlässlich des **6. Europäischen Datenschutztages** führten wir wieder eine Veranstaltung mit dem Institut für Wirtschaftsinformatik der Universität Liechtenstein durch. Der Vortragsabend stand ganz im Zeichen des Internets. Unter dem Titel *„Was weiss das Internet über mich?" – Meine Daten als Handelsware!* veranstalteten wir einen Vortragsabend zum Spannungsverhältnis von nutzerbasierter Online-Werbung und Datenschutz. Das Internet ist zum vermeintlich unentbehrlichen Hilfsmittel geworden. Wir surfen täglich im Internet, holen uns Informationen, wickeln Geschäfte ab – und hinterlassen Spuren. Ob das Internet wirklich „gratis" ist oder wir mit unseren persönlichen Daten „bezahlen", diesen und anderen Fragen gingen wir nach. Hauptakteure waren Vertreter des IT Crowd Club Liechtenstein[70], die das Publikum zu verschiedenen Themen direkt befragten sowie ein Vortrag von Dr. Günter Karjoth. Im Internet stellt die **Online-Werbung** eine zentrale Einnahmequelle für eine Vielzahl von Online-Diensten dar und ist somit ein wichtiger Faktor für das Wachstum und die Expansion der Internetwirtschaft. Behavioural Targeting (auch „Online Targeting")[71] bezeichnet eine besondere Art der Werbung, welche grundsätzlich Bedenken in Bezug auf den Datenschutz und die Privatsphäre hervorruft. Behavioural Targeting beruht im weitesten Sinne darauf, dass das Surfverhalten von Internetnutzern durch den Einsatz verschiedenster Techniken beobachtet und ausgewertet wird, um mit den dadurch gewonnenen Erkenntnissen ein Benutzerprofil mit den Interessen des jeweiligen Nutzers zu erstellen. In weiterer Folge können jedem Internetnutzer somit entsprechend zugeschnittene Werbeinhalte bereitgestellt werden.[72]

Im August 2011 hatten wir erstmals alle **Datenschutzverantwortlichen** zu einer Informationsveranstaltung eingeladen, bei der es um das Thema *„Aufgaben und Stellung eines Datenschutzverantwortlichen"* ging.[73] Die Erfahrung hatte gezeigt, dass die Unterschiede zwischen den behördlichen und betrieblichen Verantwortlichen in der Praxis zu gross sind. Deshalb führten wir diesmal zwei getrennte Veranstaltungen durch. Bei der Informationsveranstaltung für die Behörden wurde durch das Ressort Justiz die letztjährige Revision des DSG vorgestellt. Danach informierten wir jeweils über unsere Tätigkeiten seit der letzten Veranstaltung. Abschliessend fand ein Meinungsaustausch mit den Verantwortlichen, aber auch den Datenschutzberatern, statt. Dieser Erfahrungsaustausch zeigte, dass aufgrund der Kleinheit des Landes Synergien sinnvoll sind. Wir sehen es als unsere Aufgabe an, auch die Datenschutzverantwortlichen bei ihrer Tätigkeit zu beraten; schliesslich ist die Beratung eine unserer gesetzlichen Aufgaben.

Neben diesen Veranstaltungen, die wir selbst organisierten, konnten wir an verschiedenen anderen teilnehmen, so bei **Diskussionsveranstaltungen** in Eschen, Planken und Balzers, organisiert durch den Jugendschutzbeauftragten des Landes. Im Zentrum standen *neue Medien und soziale Netzwerke*. Zweck war die Sensibilisierung von Eltern und Jugendlichen für die Gefahren und Chancen neuer Medien und sozialer Netzwerke im Internet. Im Rahmen des „Europäischen Jahres für aktives Altern und Solidarität zwischen den Generationen" fand in Schaan eine *grosse Generationentagung* statt. Auch dort wiesen wir in einem generationsübergreifenden Workshop auf die Gefahren und Risiken bei der Nutzung von sozialen Netzwerken hin.[74]

67 http://www.llv.li/amtsstellen/llv-dss-spezialthemen/llv-dss-spezialthemen-biometrische_daten.htm.
68 https://review.datenschutz.ch/passwortcheck/check.php?lang=de.
69 Art. 19 DSG sowie http://www.llv.li/amtsstellen/llv-dss-spezialthemen/llv-dss-spezialthemen-datenbearbeitung.htm
70 https://itcc.li.
71 Siehe auch oben, 1.6. und 2.1.; vgl. auch Tätigkeitsbericht 2009, 1.1.2.
72 Weitere Informationen zum Datenschutztag unter http://www.llv.li/amtsstellen/llv-dss-datenschutztag/llv-dss-datenschutztag-6.htm. Vgl. auch oben, 2.1.
73 Tätigkeitsbericht 2011, 2.1.
74 http://www.generationen-begegnungen.li/Portals/0/docs/Generationentagung_2012_web.pdf, S. 43ff.

Neben der seit Jahren üblichen **Datenschutz-Schulung** in der *Landesverwaltung* führten wir wiederum eine *Schulung an der Universität* des Master-Studiengangs Business Process Engineering der Wirtschaftsinformatik durch.[75] Neben einer juristischen Einleitung zur Vorstellung und Anwendung des DSG im betrieblichen Umfeld wurden den Studenten insbesondere die technischen Aspekte wie die Unterschiede zwischen IT-Sicherheit und Datenschutz, Standards und Leitfäden, Privacy Enhancing Technologies (PETs) und deren Anwendung in einem Unternehmen aufgezeigt.

2.3. Neuigkeiten auf der Internetseite

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

Das Internet hat sich in den letzten Jahren rasant zu einem Instrument entwickelt, das bei der Arbeit und im Privatleben kaum mehr wegzudenken ist. Mehr noch, die stetig steigenden Speicherkapazitäten von mobilen Geräten und die immer schneller werdenden drahtlosen Netzwerke erlauben eine mobile und internetbasierte Datenverarbeitung in einer Art und Weise, die in der Vergangenheit nur in festen und sichereren Umgebungen möglich war. **Das Internet – jederzeit und überall!** Wir haben Tipps für Massnahmen für einen erweiterten Basisschutz als auch weitere Informationen zu Datensicherheit im Internet veröffentlicht.[76]

Das DSG enthält *keine* Begriffsdefinitionen für das **Anonymisieren** oder das **Pseudonymisieren** von Personendaten. Dieses Fehlen einer Legaldefinition bringt eine gewisse Rechtsunsicherheit für den Dateninhaber mit sich, wie die Begriffe auszulegen und in der Praxis anzuwenden sind. Obwohl die Begriffe im umgangssprachlichen Gebrauch häufig synonym verwendet werden, gibt es signifikante Unterschiede. Gemeinsam ist beiden, dass sie darauf abzielen, einen direkten bereits bestehenden oder möglichen Bezug zwischen Personendaten und einer bestimmten oder bestimmbaren Person zu entfernen. Der wesentliche Unterschied besteht darin, dass bei der Pseudonymisierung eine charakteristische Zuordnungsregel zwischen pseudonymisierten Daten und Personendaten existiert. Während bei der *Anonymisierung* durch Verfahren wie z.B. das Löschen der Identifikationsmerkmale oder das Zusammenfassen von Datensätzen (Aggregation) ein *Personenbezug unwiderruflich*[77] entfernt wird, werden bei der *Pseudonymisierung* die *Identifikationsmerkmale durch Aliase* ersetzt, wodurch ein Personenbezug bestehen bleibt.[78] Die Pseudonymisierung setzt also im Unterschied zur Anonymisierung eine Regel oder Vorschrift voraus, aus der sich die Zuordnung des Alias zu einer bestimmten Person ergibt. Somit ist es bei der *Pseudonymisierung* möglich, durch die Kenntnis bestimmter Parameter und Verfahren aus den vorhandenen oder noch vorhandenen Daten wieder einen *Personenbezug herzustellen*. Anonymisierung und Pseudonymisierung stellen Verfahren für Privacy Enhancing Technologies (PETs)[79] dar und sollten bereits bei der Planung von automatisierten Datenbearbeitungssystemen entsprechend berücksichtigt werden *(engl. privacy by design)*. Zu diesem Thema haben wir eine **Richtlinie** ausgearbeitet, die anhand von kurzen Beispielen in die Begrifflichkeiten Anonymisierung und Pseudonymisierung einführt und die wesentlichen Merkmale sowie Abgrenzungen im Detail erläutert.[80]

Seit Dezember 2011 ist Liechtenstein Mitglied des Schengenraums. Im Rahmen von Schengen werden die systematischen Personenkontrollen an den

75 Vgl. Tätigkeitsbericht 2009, 2.1.

76 Internetsicherheit, http://www.llv.li/amtsstellen/llv-dss-spezialthemen/llv-dss-spezialthemen-technisches/llv-dss-informationssicherheit-internetsicherheit.htm.

77 Einmal anonymisierte Daten können keinesfalls oder nur mit unverhältnismässig grossem Aufwand an Zeit, Kosten und Arbeitskraft wieder einer bestimmten oder bestimmbaren Person zugeordnet werden. Für die ordnungsgemässe Anonymisierung von Personendaten ist es nicht ausreichend, lediglich die direkten Identifikationsmerkmale zu entfernen.

78 Abhängig vom Einsatzzweck dürfen Pseudonyme auch nicht anwendungsübergreifend, sondern nur für jeweils ein Verfahren, einen Prozess oder einen bestimmten Dienst eingesetzt werden. Bereichsspezifische Identifier (PEID). Zur PEID vgl. auch Tätigkeitsbericht 2009, 1.2. und Tätigkeitsbericht 2008, 3.1. sowie Tätigkeitsbericht 2007, 5.1.2., mit dem Hinweis auf das Rechtsgutachten von Giovanni Biaggini, Professor für Staats- und Verwaltungsrecht an der Universität Zürich, „Ein Personenidentifikator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes (Art. 13 BV, Dezember 2002)", abzurufen unter: http://www.edoeb.admin.ch.

79 http://www.llv.li/amtsstellen/llv-dss-spezialthemen/llv-dss-spezialthemen-technisches/llv-dss-privacy_enhancing_technolgies.htm.

