DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Tätigkeitsbericht 2009

Datenschutzstelle des Fürstentums Liechtenstein

INHALTSVERZEICHNIS

I. VORWORT

Die Datenschutzstelle (DSS) wurde im Jahre 2009 dem Landtag zugeordnet. Neu ist auch, dass nach Art. 31 Abs. 1 des Datenschutzgesetzes (DSG) die DSS dem Landtag und der Regierung jährlich einen Tätigkeitsbericht erstattet, in dem sie über den Umfang und die Schwerpunkte ihrer Tätigkeit sowie über Feststellungen und Empfehlungen und deren Umsetzung informiert. Der Bericht wird veröffentlicht.

Dies ist unser 8. Tätigkeitsbericht.
Wir konnten wieder zahlreiche Anfragen von anderen Behörden, Unternehmen und Bürgern beantworten – ein neuer Rekord an eingegangenen Fragen. Einige davon werden im Bericht ausführlich dargestellt, da sie aus unserer Sicht für die Öffentlichkeit von Interesse sind. Daneben war unsere Arbeit von folgenden Schwerpunkten gekennzeichnet:

- Aus Anlass des *Europäischen Datenschutztages* am 28. Januar haben wir erstmals, gemeinsam mit der Hochschule, eine öffentliche Veranstaltung organisiert. Thema waren die „Sozialen Netzwerke".
- Mitte des Jahres trat eine weitere Revision des DSG in Kraft. Die wesentliche Neuerung besteht darin, dass wir eine Bewilligung für *Videoüberwachungsanlagen* im öffentlichen Raum zu erteilen haben. Dies ist eine Folge der Entscheidung der Datenschutzkommission (DSK) im Fall der Videoüberwachung der Fussgängerzone Vaduz, was durchaus zu begrüssen ist. Wir haben bereits im Tätigkeitsbericht 2007 darüber ausführlich berichtet. Verschiedene Fragen, die das Gesetz offen liess, waren intern zu klären, wie die Regelung des Bewilligungsverfahrens und die Ausarbeitung eines entsprechenden Instrumentariums für die Antragsstellung.
- Die Vorbereitungsarbeiten für einen künftigen Beitritt zu „*Schengen*" und „*Dublin*" beschäftigten uns auch vergangenes Jahr intensiv. „Schengen" ermöglicht liechtensteinischen Behörden Zugang zu Tausenden von Datensätzen, die im Schengen Informationssystem (SIS) gespeichert sind. Eine wichtige Voraussetzung für den Zugriff auf diese Daten besteht darin, dass die Daten entsprechend geschützt werden. Aus diesem Grund wird im Vorfeld eines Beitrittes eine sogenannte Datenschutzevaluation durchgeführt. Nur wenn diese Evaluation bestanden wird, und ein Beitrittskandidat den Schengen-Standard im Bezug auf den Datenschutz erfüllt, finden weitere Evaluationen im Polizeibereich statt. Anfang November wurde zum Thema Datenschutz eine Probe-Evaluation durchgeführt, die erfolgreich abgeschlossen werden konnte.
- Ab und zu wird argumentiert, die Gesellschaft habe sich gewandelt und die Privatsphäre sei nicht mehr so wichtig. Es ist die Rede von „*Small Brothers*" statt dem bekannten *Big Brother*. Auch der Begriff der Überwachungsgesellschaft wird immer wieder gebraucht. Fest steht, dass insbesondere technologische Entwicklungen, aber auch die Globalisierung den Schutz der Privatsphäre vor neue Herausforderungen stellt. Diesen *Herausforderungen* müssen wir uns stellen. Dazu haben wir einige *Grundgedanken zum Schutz der Privatsphäre in Liechtenstein* erarbeitet.
- Der Schutz der Privatsphäre kann in einer zusammenwachsenden Welt nicht in Liechtenstein isoliert angegangen werden. Deshalb ist die Mitarbeit in internationalen Gremien wichtig. Liechtenstein ist keine Insel. Gerade im Bereich der Privatsphäre gibt es zahlreiche Themen, die eine europäische oder gar eine internationale Lösung fordern.
- Schliesslich waren mit unserer neuen organisatorischen Zuordnung einige *Massnahmen* zu treffen. Um weiterhin von verschiedenen organisatorischen und administrativen Abläufen in der Landesverwaltung profitieren zu können, haben wir eine Leistungsvereinbarung mit der Landesverwaltung abgeschlossen. Auch ein internes Organisationsreglement haben wir erarbeitet.