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

Binnengrenzen zwischen den Schengenstaaten aufgehoben, um den Reiseverkehr zu erleichtern. Gleichzeitig sollen durch eine stärkere grenzüberschreitende Polizeizusammenarbeit Ordnung und Sicherheit im Schengenraum gewährleistet werden. Im Kern des Abkommens von Schengen steht das Schengen Informationssystem SIS.[81] Im Anschluss an die Datenschutzevaluation haben wir ein **Merkblatt und Musterbriefe** zur Geltendmachung der Rechte veröffentlicht,[82] wie dies auch bei anderen Datenschutzbehörden der Fall ist.

Bekanntermassen wollte Google das Vorhaben **Google Street View** auch in Liechtenstein umsetzen.[83] Dies wurde jedoch (noch) nicht durchgeführt. Ein Grund dafür mag darin bestehen, dass in der Schweiz eine gerichtliche Lösung gesucht wurde. Im entsprechenden Entscheid bestätigt das **Schweizerische Bundesgericht**, dass Google die *Öffentlichkeit besser über bevorstehende Fahrten zu informieren hat*. Ausserdem sind die aufgenommenen Bilder besser zu *anonymisieren*. Im Nahbereich von *sensitiven Einrichtungen* wie Frauenhäusern, Gerichten, Gefängnissen, Kirchen usw. sind sogar nicht nur Gesichter unkenntlich zu machen; es ist auch dafür Sorge zu tragen, dass die *Kamerahöhe* bei den Aufnahmefahrzeugen gesenkt wird. Somit werden bedeutend weniger Einblicke in umfriedete Gärten möglich sein. Als Vertreter von Google mit uns Kontakt aufgenommen hatten, betonten sie die Nähe des liechtensteinischen DSG zum schweizerischen Bundesgesetz. Fragen ergäben sich nach diesem Argument ja kaum, da aufgrund der Lage in der Schweiz alles geklärt sei. Da damals schon Fahrten in der Schweiz durchgeführt worden waren, sollte dies auch in Liechtenstein möglich sein. Bei einer erneuten Kontaktaufnahme durch Google werden wir sie beim Wort nehmen und auf den Entscheid des Bundesgerichts hinweisen. Auf die **Revision der DSV**[84] im Zusammenhang mit den Bestimmungen zum Auslandsdatentransfer sowie auf die **Revision des DSG**[85] wurde jeweils mit Newsbeiträgen ausführlich hingewiesen. Zeitgleich mit dem Inkrafttreten der Abänderungen wurden die Informationen auf den diesbezüglichen Internetseiten[86] ebenfalls der neu geltenden Rechtslage angepasst.

Ergänzend zu den bereits auf der Internetseite veröffentlichten Informationen und Hilfsmitteln zum Selbstdatenschutz haben wir einen Hinweis auf den interaktiven Online-Dienst **Think Data**[87] aufgenommen. Dort werden beispielhafte Szenarien, die aus der Praxis stammen, beschrieben: Die Themen reichen von den Rechten als Angestellter über Geolokalisierung und Personaldossiers bis hin zur Veröffentlichung von Bildern im Internet. Der Dienst ist aus einer interdisziplinären Arbeitsgruppe in der Schweiz entstanden und bezieht sich auf die schweizerische Rechtslage. Dabei wiesen wir darauf hin, dass wir bei Fragen zur Rechtslage in Liechtenstein kontaktiert werden können.

Wir berichteten zudem über unsere Veranstaltung zum 6. Europäischen Datenschutztag unter dem Titel **„Was weiss das Internet über mich?" – Meine Daten als Handelsware!**

3. Mitarbeit bei der Gesetzgebung

Die Mitarbeit bei der Gesetzgebung ist eine weitere unserer Kernaufgaben. Dabei haben wir darauf zu achten, dass der Gesetzgeber die Privatsphäre der Bürger beim Erlass neuer Vorschriften respektiert. Es hat sich sehr bewährt, wenn wir in einem *möglichst frühen Verfahrensstadium* einbezogen werden. Insgesamt gaben wir zu 9 Gesetzesvorhaben in verschiedenen Stadien des Gesetzgebungsverfahrens eine Stellungnahme ab. Wir nahmen zu weniger Gesetzesvorhaben als in der Vergangenheit Stellung, da wir uns mehr auf praktische Fragen konzentrierten.

Exemplarisch soll im Folgenden aufgrund besonderer datenschutzrechtlicher Relevanz nur auf einzelne ausgesuchte Gesetzesvorhaben näher eingegangen werden:

81 Dabei handelt es sich um ein europaweites elektronisches Personen- und Sachfahndungssystem, das durch die Schengenstaaten gemeinsam betrieben wird. Der Umfang, ca. 35 Millionen gespeicherte Daten im SIS, weist auf die grosse Bedeutung des Datenschutzes im Zusammenhang mit „Schengen und Personendaten" hin.

82 http://www.llv.li/amtsstellen/llv-dss-internationale_beziehungen/llv-dss-schengen.htm

83 Vgl. Tätigkeitsbericht 2010, 1.2.

84 LGBl. 2012 Nr. 154 mit Anpassungen der Anhänge 1 und 2.

85 LGBl. 2012 Nr. 28. Vgl. auch unten, 6.

86 Vgl. insb. zum Auslandsdatentransfer: http://www.llv.li/amtsstellen/llv-dss-datentransfer_ins_ausland.htm; zum Register der Datensammlungen siehe http://www.llv.li/amtsstellen/llv-dss-register_datensammlungen.htm.

87 http://www.thinkdata.ch/de.

Obwohl wir nicht für die Ausschaffung von Rechtsgrundlagen zuständig sind, arbeiteten wir bei der Vorbereitung zu einer **Datenschutz-Zertifizierungsverordnung** sehr eng mit den Zuständigen zusammen. Wir sind nämlich der Ansicht, dass mit der Einführung eines solchen Gütesiegels der Datenschutz als ein Wettbewerbsvorteil etabliert werden kann. Zudem ist ein solches Siegel ein Zeichen der Öffentlichkeit gegenüber, dass der Datenschutz ernst genommen wird. Mit einem Inkrafttreten der Verordnung ist 2013 zu rechnen.

Im Europarat und in Brüssel wird derzeit der bestehende **Rechtsrahmen für den Datenschutz** überarbeitet.[88] Neben damit befassten Gremien, in denen wir Liechtenstein vertreten, hatten wir auch Gelegenheit, über die liechtensteinische Mission in Brüssel im Rahmen der Tätigkeiten der entsprechenden *Arbeitsgruppe des Europäischen Rates* Stellung zu nehmen. Dabei unterstützten wir das Vorhaben der Europäischen Kommission, eine *allgemeine Datenschutz-Verordnung* zu erlassen. Eine Verordnung ist direkt anwendbar. Dies hat unserer Ansicht nach den entscheidenden Vorteil, dass wir uns in Zukunft stark auf die Praxis z.B. in Österreich oder Deutschland stützen könnten. Gegenwärtig ist das nicht der Fall. Damit wären in Zukunft derart stark divergierende Ansichten der Datenschutzbehörden wie im Fall *Google Street View* nicht mehr möglich. Im Gegenteil sieht der Vorschlag der Verordnung eine verstärkte Zusammenarbeit der Datenschutzbehörden vor. Die Wahl einer Verordnung wurde auch von der Wirtschaft im Sinne der Rechtssicherheit begrüsst. Allerdings sollte unserer Ansicht nach die angestrebte Harmonisierung des Datenschutzes nicht zu absolut sein und einen gewissen *nationalen Spielraum* zulassen. So werden in Liechtenstein auch *juristische Personen* geschützt, was für sie ein zusätzlicher Schutz bedeutet und auch als ein gewisser Standortvorteil angesehen werden kann. Auch muss das ganze Vorhaben gewisse natürliche Begebenheiten berücksichtigen, wie z.B. kulturell oder strukturell bedingte Unterschiede. Liechtenstein als kleinstes EWR-Mitglied sollte schon andere Erwartungen erfüllen müssen als z.B. Deutschland. Eine Idee der Reform besteht ja darin, Bürokratie abzubauen bzw. gar zu vermeiden. Dies sollte auch für Liechtenstein gelten. Der Umstand, dass in Zukunft eine direkt anwendbare Verordnung gelten wird, sollte keinesfalls dazu führen, dass in Liechtenstein mehr *Bürokratie* entsteht. Im Gegenteil: Der Schutz der Bürger sollte verstärkt werden, was die Kommission zu einem Ziel erklärt hat. Neben der allgemeinen Datenschutzverordnung wird auch eine **Richtlinie im Bereich justizielle und polizeiliche Zusammenarbeit** vorgeschlagen. Diese stellt zwar im EU-Bereich einen Fortschritt gegenüber dem bisher gültigen Rahmenbeschluss zum Datenschutz in der Dritten Säule dar. Dies gilt jedoch nicht in Bezug auf Länder wie Liechtenstein, die bereits jetzt den Datenschutz in diesem Bereich berücksichtigen. In diesen Fällen stellt die Richtlinie einen *Rückschritt* dar, was vermieden werden sollte. Darauf wiesen wir ebenfalls hin. Das Polizeigesetz sieht verschiedene Datenschutzbestimmungen vor. Eine Schwächung des Status Quo ist jedenfalls zu vermeiden. Denn die Revision des Rechtsrahmens in Brüssel steht unter dem Motto „Stärkung des Datenschutzes in Europa".