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 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 Mai 2010

Dr. Philipp Mittelberger
Datenschutzbeauftragter

II. GRUNDLEGENDE THEMEN

1. Aktuelle Entwicklungen

Der Datenschutz und damit der Schutz der Privatsphäre gilt als eigentliche **„Querschnittsmaterie"**, da er sich auf etliche Lebensbereiche auswirkt. Dies bedeutet aber auch, dass sich der Datenschutz ständig neuen Aufgaben und Herausforderungen[1] stellen muss, die vor allem auf technologische Entwicklungen, die Diskussion um mehr Sicherheit und die Globalisierung zurückzuführen sind. Insbesondere das Internet, in dem jede Person zum Akteur werden kann, und die immer beliebter werdenden sozialen Netzwerke stellen den Schutz der Privatsphäre vor neue Herausforderungen. Generell scheint zu gelten: *„Wer nicht angeschlossen ist, ist ausgeschlossen"*. Das *Internet* hat das Leben unserer Gesellschaft verändert. *„Freunde"* scheinen eine neue Bedeutung zu bekommen. Der Schutz der Privatsphäre ist natürlich auch mit Fragen gesellschaftlicher Entwicklungen konfrontiert.

Vor diesem Hintergrund verwundert es nicht, wenn verschiedentlich argumentiert wird, dass der *rechtliche Rahmen zum Schutz der Privatsphäre nicht mehr zeitgemäss* ist. Dies ist vor allem im Hinblick auf das Internet nicht überraschend, da die allgemeine Datenschutzrichtlinie 1995 geschaffen wurde, als das Internet noch nicht die zentrale Rolle einnahm, wie dies heute der Fall ist. So hat die Europäische Kommission eine öffentliche Anhörung über den Rechtsrahmen zum Grundrecht Datenschutz durchgeführt, zu der die Art. 29 Datenschutzgruppe, in der wir den Beobachterstatus innehaben, Stellung genommen hat.[2]

Die *Datenschutzrichtlinie in der elektronischen Kommunikation* wurde bereits geändert. Unter anderem wurde eine Informationspflicht für den Fall von Sicherheitsverletzungen aufgenommen.[3] Diese Pflicht ist aus Sicht der betroffenen Personen gewiss sehr wichtig, denn nur wer informiert ist, kann über seine Daten bestimmen. Österreich hat bereits das DSG angepasst und eine entsprechende allgemein gültige Pflicht eingeführt.[4] Liechtenstein als Mitglied des EWR und - künftig auch als Schengen-Mitglied - sollte sich solchen Tendenzen anschliessen. Dies hängt nicht zuletzt damit zusammen, dass der Datenschutz in der EU mit dem Inkrafttreten des Vertrages von Lissabon aufgewertet wurde, da die *Grundrechtscharta*, in der der Datenschutz explizit als ein Grundrecht genannt wird, verbindlich wurde. Eine Arbeitsgruppe, die von der Regierung eingesetzt worden war und sich hauptsächlich mit der Zukunft der Privatsphäre befasste, kam zum Ergebnis, dass es noch verschiedene Aspekte der *allgemeinen Datenschutzrichtlinie* gibt, die in Liechtenstein *nicht umgesetzt* sind, aber den Schutz der Privatsphäre stärken würden. Demgemäss sollte die Privatsphäre, und damit auch der Datenschutz, auch in Liechtenstein gestärkt werden. Mit der Übernahme dieser Massnahmen ins DSG würde bereits *geltendes Recht* des EWR bzw. künftig geltendes Recht des Schengen-Raumes übernommen. Nicht mehr und nicht weniger. Die weiter oben angeführten Herausforderungen, allem voran aufgrund technologischer und gesellschaftlicher Entwicklungen und der Globalisierung sind hiervon noch unberührt. Das *DSG* wurde zwar erst *2008 zweimal revidiert*. Die *Dynamik* auf diesem Gebiet fordert jedoch, dass auf die erwähnten Herausforderungen eingegangen werden muss.[5]

1. Vgl. Stefano Rodota: Data Protection as a Fundamental Right, in: Reinventing Data Protection?, Gutwirth, S.; Poullet, Y.; Hert, P.; Terwangne, C.; Nouwt, S. (Hrsg.), Springer Verlag, 2009, S. 78.
2. Vgl. Stellungnahme der Art. 29 Arbeitsgruppe "Die Zukunft des Datenschutzes", III. 4.1.
3. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:DE:pdf.
4. In einem neuen § 24 Abs. 2a öDSG wurde eine besondere Informationsverpflichtung jener Auftraggeber geschaffen, die Kenntnis von einer systematischen und schwerwiegenden unrechtmässigen Verwendung ihrer Datenbestände erlangen. Diese haben die Betroffenen unverzüglich darüber zu informieren, was vor allem der Vermeidung von Vermögensschäden der Betroffenen dienen soll.
5. Die Landtagsabgeordneten Günther Kranz und Doris Frommelt wiesen anlässlich der 1. Lesung zur Abänderung des DSG am 24.10.2008, S. 2541 ff. insbesondere auf die gestiegene Bedeutung des Datenschutzes aufgrund der dynamischen technologischen Veränderungen hin. Der damalige Justizminister Klaus Tschütscher ergänzte, dass „ein hohes Datenschutzniveau ein wichtiges Kennzeichnen auch für Rechtstaatlichkeit" ist, weshalb das Bemühen aller notwendig sei. Die Entwicklung hin zu einer privaten Überwachungsgesellschaft thematisierte auch der Präsident des deutschen Bundesverfassungsgerichts, Hans-Jürgen Papier in: „25 Jahre Volkszählungsurteil. Datenschutz – Durchstarten in die Zukunft", hrsg. vom deutschen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 2009, S. 23 ff. Angesichts der häufig aufgetretenen Skandale betreffend Datendiebstahl oder die Überwachung von Arbeitnehmern und ein Internet, das nichts vergisst, erscheine eine „zweckwidrige Verwendung von heute im Internet kommunizierten Daten in der Zukunft geradezu programmiert."

Um den dynamischen Entwicklungen gerecht zu werden, haben wir einige **Grundgedanken zum Schutz der Privatsphäre in Liechtenstein** erarbeitet, die den *Weg für die Zukunft* aufzeigen sollen. Einige dieser Gedanken und Projekte finden sich auch in der nachfolgenden Berichterstattung[6] wieder.

- Der Begriff *Datenschutz* hängt sehr stark mit den Begriffen Vertrauen und Transparenz zusammen. Ein Kernanliegen des DSG ist es, dass der Bürger jederzeit wissen sollte, wer welche Daten über ihn bearbeitet: daher der Begriff „informationelle Selbstbestimmung". Aus dem DSG lassen sich die dafür notwendigen Rechte ableiten: vorherige Information, Einwilligung, Auskunfts-, Widerspruchs-, Lösch- und Berichtigungs- bzw. Sperrrecht. Jede betroffene Person soll im Rahmen des gesetzlich Erlaubten über ihre Daten verfügen können. Wobei der Begriff Daten nicht sehr persönlich ist. Dieser Begriff verdeckt den eigentlichen Kern, nämlich die durch die Verfassung geschützte Privatsphäre der einzelnen Person. Zwar mag es Abweichungen zwischen dem Recht auf Datenschutz und dem Recht auf Achtung der *Privatsphäre* geben[7], doch entscheidend ist, dass der Datenschutz nach der Rechtsprechung des Europäischen Menschenrechtsgerichtshofes als ein wesentlicher Teil der Privatsphäre angesehen wird.[8] Es wäre gewiss besser, vom *Schutz der Privatsphäre* zu sprechen, da dies den Fokus besser zeigt.

- Voraussetzung dafür, dass eine Person aber ihre Rechte wahrnehmen kann, ist, dass sie entsprechend *sensibilisiert* wird.[9] Obwohl das DSG nun einige Jahre in Kraft ist, kann unserer Ansicht nach noch nicht von einer genügenden Sensibilisierung für den Schutz der Privatsphäre in der Bevölkerung gesprochen werden. Dies ist auch auf die angesprochene Dynamik zurückzuführen. Die Sensibilisierung ist uns wichtig. So informieren wir beispielsweise regelmässig auf unserer *Internetseite*[10] über aktuelle Themen und Entwicklungen. Im Rahmen der Sensibilisierung ist auch denkbar, dass im Laufe der kommenden Jahre eine Art *Datenschutzpreis* (privacy award) an Unternehmen oder Behörden verliehen wird, welche sich vorbildlich und über das gesetzliche Mass hinaus für den Schutz der Privatsphäre einsetzen. Ziel der Sensibilisierung ist es, die jeweils betroffene Person so gut wie möglich zu informieren, damit sie selbst ihre Rechte wahrnehmen und sich so gut wie möglich selbst schützen kann.