Weiters haben wir zu folgenden Gesetzesprojekten eine Stellungnahme abgegeben:

- Forschungsförderungsgesetz
- Gesetz über die Umweltverträglichkeitsprüfung (UVPG)
- Gesetz über die Verwalter alternativer Investmentfonds (AIFMG)
- IMI-Verordnung (Internal Market Information System)
- Invalidenversicherungsgesetz
- Treuhändergesetz
- Zusammenführung von Aufgaben des Amtes für Soziale Dienste, des Ausländer- und Passamtes sowie der Stabsstelle für Chancengleichheit in ein Amt für Soziales und Gesellschaft sowie über die Schaffung des Psychosozialen Dienstes Liechtenstein sowie über die Schaffung des Liechtensteinischen Zentrums für Menschenrechte

4. Kontrollen

Ein Arzt hatte uns ein Schreiben übergeben, in dem die Freiwillige Krankenkasse Balzers (FKB) im Rahmen einer Kostengutsprache detaillierte Diagnoseangaben an einen anderen Arzt weitergeleitet hatte. Der Arzt, der sich an uns gewandt hatte, wollte nicht namentlich erwähnt werden. Deshalb konnten wir das Schreiben nicht an die FKB zur Stellungnahme weiterleiten. Aus diesem Grund entschieden wir uns dafür, die **Datenflüsse zwischen dem Vertrauens-**

88 Vgl. Tätigkeitsbericht 2011, 5.1. und 5.4. sowie unten, 5.1. und 5.5.

arzt und der Verwaltung der FKB zu untersuchen. Im Rahmen dieses eingeschränkten Kontrollumfangs konnten wir feststellen, dass die Bearbeitung von Personendaten durch die FKB im Zusammenhang mit dem vertrauensärztlichen Dienst in fast allen wesentlichen Bereichen datenschutzkonform erfolgt. In einigen wenigen Punkten konnte Verbesserungspotential herausgearbeitet werden. So hat die FKB beispielsweise aktiv und in angemessener Weise darauf hinzuweisen, dass sowohl Versicherte als auch Leistungserbringer die Möglichkeit haben, die medizinischen Daten *direkt an den Vertrauensarzt bekannt zu geben*.[89] In diesem Zusammenhang war auch das System der *sogenannten Hilfspersonen*[90] zu überprüfen: Der Vertrauensarzt ist zwar durch eine Krankenkasse angestellt, nimmt aber eine Filterfunktion zwischen den Leistungserbringern und der Verwaltung einer Krankenkasse wahr.[91] Nun kam es vor, dass Unterlagen zu Handen des Vertrauensarztes an die Verwaltung der FKB gesandt wurden. In diesen Fällen wurden die Unterlagen dort durch die erwähnten Hilfspersonen, stellvertretend für den Vertrauensarzt, eingesehen und in ein entsprechendes IT-System eingegeben. Es wurde der FKB empfohlen, das durch den vertrauensärztlichen Dienst implementierte System der Hilfspersonen genau zu überprüfen und bestehende mögliche Interessenskonflikte (die auf der Kleinheit des Unternehmens gründen) aufzulösen. Ausserdem war uns wichtig, dass die FKB auch darauf einwirkt, dass der **Vertrauensarzt** seine Filterfunktion effektiv ausübt: Demnach hat sich der Vertrauensarzt in seinen Stellungnahmen stets auf die absolut notwendigen Angaben zu beschränken. Unsere Empfehlungen werden in einem Follow-up zu einem späteren Zeitpunkt überprüft werden.

Die **Gemeinsame Kontrollinstanz Schengen (GKI)** initiierte die Durchführung einer gemeinsamen Kontrolle, wobei erstmalig *Artikel 95 des Schengener Durchführungsübereinkommens (SDÜ)* im Fokus einer Kontrolle stand.[92] Für Liechtenstein relevant war der Zeitraum vom 19. Juli 2011[93] bis zum 31. Dezember 2011, in welchem insgesamt dreizehn Ausschreibungen im SIS erfasst worden waren. 2012 fand bei der SIRENE[94] eine Vorortkontrolle der Abläufe statt. Exemplarisch wurden die *Abläufe um eine Ausschreibung* anhand eines aktuellen Falles nachvollzogen und auf die Vorgaben des SDÜ und des SIRENE-Handbuchs geprüft. Uns wurden auch die entsprechenden Applikationen zur Fahndungsausschreibung, SISone4ALL und die SIRENE-Applikation (SIRA), vorgeführt. Es konnte festgestellt werden, dass die Abläufe im SIRENE-Büro den Vorgaben gemäss SDÜ und des SIRENE-Handbuchs entsprechen, standardisiert und auch durch Trainings den Mitarbeitern kommuniziert sind. Es ist den Vorgesetzten sowie der Leitung möglich, die Einhaltung der geltenden Bestimmungen zu überwachen und nötigenfalls Änderungen zu bewirken. Die Abläufe werden auch, im Austausch mit anderen SIRENE-Büros in Europa, laufend verbessert. Im Zusammenhang mit der gegenständlichen Kontrolle gab es von unserer Seite keine Empfehlungen oder Bemerkungen. Dies meldeten wir der GKI für den Bericht über die harmonisierte Kontrolle.

5. Internationale Zusammenarbeit

5.1. Artikel-29-Datenschutzgruppe

Wie erwähnt stellte die Europäische Kommission Anfang des Jahres den Vorschlag für einen **neuen Rechtsrahmen im EWR** vor. Dies wurde nötig, da die bisher geltende Richtlinie 1995 verabschiedet wurde und somit aus einer Zeit stammt, als das Internet noch in den Kinderschuhen steckte. Die Richtlinie gilt als veraltet. Mit dem neuen Rechtsrahmen soll eine wirtschaftsfreundliche Lösung entstehen. Vorgeschlagen wurde die Form einer Verordnung, die in den Staaten direkt anwendbar ist. Mit dieser stärkeren Harmonisierung soll auch die Rechtssicherheit, u.a. für die Wirtschaft, verbessert werden. Der Datenschutz, der seit dem In-

89 Die FKB hat in diesem Zusammenhang auf deren Internetseite unter http://www.fkb.li/weitergabe-von-gesundheitsdaten-004-050212-de.htm einen entsprechenden Hinweis samt Verweis auf ein Musterschreiben veröffentlicht.

90 Der Vertrauensarzt benennt und autorisiert Hilfspersonen in der jeweiligen Krankenkasse und hat diesen gegenüber für die vertrauensärztlichen Aufgaben fachtechnisch ein Weisungsrecht. Die entsprechenden Personen üben parallel zwei unterschiedliche Funktionen aus: auf der einen Seite sind sie Mitarbeiter der Verwaltung der FKB, auf der anderen Seite sind sie Hilfspersonen für den Vertrauensarzt.

91 Vgl. Art. 20, 20a Krankenversicherungsgesetz (KVG).

92 Art. 95 SDÜ, Ausschreibungen von Personen, die von Justizbehörden zum Zwecke der Auslieferung gesucht werden: vgl. Tätigkeitsbericht 2011, 5.2.

93 Zeitpunkt der produktiven Inbetriebnahme des Schengener Informationssystems (SIS) in Liechtenstein.

94 Die **S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry (SIRENE)-Büros liefern Zusatzinformationen zu Ausschreibungen und koordinieren u.a. Massnahmen im Zusammenhang mit Ausschreibungen im Schengener Informationssystem (SIS).

krafttreten des Vertrages von Lissabon in der EU einen Grundrechtscharakter bekommen hat, soll insgesamt dementsprechend gestärkt werden: Die Rechte der Bürger und die Aufgaben der Datenschutzbehörden werden ausgebaut und die Pflichten der Dateninhaber verstärkt. So sollen die Datenschutzbehörden bei Verstössen Sanktionen bis zur Höhe von 2 % des Jahresumsatzes erteilen können. Die europäische Zusammenarbeit der Datenschutzbehörden wird intensiviert, die bisherige Artikel-29-Datenschutzgruppe durch ein European Data Protection Board (EDPB) abgelöst, das neu ein eigenes Sekretariat bekommen soll. Fälle von grenzüberschreitender Dimension werden im EDPB in einem Kohärenzverfahren behandelt. Entsprechend dem Grundsatz des „One-Stop-Shops" sollen Fälle wie Google Street View, wo es stark divergierende Ansätze gab, vermieden werden. Nationale Abweichungen von einer harmonisierten Praxis müssen „Brüssel" gegenüber begründet werden. Auch soll die Europäische Kommission als „Hüterin der Verträge" eine inhaltliche Rolle bekommen, die sie bisher nicht hat; alles in allem ein Quantensprung, auch für Liechtenstein. Die Artikel-29-Datenschutzgruppe erarbeitete eine eigene Stellungnahme zum Verordnungsentwurf.[95]

Eine weitere Stellungnahme wurde zu Entwicklungen im Bereich **biometrischer Technologien** erarbeitet.[96] Sie stellt eine Weiterentwicklung des bereits 2003 veröffentlichten Arbeitspapiers dar[97] und richtet sich insbesondere an gesetzgebende Institutionen auf europäischer und auf nationaler Ebene sowie an die entsprechende Industrie und an die Nutzer der entsprechenden Technologien. Technologische Innovationen werden häufig nur aus dem positiven Blickwinkel (Verbesserung des Erscheinungsbildes und der Bedienungsfreundlichkeit von Anwendungen) dargestellt. Sie können aber auch zu einem schrittweisen Verlust der Privatsphäre führen, wenn nicht gleichzeitig angemessene Schritte zu deren Erhalt unternommen werden. Daher werden in der genannten Stellungnahme insbesondere technische und organisatorische Gegenmassnahmen erläutert.

Zum Beispiel wurden bereits biometrische Technologien für die Identifizierung, Authentifizierung/Verifizierung oder Kategorisierung von natürlichen Personen in Online- und Mobilfunkdienste integriert. So bieten heute schon Online-Dienste Nutzern die Möglichkeit, Bilder hochzuladen, die sie mit dem jeweiligen Nutzerprofil verknüpfen können, wobei Systeme zur Gesichtserkennung zur Anwendung kommen können. Aufgrund dieser Entwicklungen hat die Artikel-29-Datenschutzgruppe eine spezifische **Stellungnahme zur Gesichtserkennung bei Online- und Mobilfunkdiensten**[98] veröffentlicht, worin sie den Rechtsrahmen prüft und angemessene Empfehlungen gibt, welche auf die Technologie zur Gesichtserkennung anzuwenden sind.[99] Sie richtet sich insbesondere an europäische und nationale Rechtsetzungsbehörden, an für die Datenbearbeitung Verantwortliche und an die Nutzer solcher Technologien. Als Beispiel für eine Gesichtserkennung in Online-Diensten wird *Facebook* aufgeführt. Das Online-Netzwerk startete bereits im Dezember 2010 mit „Markierungsvorschlägen für Fotos".[100] Dabei wurden die Fotos der Nutzer automatisch nach Gesichtern gescannt und in weiterer Folge versucht, die gefundenen Gesichter bekannten Facebook-Profilen zuzuordnen.