- Gesamthaft soll der Datenschutz als *Wettbewerbsvorteil* wahrgenommen werden. Bereits heute existiert ein *Datenschutz Gütesiegel*,[11] das bereits einzelne Unternehmen in Liechtenstein innehaben. Auch die gesetzliche Regelung zu *Zertifizierungen*[12] könnte zukünftig ein weiterer Anreiz zur Implementierung von datenschutzfreundlichen betrieblichen Abläufen und Produkten sein. Unserer Ansicht nach bieten sich v.a. zwei Felder an, die eine interessante wirtschaftliche Möglichkeit eröffnen. Dabei geht es beispielsweise um die Idee der Schaffung eines *„Datenstandorts Liechtenstein"*.[13] Die Europäische Kommission fördert die Schaffung von *Privacy Enhancing Technologies (PETs)*.[14] PETs bieten die Möglichkeit, einerseits den Nutzen aus einer sich zusehends automatisierenden Welt zu ziehen und andererseits damit aber auch die Privatsphäre zu schützen. In diesem

6. Abschnitt III dieses Berichts.
7. So enthält die Charta der Grundrechte der Europäischen Union zwei separate Bestimmungen: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000X1218(01):DE:html.
8. S. EGMR-Urteil gegen Finnland vom 17. Juli 2008, § 38: „ The protection of personal data … is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention."
9. Vgl. auch Peter Hustinx: The role of Data Protection Authorities, in: Reinventing Data Protection?, Gutwirth, S.; Poullet, Y.; Hert, P.; Terwangne, C.; Nouwt, S. (Hrsg.), Springer Verlag, 2009, S. 135.
10. Vgl. III. 2.
11. Vgl. auch, Peter Hustinx: The role of Data Protection Authorities, in: Reinventing Data Protection?, Gutwirth, S.; Poullet, Y.; Hert, P.; Terwangne, C.; Nouwt, S. (Hrsg.) Springer Verlag, 2009, S. 137.
12. Art. 14a DSG.
13. Vgl. Tätigkeitsbericht 2008, 4.
14. S. III. 1.2; vgl. weiters http://www.llv.li/amtsstellen/llv-dss-spezialthemen/llv-dss-spezialthemen-technisches/llv-dss-privacy_enhancing_technolgies.html. Die Bezeichnungen Privacy by design/Privacy impact assessment/Datenschutzkonzept/Datenschutzmanagementsystem bezeichnen Produkte, welche, wie die PETs die Privatsphäre berücksichtigen.

Zusammenhang könnte sich z.B. die Hochschule als eine Art „*Think Tank*" bei der Forschung zu PETs entwickeln. Im Sinne der letzten Revision des DSG sollen *Selbstregulierungsprozesse* und interne Kontrollen in der Privatindustrie optimiert werden. Durch Audits der DSS im Bereich Datenschutz und Datensicherheit soll die Qualität der Prozesse in Unternehmen und/oder Behörden weiter verbessert werden. Dies zusätzlich zur nun möglichen Institution des *betrieblichen Datenschutzverantwortlichen* bzw. des Datenschutzberaters bei Behörden. Denkbar für die Zukunft ist ein Forum, in dem Fragen rund um den Datenschutz behandelt werden, wie dies z.B. in der Schweiz beim Verein Unternehmens-Datenschutz (VUD) der Fall ist.[15]

- Neben der Information der Öffentlichkeit ist auch die *Beratung* sehr wichtig, wie die weiterhin steigende Zahl der Anfragen zeigt.

- Gewiss gehört auch die *Aufsicht* zu unseren gesetzlichen Aufgaben, die ebenfalls wahrgenommen werden muss. Die klassische Aufsicht soll aber erst als letzte Möglichkeit in Betracht kommen, wenn die Vorstufen der Sensibilisierung, des Selbstschutzes, der Selbstregulierung und der Beratung nicht zum erwünschten Ziel geführt haben.