Eben diese **Gesichtserkennung** war Teil des **Audits** der irischen Datenschutzbehörde bei **Facebook**, wo in diesem Zusammenhang zusätzliche Schritte zur Einholung einer Einwilligung der Betroffenen

95 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

96 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_de.pdf. Biometrische Daten spielen u.a. eine wichtige Rolle bei Systemen zur Zugangskontrolle. Sie können helfen, das Sicherheitsniveau zu erhöhen, und sie können dazu beitragen, Identifikations- und Authentifikationsverfahren zu vereinfachen, zu beschleunigen und bequemer zu gestalten. Die neuen technologischen Entwicklungen haben allerdings auch neue Bedrohungen der Grundrechte mit sich gebracht. Die genetische Diskriminierung hat sich zu einem echten Problem entwickelt, und der Diebstahl von Identitäten ist nicht mehr nur eine theoretische Gefahr. Biometrische Daten sind direkt mit einer einzigen Person verknüpft; sie sind höchstpersönlich und in der Regel einzigartig und unveränderbar. Im Gegensatz zu einem Passwort können biometrische Daten daher nicht geändert oder zurückgerufen werden.

97 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_de.pdf.

98 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_de.pdf.

99 Beispielsweise muss der für die Datenbearbeitung Verantwortliche sicherstellen, dass eine gültige Einwilligung der betroffenen Personen bereits vor der Erfassung von Bildern vorliegt, und ausreichende Informationen bereitstellen. Auch müssen die für die Datenbearbeitung Verantwortlichen sicherstellen, dass digitale Bilder und Templates nur für den angegebenen Zweck genutzt werden, für den sie zur Verfügung gestellt wurden. Es sind geeignete Schritte zu unternehmen, um die Sicherheit der gespeicherten Daten sicherzustellen. Dazu kann die Verschlüsselung des Templates gehören. Ein unbefugter Zugang zu dem Template oder dem Speicherort sollte nicht möglich sein.

100 http://blog.facebook.com/blog.php?post=467145887130.

empfohlen wurden.[101] Facebook hat daraufhin diese Funktionalität in den EWR-Ländern und somit auch in Liechtenstein im September 2012 deaktiviert. Alle bis dahin gesammelten biometrischen Daten wurden zwischenzeitlich gelöscht. Aus dem Datenschutzaudit der irischen Datenschutzbehörde bei Facebook gingen weitere Empfehlungen hervor.[102] U.a. müssen die *Privatsphäreneinstellungen übersichtlicher gestaltet und die Datenschutzerklärung einfacher dargestellt* werden. Auch sind die gesammelten Daten nach Zweckerreichung unverzüglich zu löschen. Der Bericht der Nachkontrolle vom Juli 2012 zeigt, dass Facebook zahlreichen Empfehlungen nachgekommen ist. Doch sind nach wie vor Punkte offen. So werden z.B. Benutzerkonten bei Löschgesuchen nach Ablauf einer bestimmten Frist noch immer nicht ordnungsgemäss gelöscht, die Einführungsinformationen neuer Facebook-Nutzer ist nicht ausreichend und die Löschung der im Zusammenhang mit Social-Plugins gesammelten Daten wurde noch nicht entsprechend der Empfehlung umgesetzt.[103] Erwähnenswert ist auch, dass bei der Erstellung von Werbeanzeigen auf Facebook eine bestimmte Zielgruppe festgelegt werden kann. Bei dieser Festlegung sind auch freie Schlüsselwörter zulässig, die theoretisch sensitive Datenkategorien betreffen können, was unter Umständen einen Eingriff in die Privatsphäre der Betroffenen darstellen kann.[104] Jedenfalls sind die Auditberichte der irischen Datenschutzbehörde ein erster Schritt in Richtung mehr Datenschutz bei Facebook. Die weitere Entwicklung wird zu beobachten sein, um bei Bedarf frühzeitig zum Schutz der Privatsphäre der Nutzer regulierend eingreifen zu können.

5.2. Gemeinsame Kontrollinstanz Schengen (GKI Schengen)

Wie bereits erwähnt, führte die Kontrollinstanz erstmals eine europaweite Untersuchung zu **Art. 95 SDÜ**[105] durch. Als zuständige Datenschutzbehörde trugen wir unseren Teil zu dieser Untersuchung bei.

Ein definitiver Schlussbericht der GKI Schengen wird im Jahr 2013 erwartet. Ein weiteres wichtiges Thema bestand im Wechsel von SIS I+ zu **SIS II**. Dieser soll Anfang 2013 vonstattengehen. Änderungen betreffen vor allem die Beschreibung der Systeme[106] und eine Ausweitung der Datenkategorien für Ausschreibungen. Eine Protokollierung erfolgt zum Teil in anderen Systemen als bisher. In Anbetracht der Tatsache, dass es einen baldigen Systemwechsel gibt, hat keine Inspektion des SIS I+ stattgefunden.

5.3. Eurodac Supervision Coordination Group

Ein brennendes Thema der Gruppe ist der vorgesehene **Zugriff von Strafverfolgungsbehörden auf die Fingerabdrücke** im Eurodac-System. Im neuen Entwurf der Eurodac Verordnung[107] soll dieser zukünftig unter bestimmten, streng regulierten Voraussetzungen möglich sein, d.h. jedenfalls nur dann, wenn die Strafverfolgungsbehörden vorgängig die jeweiligen nationalen Datenbanken geprüft haben. Danach erfolgt eine weitere Überprüfung, die jedoch für die liechtensteinischen Strafverfolgungsbehörden derzeit nicht möglich ist. Weiters soll eine zusätzliche Hürde über die *Schwere der Straftat* geschaffen werden. Es soll jedenfalls keine systematische Überprüfung geben. Auch ist kein Abgleich bei „minderschweren" Straftaten vorgesehen.

Ein anderes Thema besteht in der **Qualität von Fingerabdrücken**, insbesondere von **nicht lesbaren Fingerabdrücken**. Hier bestehen Probleme bei der Verwendung solcher Fingerabdrücke im Asylverfahren. Nach Ansicht der Gruppe sollte ein Asylverfahren die Nichtverwendbarkeit von Fingerabdrücken jedenfalls berücksichtigen, was bisher nicht durchwegs der Fall ist.

5.4. Europarat

Der Vorschlag der Europäischen Kommission zu einem neuen Rechtsrahmen des Datenschutzes hatte einen Einfluss auf die Arbeit des Konventionsausschusses des Europarates zur **Revision des Datenschutzabkommens**,[108] da ja die 30 EWR-Mit-

101 http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf, S. 8f.
102 Siehe Tätigkeitsbericht 2011, 1.2.
103 Report of Re-Audit, 21. September 2012, http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf.
104 Im November 2012 ergab die Reichweitenmessung einer fiktiven Werbeanzeige mit der Einschränkung auf Liechtenstein und dem präzisen Interesse für #Gay eine Zielgruppe von 80 Personen.
105 Vgl. oben, 4.
106 In Liechtenstein gibt es keine nationale Kopie des SIS mehr. Es wird ein direkter Zugriff auf SIS II eingerichtet.
107 Die neue Verordnung soll jene vom 11. Oktober 2010 ersetzen.
108 Vgl. Tätigkeitsbericht 2011, 5.4.

glieder auch Mitglied des Europarates sind. Mit anderen Worten waren nun zwei Revisionsvorschläge bekannt, die einander beeinflussen. Wie schon im letzten Tätigkeitsbericht beschrieben ist für uns die Revision in Brüssel wichtiger; nicht zuletzt weil es mit der ESA hier eine Überwachungsbehörde gibt. Der Konventionsausschuss schloss die Arbeit am Entwurf eines neuen Abkommens ab.

5.5. Europäische Datenschutzkonferenz

Zum ersten Mal seit einigen Jahren nahmen wir wieder an der Europäischen Datenschutzkonferenz teil, die in Luxemburg stattfand. Thema war der **neu vorgesehene Rechtsrahmen für Europa**; somit primär der Vorschlag der Europäischen Kommission einer *Verordnung zum Datenschutz* und einer *Richtlinie zum Datenschutz im Bereich Polizei und Justiz*. Während der Vorschlag einer Verordnung allgemein als Fortschritt begrüsst wird, sieht dies beim Richtlinienentwurf anders aus. Dieser gewährleistet nicht annähernd dasselbe Schutzniveau, was auf EU-interne Umstände zurückzuführen ist. Der derzeitige Richtlinienvorschlag würde gegenüber dem geltenden Recht in Liechtenstein einen Rückschritt bedeuten. Dies gilt es auf alle Fälle zu vermeiden, ist doch Ziel und Zweck der beiden Vorschläge eine Stärkung des Datenschutzes, der seit dem Inkrafttreten des Vertrags von Lissabon zu einem Grundrecht aufgewertet wurde. Im Rahmen der Verordnung ist grundsätzlich eine Stärkung der Rechte der Bürger, eine stärkere Verpflichtung der Dateninhaber und eine Stärkung der Datenschutzbehörden vorgesehen, die neu auch Sanktionen erteilen können sollen. Zudem wurde der Entwurf einer überarbeiteten *Datenschutzkonvention des Europarates* vorgestellt.[109]

Mit dem Wegfall der Drei-Säulen-Struktur durch den Vertrag von Lissabon ändert sich auch die Grundlage der **Working Party on Police and Justice** (WPPJ). Während unter der alten allgemeinen Datenschutzrichtlinie die Artikel-29-Datenschutzgruppe im Polizei- und Justizbereich nicht zuständig war, ändert sich dies unter dem neuen Rechtsrahmen. Deshalb wurde entschieden, eine Untergruppe „Border, Travel & Law Enforcement" (BTLE) zu bilden, welche die Aufgaben der WPPJ übernehmen sollte. An der Frühjahrskonferenz in Luxemburg wurde demgemäss entschieden, diese Arbeitsgruppe aufzuheben. Da in der WPPJ auch Nicht-EWR-Staaten vertreten waren, sollte der Konventionsausschuss des Europarates auch beigezogen werden.

Im Rahmen der europäischen Konferenz wird mindestens einmal im Jahr ein so genannter **Case Handling Workshop** abgehalten. Bei diesen Workshops werden aktuelle Themen und konkrete Fälle behandelt, welche für die europäischen Datenschutzbehörden wichtig sind. Nachdem wir im letzten Jahr auf eine Teilnahme verzichtet hatten, nahmen wir wieder teil. Einer der Schwerpunkte war die Durchführung von Datenschutzkontrollen.[110] Mit dem Beitritt zu „Schengen" erhielten wir ja die Aufgabe, Kontrollen durchzuführen. Die Teilnahme am Workshop ermöglichte uns einen wertvollen Input für die Durchführung unserer eigenen Kontrollen.

5.6. Internationale Datenschutzkonferenz

Die **International Working Group on Data Protection in Telecommunications (IWGDPT)** ist der Internationalen Datenschutzkonferenz unterstellt. Die Gruppe erarbeitete ein Papier zu *„Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes"*.[111] In diesem Arbeitspapier wird insbesondere die Verarbeitung personenbezogener Daten im Cloud Computing Umfeld untersucht und ausführlich dargestellt. In Abgrenzung zur Stellungnahme der Artikel-29-Datenschutzgruppe zu Cloud Computing[112] behandelt es die Nutzung von Cloud-Diensten durch Unternehmen und Behörden, die bereits bestehende Verfahren „in die Cloud" verlagern. Die Nutzung von Cloud-Diensten durch Privatpersonen ist nicht Inhalt des Arbeitspapiers. Es gibt konkrete Empfehlungen, lässt den Rechtsrahmen jedoch unberücksichtigt.[113]

109 Vgl. dazu 3. und 5.1.

110 Vgl. Tätigkeitsbericht 2010, 4.5.

111 http://www.datenschutz-berlin.de/attachments/882/675.44.10.pdf.

112 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf.

113 Allgemeine Empfehlungen: (1) Datenschutzstandards dürfen durch Cloud Computing (CC) im Vergleich zur herkömmlichen Datenverarbeitung nicht abgesenkt werden; (2) Vor dem Einstieg in CC-Projekte ist von den für die Verarbeitung Verantwortlichen eine Abschätzung der Folgen für den Datenschutz und eine Risikoabschätzung vorzunehmen (ggf. mithilfe vertrauenswürdiger Dritter); (3) Die Anbieter von Cloud-Diensten haben ihre Verfahren weiterzuentwickeln, um mehr Transparenz, Sicherheit, Nachprüfbarkeit und Vertrauen in CC-Lösungen zu schaffen; (4) Es sind weitere Bemühungen in der Forschung, der Zertifizierung durch Dritte, der Standardisierung, von „Privacy by Design"-

6. In eigener Sache

Wie bereits erwähnt,[114] wurde zur Umsetzung des Rahmenbeschlusses zum Datenschutz in der Dritten Säule das **DSG** erneut revidiert. Diese **Revision** trat am 1. Oktober 2012 in Kraft.[115] Hauptgegenstand war die *Aufhebung des Vorbehaltes für hängige Straf- und Rechtshilfeverfahren*.[116] Neben dieser Vorgabe zur Umsetzung des Rahmenbeschlusses wurden weitere Punkte gesetzlich geregelt. So wurde auf Druck der ESA die allgemeine Pflicht, *Datensammlungen* bei uns anzumelden oder einen *Datenschutzverantwortlichen* zu benennen, auch für Unternehmen eingeführt.[117] Trotz dieser Pflicht gingen bei uns weniger Anmeldungen als erwartet ein. Dies obwohl wir in der Presse auf diese neue Pflicht hingewiesen hatten. Es kann somit festgehalten werden, dass dieser gesetzlichen Pflicht, teils auch von namhaften Unternehmen, nur teilweise nachgekommen wird. Ausserdem wurde die allgemeine *vorgängige Informationspflicht* für Dateninhaber erweitert und den Bestimmungen der allgemeinen Datenschutzrichtlinie angepasst. Solche Informationspflichten sind vor allem in Allgemeinen Geschäftsbedingungen (AGBs) enthalten. Somit sind AGBs in der Praxis darauf hin zu prüfen, ob sie noch den gesetzlichen Normen entsprechen. Mit dieser Revision wurde der **Anwendungsbereich des DSG** zum wiederholten Male **ausgeweitet**. Schon früher war das DSG ja auf den *Sorgfaltspflichtbereich* ausgedehnt worden.[118] Zudem fallen die *öffentlichen Register des Privatrechtsverkehrs* seit 2009 unter das DSG.[119] Wie erwähnt wurde inzwischen auch ein *Gesetz über das Zentrale Personenregister* geschaffen, das ebenfalls, vor allem in den Materialien, Aufgaben an das Amt für Informatik enthält.[120] Datenschutz ist ja bekanntlich eine **Querschnittsmaterie**. Die allgemeine Richtlinie ist für den privaten und den öffentlichen Bereich anwendbar. Das DSG somit auch. Dies führt dazu, dass immer wieder neue datenschutzrechtliche Bestimmungen geschaffen werden. Die Bedeutung solcher Bestimmungen und der wiederholten Ausweitung des Anwendungsbereichs des DSG stellt für uns eine grosse Herausforderung dar.

7. Ausblick

Wir haben schon darauf hingewiesen, dass es in der Praxis ab und an vorkommt, dass dem Datenschutz der „schwarze Peter" zu Unrecht zugeschoben wird.[121] Für uns ist es unerlässlich, dass der Datenschutz in dem Licht gesehen wird, das ihm zukommt: es geht um einen wichtigen Aspekt des Schutzes der Privatsphäre und damit um ein Grundrecht jedes einzelnen Bürgers.

Deshalb setzen wir auf die künftige Zertifizierungsverordnung, mit der es künftig Unternehmen wie auch Behörden möglich sein wird, ein **Datenschutzgütesiegel** zu erhalten. Datenschutz kann und soll einen Wettbewerbsvorteil bedeuten. Die entsprechende Verordnung soll bald in Kraft treten.

Wie schon verschiedentlich erwähnt, ist es in einem kleinen Land mit beschränkten Ressourcen unerlässlich, **Synergien** zu schaffen. Dies gilt für die mannigfaltigen Aspekte, in denen die Privatsphäre betroffen ist (wie Fragen zum Internet). Hier sind verschiedene Stellen gefordert. Auch zeigt unsere Erfahrung, dass es Verbesserungspotential gibt, was verschiedene *Datenflüsse* angeht. Doppelspurigkeiten verhindern ab und zu einen geregelten und gesicherten Datenaustausch. Dies sollte gerade in Zeiten eines angespannten Staatshaushaltes vermieden werden.

Seit 2009 besteht der gesetzliche Vorbehalt zur Anwendung des Datenschutzes im Bereich des **Sorgfaltspflichtgesetzes** nicht mehr. Dennoch haben wir bisher auffällig wenige Anfragen in diesem Bereich bekommen. Auch im Register der Datensammlungen sind kaum Anmeldungen eingegangen. Der Staatsgerichtshof hat sich in StGH 2011/011 zum Verhältnis zwischen dem DSG und Spezialgesetzen geäussert.[122] Wir werden uns mit der Frage auseinandersetzen, was die Aufhebung dieses Vorbehaltes einerseits und das Urteil andererseits bedeutet.

Technologien und in anderen damit verbundenen Bereichen zu unternehmen, um das gewünschte Vertrauen in CC zu erreichen. Im Zusammenhang mit bewährten Verfahren („best practices") wird empfohlen, CC in sorgfältigen, massvollen Schritten umzusetzen, beginnend mit nicht-sensiblen und -vertraulichen Daten.

114 Tätigkeitsbericht 2011, 3.

115 Gesetz vom 11. Dezember 2011 über die Abänderung des Datenschutzgesetzes (LGBl. 2012 Nr. 28).

116 Früher: Art. 2 Abs. 2 Bst. c DSG.

117 Art. 15 DSG.

118 Vgl. oben, 1.6.

119 LGBl. 2009 Nr. 46.

120 Vgl. oben, 1.8.

121 http://www.llv.li/pdf-llv-dss-pressemitteilung_tb2011.pdf und oben, 1.7.

122 http://www.gerichtsentscheidungen.li/default.aspx?mode=suche&txt=DSG&gericht=2&id=3214&backurl=?mode=suche%26txt=DSG%26gericht=2.

Der Anwendungsbereich des DSG ist enorm, vor allem wenn man die zahlreichen spezialgesetzlichen Regelungen mitberücksichtigt. Betroffen sind ja nicht nur Behörden, sondern auch Unternehmen; alle fallen unter das DSG. Vor diesem Hintergrund müssen Prioritäten festgelegt werden. Wir haben uns gegenwartsnah für die Bereiche *Gesundheit*, *Soziales*, *Finanzen und Datensicherheit* entschieden.

In einzelnen Fällen hatten wir auch Anfragen zur **Sicherheit von Internetseiten** bekommen (die im Bericht jedoch nicht erwähnt werden, da es um konkrete Einzelfälle ging). Dabei konnten wir feststellen, dass die Datensicherheit zu wenig berücksichtigt wurde. Im Rahmen unserer Möglichkeiten werden wir dieses Thema angehen.

Bei der derzeit laufenden **Revision des Datenschutzes in Europa** sind noch keine grundlegenden Entscheidungen zum Vorschlag der Kommission gefallen. Weder das Europäische Parlament[123] noch der Ministerrat haben eine offizielle Stellungnahme abgegeben. Dennoch wirft die Revision bereits ihre Schatten voraus. Eine bahnbrechende Änderung besteht im Vorschlag, dass Unternehmen bei einer *Datenschutzverletzung bis 2 % des Jahresumsatzes als Busse* zahlen müssen.[124] Auch wenn diese Regelung möglicherweise abgeschwächt wird: die Revision steht unter dem Motto „Stärkung des Datenschutzes". Es wird sich also einiges ändern. Die Regelungen werden verschärft. Es ist zu empfehlen, sich frühzeitig mit den Änderungen auseinanderzusetzen. Wir werden hierzu unseren Beitrag leisten.