- „*Schengen*", wie auch „Dublin" bringen die Notwendigkeit der Durchführung von *Kontrollen* mit sich.[16] Auch das neue Kommunikationsgesetz sieht in seinem Entwurf speziell vor, dass die DSS in einem konkreten Bereich Kontrollen durchführen soll.[17] Im Rahmen einer harmonisierten Prüfung der Art. 29 Datenschutzgruppe nehmen wir schon an einer solchen koordinierten Kontrolle teil. Solche Kontrollen sollen sich aber nicht auf Behörden beschränken. Die zunehmenden technischen Möglichkeiten zur Datenbearbeitung in der Wirtschaft haben dazu geführt, dass inzwischen nicht mehr vom klassischen „*Big Brother*", dem Staat, die Rede ist, sondern von „*Small Brothers*", eben Unternehmen in der Wirtschaft.[18] Solche Aussagen wurden zwar nicht konkret in Bezug auf Liechtenstein gemacht, doch dürfte der Trend eben aufgrund der technischen Möglichkeiten auch auf Liechtenstein zutreffen. Somit sind Kontrollen natürlich auch im Privatrechtsbereich durchzuführen, wenn sich die Notwendigkeit dazu ergibt. Eine in Liechtenstein tätige Krankenkasse wandte sich beispielsweise mit dem Anliegen an uns, geprüft zu werden. Der Grund dieses Anliegens bestand darin, dass sich in Bezug auf Krankenkassen immer wieder Fragen stellen, ob der Datenschutz eingehalten wird. Wir begrüssen solche Anliegen.

- In Bezug auf die Aufsicht ist festzustellen, dass es bisher nach unserer Kenntnis nur wenige Gerichtsentscheide oder Entscheidungen der DSK gibt. Und dies, obwohl das DSG vorsieht, dass die DSK bei Verfügungen von Behörden in Datenschutzfragen - mit Ausnahme der Regierung - direkt angerufen werden kann.[19] Auch die anderen *Rechtsschutzmechanismen* werden, soweit uns bekannt ist, nicht sehr häufig genutzt,[20] wobei einschränkend zu sagen ist, dass wir nur teils beurteilen können, ob dies in der Praxis wirklich nötig ist.

- In Bezug auf die *Landesverwaltung* ist festzuhalten, dass der Datenschutz zwischen Amtshilfe und Amtsgeheimnis steht. Etliche gesetzliche Spezialregelungen sehen etwa eine Schweigepflicht vor, der Amtshilfebestimmungen aus anderen Gesetzen entgegen stehen können. Die Auslegung dieser Gesetze wird durch die Regel der *lex posterior* und der *lex specialis* nicht erleichtert.[21] Im Falle eines amtsübergreifenden Datenaustauschs sind

15. www.vud.ch.
16. Vgl. II. 2 sowie III. 4.2 und 4.3.
17. Art. 52b KomG (neu) der Vorlage gemäss BuA 110/2009.
18. In diesem Sinn auch der Bericht der Internationalen Datenschutzkonferenz 2006, an dem ein Bericht über die Überwachungsgesellschaft thematisiert wurde: Vgl. Tätigkeitsbericht 2006, 7.5; oder auch der Präsident des deutschen Bundesverfassungsgerichts, Hans-Jürgen Papier, Das Volkszählungsurteil des Bundesverfassungsgerichts, in: „25 Jahre Volkszählungsurteil. Datenschutz – Durchstarten in die Zukunft", hrsg. vom deutschen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 2009, S. 15 und der Sicherheitsexperte Bruce Schneier: http://www.schneier.com/blog/archives/2007/05/is_big_brother_1.html. Vgl. weiters Peter Schaar, Das Ende der Privatsphäre – Der Weg in die Überwachungsgesellschaft, München 2009.
19. Art. 34b DSG.
20. Art. 37 und 38 DSG.
21. Vgl. zum Thema Amtshilfe und Amtsgeheimnis, III. 1.8.

die jeweiligen Rechtsgrundlagen im Vorfeld zu prüfen, damit die Umsetzung datenschutzkonform erfolgen kann; dies wird durch die Einführung neuer Lösungen zukünftig aufwändiger. In diesem Zusammenhang sind hier insbesondere das Enterprise Content Management (ECM), eGovernment sowie Vorgänge innerhalb der zentralen Personenverwaltung (ZPV) zu nennen. Als Grundsatz gilt, dass Daten dort fliessen müssen, wo dies nötig ist.