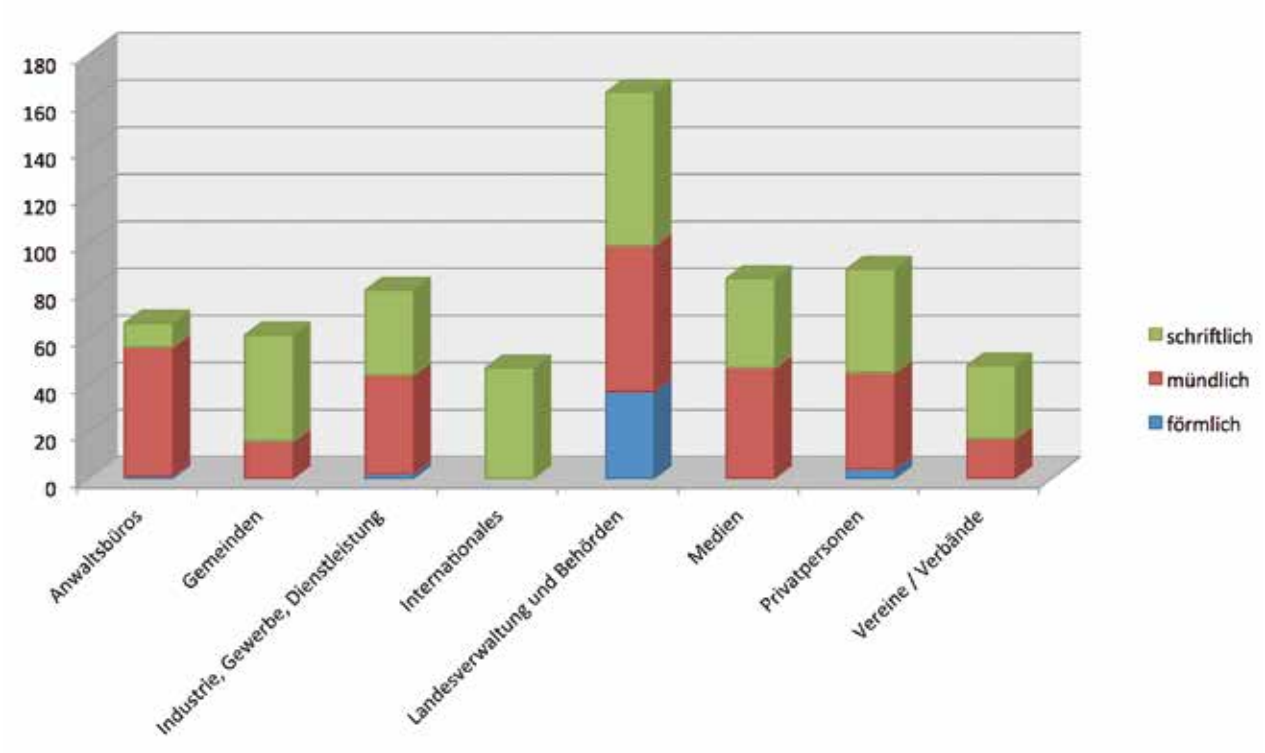
123 Dem Europäischen Parlament liegen 3'133 Änderungsanträge vor! http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/alles-wichtige-zur-datenschutzreform.html.

124 Art. 79 des Vorschlages zu einer Verordnung.

8. Anhang 1

8.1. Statistik: Beratung privater Personen und Behörden

Die Beratung privater Personen und Behörden ist eine Kernaufgabe. Im Berichtsjahr gingen insgesamt 640 Anfragen ein, so viele Anfragen wie nie zuvor. Gegenüber dem Vorjahr bedeutet das eine Zunahme um 81 Anfragen. Wie die nachfolgende Übersicht zeigt, stammen die meisten Anfragen nach wie vor von der Landesverwaltung.

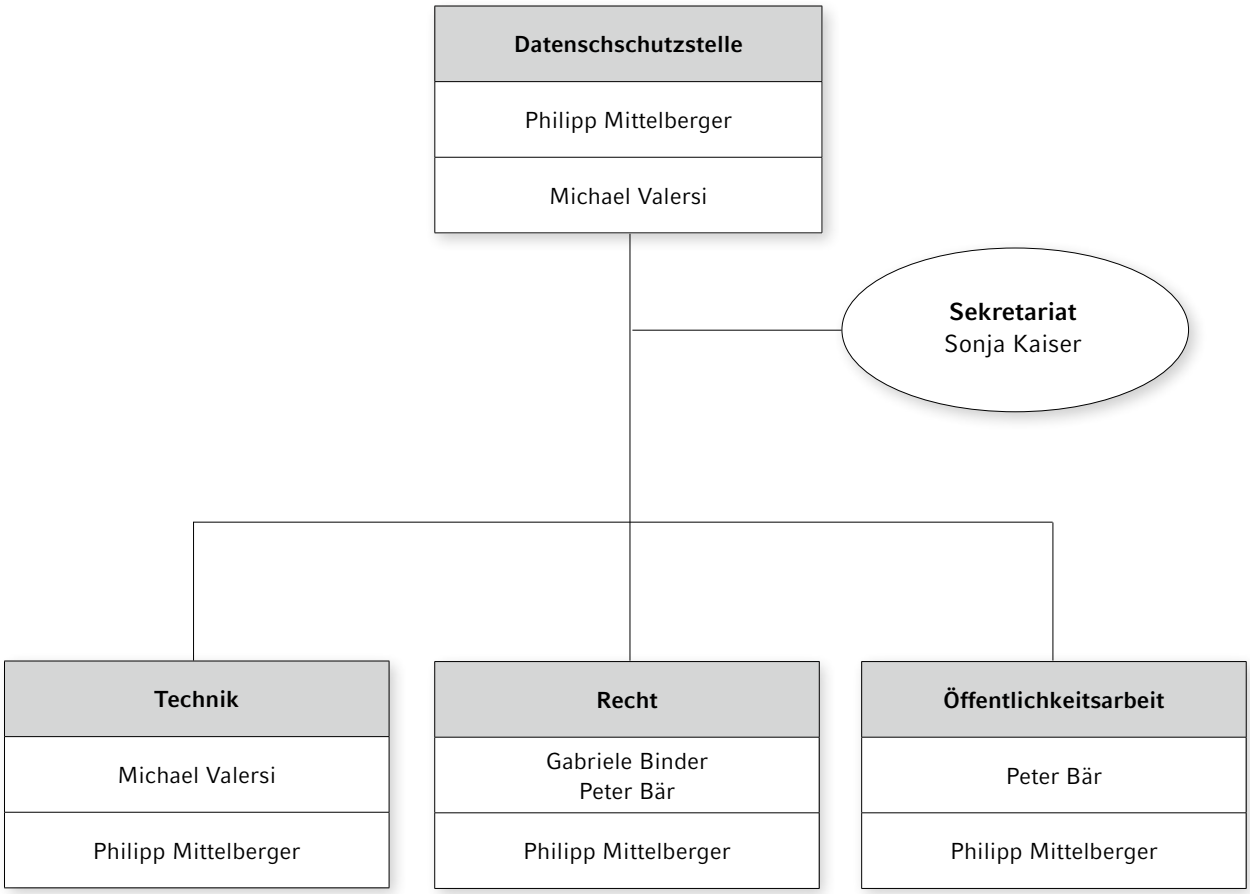


Gesetzesthemen

Aufgegliedert nach Sachgebieten standen allgemeine Datenschutzthemen, gefolgt von Anfragen zur Datenbekanntgabe im Inland, im Vordergrund. Vertikal sind die Themen und Sachgebiete aufgeführt, auf horizontaler Ebene, wer angefragt hat.

	Anwaltsbüros	Gemeinden	Industrie, Gewerbe, Dienstleistungen	Internationales	Landesverwaltung und Behörden	Medien	Private Personen	Vereine / Verbände
Datenschutz allgemein	14	8	16	35	55	63	25	36
andere Gesetzesvorhaben				2	9			
Arbeitsbereich	2		2		6		3	
Datenbekanntgabe Inland	5	51	9		27		6	3
Datenbekanntgabe Auslandsbezug	17		14	6	6	1	4	1
Geltenmachung gesetzlicher Rechte	5	1		1	8		25	4
Gesundheit / Soziales			3		4			1
Keine Zuständigkeit DSS			1		1		6	1
Polizei / Sicherheit					5	1	3	
Register der Datensammlungen	14		21		10			1
Schengen / Dublin					1			
Technologischer Datenschutz		1	4		8	20	9	1
Telekommunikation	3		1		1		1	
Umsetzung / Anwendung europäischen Rechts				3				
Vernehmlassung ohne Stellungsnahme					22			
Videoüberwachung			6		1		7	
Wirtschaft / Finanzen Gewerbe / Versicherungen	6		3					
Gesamtergebnis	**66**	**61**	**80**	**47**	**164**	**85**	**89**	**48**

Organigramm



Stand: 31. Dezember 2012

9. Anhang 2

9.1. Resultate der Sensibilisierungsumfrage zum Thema Datenschutz

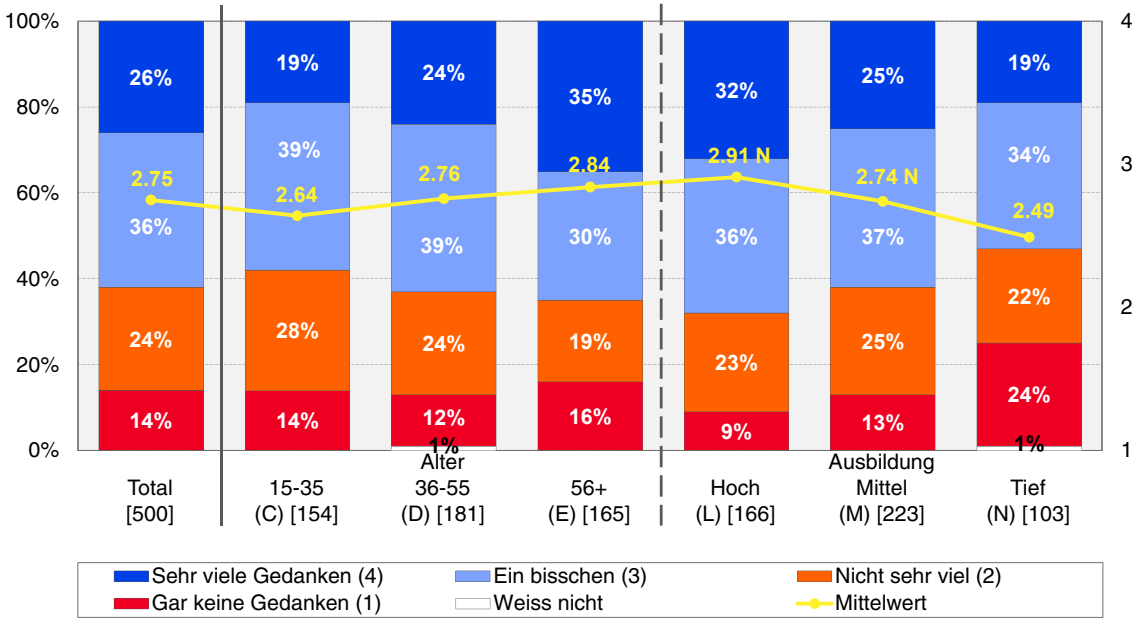
Präsentation anlässlich der Medienorientierung vom 20. August 2012

Projektinformationen

- Projektname: Sensibilisierungsumfrage zum Thema Datenschutz
- Auftraggeber: Datenschutzstelle Fürstentum Liechtenstein
  Dr. Philipp Mittelberger
- Methode: Telefonische Interviews (CATI)
- Stichprobe: N = 500 Interviews
  Repräsentative Bevölkerungsstichprobe, Zufallsauswahl
  ab Einwohnerregister
- Universum: Sprachassimilierte Wohnbevölkerung ab 15 Jahren, die über einen eingetragenen Festnetzanschluss erreichbar ist
- Befragungszeitraum: 19. April bis 21. Mai 2012
- Durchführung: LINK Institut für Markt- und Sozialforschung, Luzern

Wie sehr macht sich die Bevölkerung Gedanken über den Schutz persönlicher Daten?

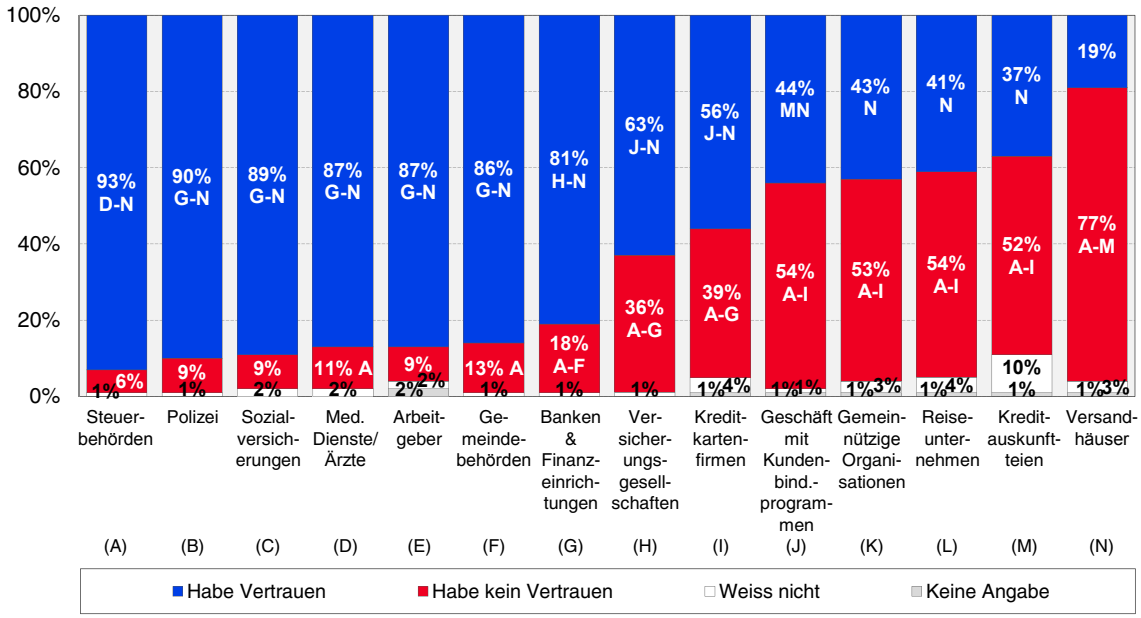
Zwei Drittel der Bevölkerung macht sich "ein bisschen" oder "sehr viele Gedanken".



Statistisch signifikante Abweichung(en) (T-Test)
Basis: [ ] befragte Personen

Wie gross ist das Vertrauen in Institutionen, wenn es um persönliche Daten geht?

Öffentliche Institutionen geniessen sehr grosses Vertrauen.

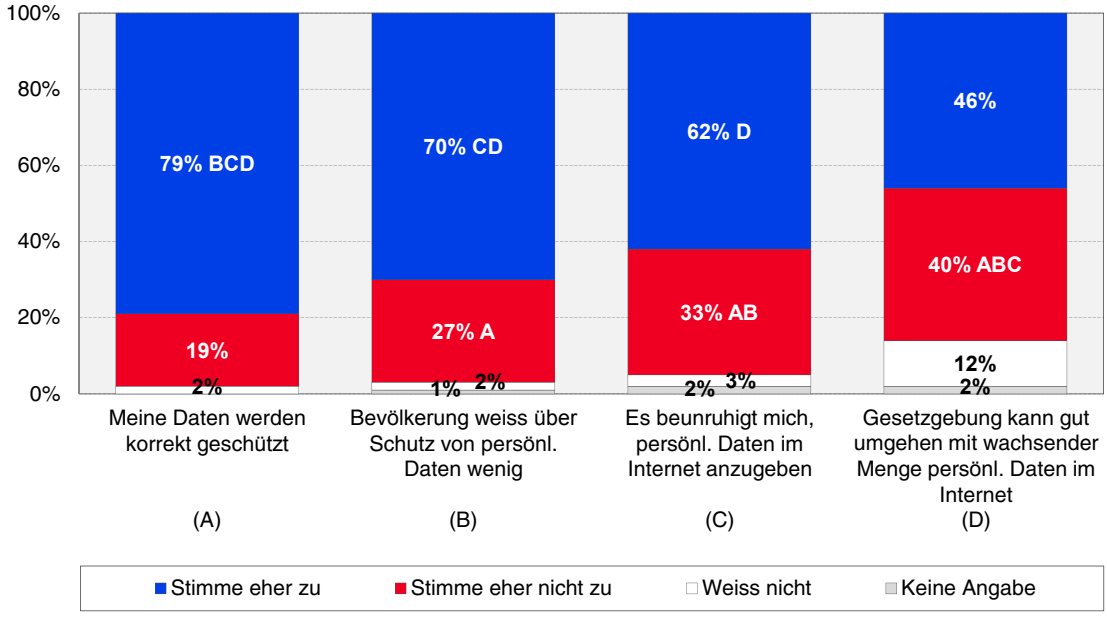


Statistisch Signifikante Abweichung(en) (T-Test)
Basis: 500 befragte Personen

LINK Institut

Was denkt die Bevölkerung über Datenschutz?

Das Vertrauen in die Gesetzgebung ist hoch, das Wissen darüber jedoch gering.

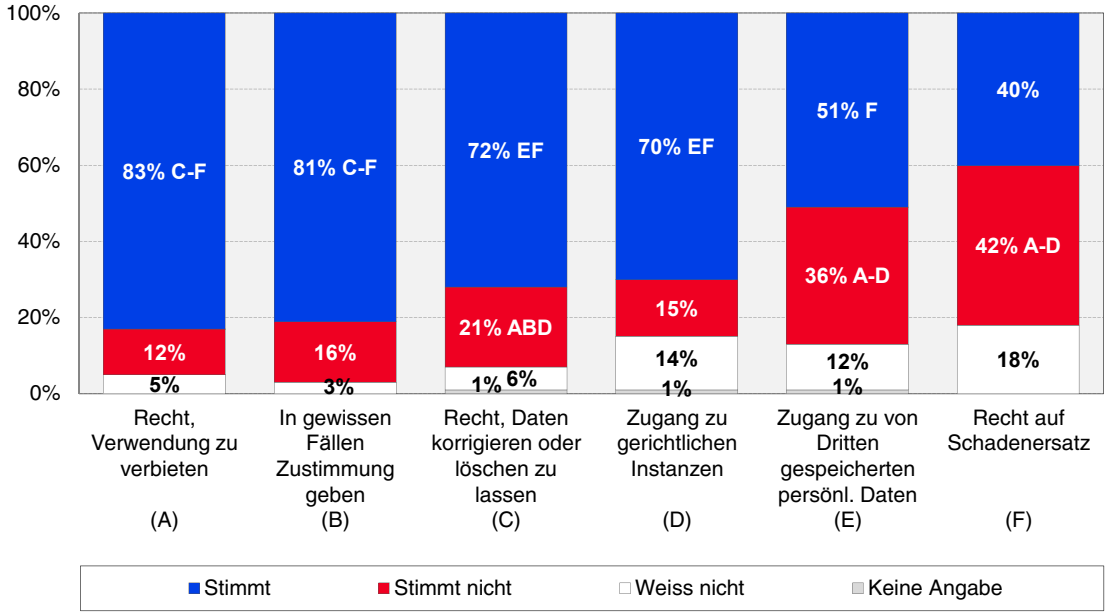


Statistisch Signifikante Abweichung(en) (T-Test)
Basis: 500 befragte Personen

LINK Institut

Was weiss die Bevölkerung über ihre Rechte zu persönlichen Daten?

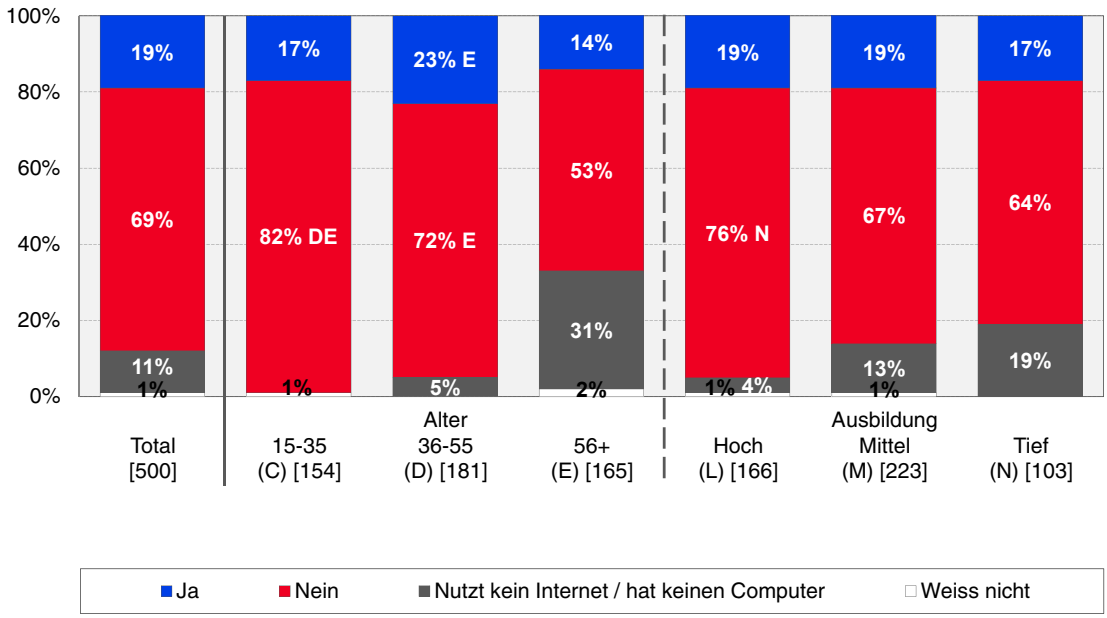
Es besteht Unsicherheit über die Rechte des Einzelnen.



Statistisch Signifikante Abweichung(en) (T-Test)
Basis: 500 befragte Personen

Ist die Übermittlung persönlicher Daten im Internet sicher?

Die Mehrheit betrachtet die Übermittlung persönlicher Daten im Internet als nicht sicher.

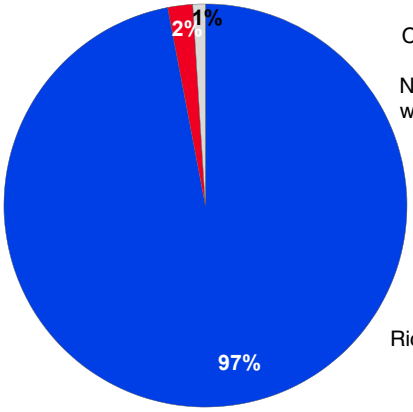


Statistisch Signifikante Abweichung(en) (T-Test)
Basis: [ ] befragte Personen

Schützen die Internetnutzer ihre persönlichen Daten?

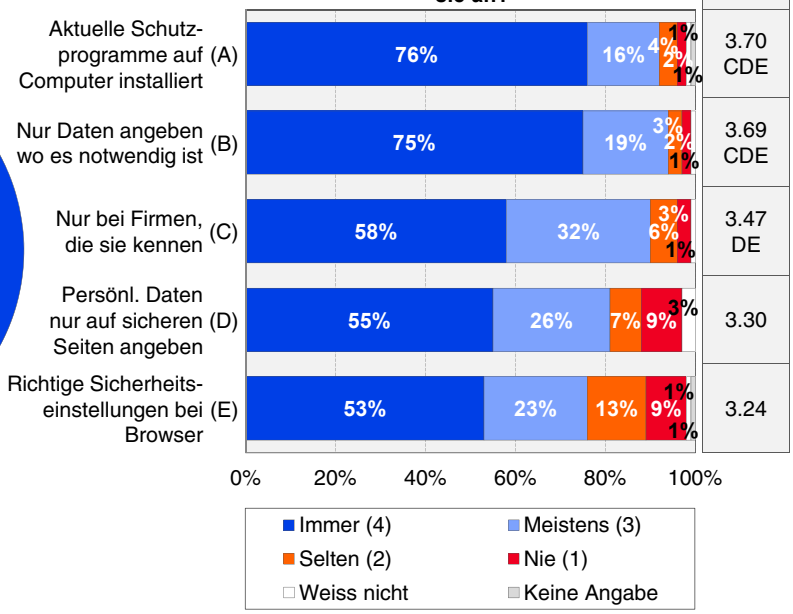
Die meisten Internetnutzer achten auf den Schutz ihrer Daten im Internet.

Achten die Internetnutzer auf Datenschutz im Internet?



- Ja
- Nein
- Weiss nicht
- Keine Angabe

Welche Schutzmassnahmen wenden sie an?



- Immer (4)
- Meistens (3)
- Selten (2)
- Nie (1)
- Weiss nicht
- Keine Angabe

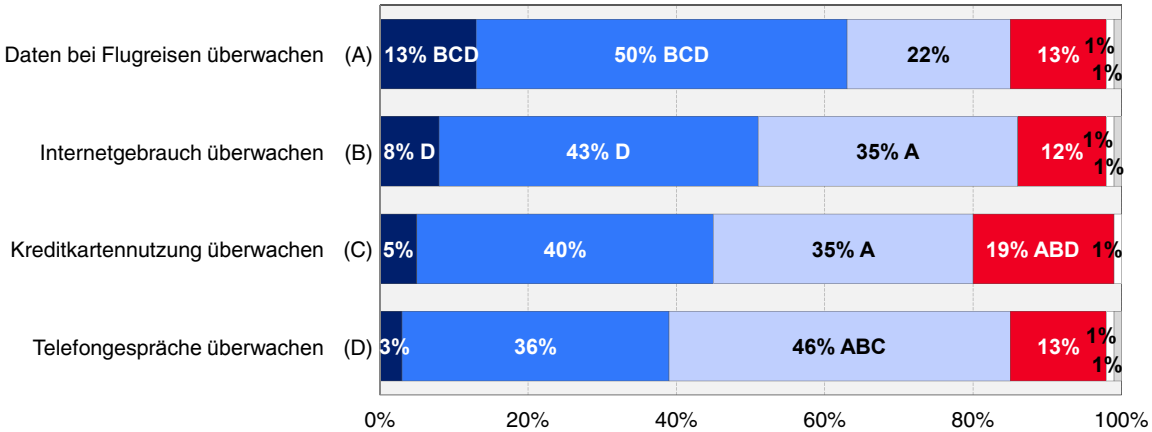
Basis: 441 befragte Personen, die das Internet nutzen (F74.00)

Statistisch signifikante Abweichung(en) (T-Test)
Basis: 426 befragte Personen, die das Internet nutzen und darauf achten, welche Daten sie wo angeben (F75.00)

LINK Institut

Wie viel Überwachung soll erlaubt sein?

Die Mehrheit der Bevölkerung befürwortet Überwachung, wenn Verdacht auf kriminelle Handlungen besteht.



- Ja, in jedem Fall
- Ja, bei Personen, bei denen Verdacht auf kriminelle Handlungen/terroristische Aktivitäten besteht
- Ja, aber auch verdächtigte Personen sollen nur unter Aufsicht überwacht werden dürfen
- Nein, in keinen Fall
- Weiss nicht
- Keine Angabe

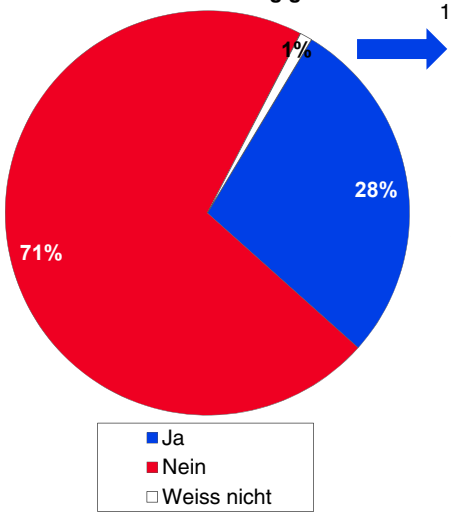
Statistisch Signifikante Abweichung(en) (T-Test)
Basis: 500 befragte Personen

LINK Institut

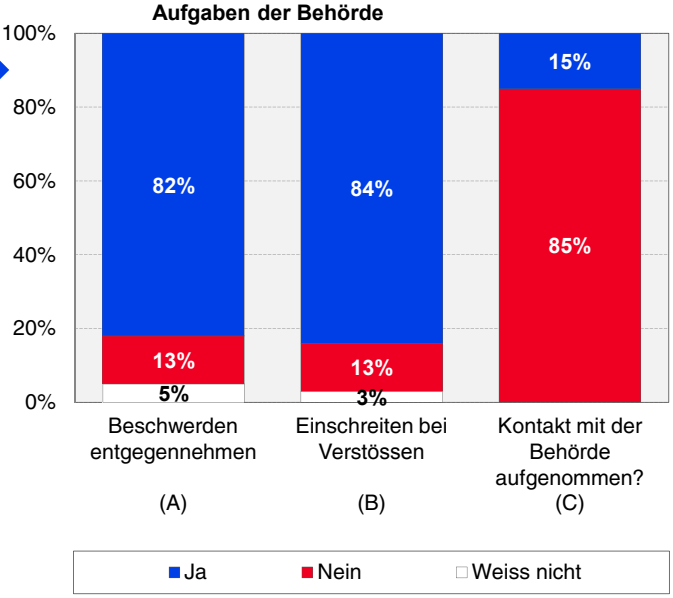
Ist eine unabhängige Behörde und deren Aufgaben bekannt?

28% der Bevölkerung wissen, dass es eine Datenschutzbehörde gibt.

Bekanntheit einer unabhängigen Behörde



Aufgaben der Behörde



Basis: 500 befragte Personen

Basis: 142 befragte Personen, die von der Behörde gehört haben (F41/42/43.00)

Fazit

- Die Mehrheit der Bevölkerung macht sich zwar Gedanken zum Schutz ihrer persönlichen Daten, das Wissen um ihre Rechte und Möglichkeiten zum Schutz der Daten ist jedoch gering.
- Öffentliche Institutionen, medizinische Dienste, Arbeitgeber und Finanzdienstleister geniessen sehr grosses Vertrauen.
- Das Wissen über die Gesetzgebung ist relativ gering, trotzdem ist das Vertrauen gross, dass die Gesetze persönliche Daten genügend schützen.
- Das Internet wird als nicht sicher betrachtet. Die meisten Internetnutzer haben jedoch das Gefühl, dass sie auf Sicherheit im Internet achten.
- Bei Verdacht auf kriminelle Handlungen befürwortet die Mehrheit der Bevölkerung die Überwachung persönlicher Daten.
- Vielen ist nicht bekannt, dass es eine unabhängige Datenschutzbehörde gibt.

DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Kirchstrasse 8
FL-9490 Vaduz

Tel. +423 236 60 90
Fax +423 236 60 99

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

12