- Was die *Wahrnehmung des Datenschutzes* selbst angeht, soll er als Ganzes wahrgenommen werden. Heute wird der Datenschutz ab und zu nur dann erwähnt, wenn dies zum eigenen Vorteil reicht, nicht jedoch, wenn es eine Pflicht darstellt, die nicht gewünscht wird. Ein „Rosinenpicken" sollte nicht mehr vorkommen. Liechtenstein ist ein Finanzplatz und möglicher Datenstandort, in dem oft vom Schutz der Privatsphäre die Rede ist. Jedoch wird dabei häufig ausser Acht gelassen, dass die Privatsphäre nicht nur einen rein finanziellen Aspekt hat. Die Privatsphäre und damit der Datenschutz ist ein Grundrecht; damit sollte auch die Wahrnehmung einhergehen.[22] Heute besteht noch hie und da die Ansicht, dass Datenschutz ein notwendiges Übel sei. Dies hat jedoch mit der beschränkten Sichtweise auf das Thema zu tun. Unsere Öffentlichkeitsarbeit soll auch dazu beitragen, dieses schiefe Bild langfristig und nachhaltig zu korrigieren.

- Unsere Tätigkeit wird natürlich auch durch *äussere Faktoren*, wie die Gesetzgebung, die oft einen EWR- oder einen Schengen-Bezug aufweist, und die „gelebte Praxis" im Lande wesentlich beeinflusst. Liechtenstein ist ein kleines Land, in dem die soziale Kontrolle relativ stark ist.

- Im Hinblick auf eine mögliche Optimierung werden auch interne Prozesse und Abläufe laufend in Bezug auf ihre Effektivität beurteilt.

Die verschiedenen Elemente dieser Gedanken sind laufend zu ergänzen oder anzupassen, wenn sich entsprechende Entwicklungen ergeben.

2. Schengen/Dublin

Wie schon im Vorjahr haben wir weiterhin intensiv an der **Vorbereitung** des **Beitritts Liechtensteins zu den Abkommen von Schengen und Dublin** gearbeitet.[23]

Kern der Abkommen ist der Zugriff liechtensteinischer Behörden auf Tausende von Datensätzen, die entsprechend geschützt werden müssen. Um den Schutz dieser Daten zu gewährleisten, findet im Vorfeld eines Beitritts eine *Evaluation* statt. Mit dieser wird die *„Schengen Reife"* eines Beitrittslandes festgestellt. Im Zentrum der Vorbereitungen stand daher die Durchführung der *Datenschutz-Probe-Evaluation* mit einem Experten, welche positiv verlaufen ist. Für das Bestehen der Evaluation ist auch die Beantwortung eines Fragebogens wesentlich. In diesem sind die Rahmenbedingungen einer Mitgliedschaft darzulegen.

Bei der Probe-Evaluation wurden verschiedene Aspekte, wie die Unabhängigkeit und Struktur der DSS sowie deren gesetzliche Aufgaben und Prüfbefugnisse und die Rechte der Bürger geprüft. Mit unserer Zuordnung zum Landtag wurde unsere *Unabhängigkeit* gestärkt. Gleichzeitig hatte der Landtag eine Stärkung der Ressourcen und auch des Budgets beschlossen.[24] Diese beiden letzteren Aspekte sind für die künftige Durchführung notwendiger Kontrollen zentral.[25]

Für unsere Vorbereitungsarbeiten konnten wir uns, neben der Mitarbeit in den entsprechenden europäischen Gremien,[26] auch bilateral insbesondere auf die Erkenntnisse der Datenschutzbehörden von Malta, Slowenien und vor allem der Schweiz abstützen.

22. Vgl. dazu in diesem Sinne auch die Aussagen Paul Vogts anlässlich der 1. Lesung zur Abänderung des DSG am 24.10.2008, S. 2543, wonach „der Datenschutzbeauftragte und die ganze Materie bis heute nicht die Wertschätzung erhalten, die ihnen gebührt".
23. S. Tätigkeitsbericht 2008, insbesondere S. 20.
24. Vgl. dazu ausführlich Tätigkeitsbericht 2008, S. 18 und S. 26. Bis dahin war die Stabsstelle für Datenschutz der Regierung zugeordnet.
25. In einer Pressemitteilung teilte die Regierung dieses positive Ergebnis der Öffentlichkeit mit: http://www.llv.li/amtsstellen/llv-pia-pressemitteilungen/pressemitteilungen-alt.htm?pmid=133499&lpid=3789&imainpos=2165.
26. Vgl. III. 4.2 und 4.3 sowie 4.5.

Der rechtliche Rahmen ist für den Beitritt und die Mitgliedschaft im Schengenraum von besonderer Bedeutung. Wir konnten bei der Schaffung der relevanten gesetzlichen Grundlagen mitarbeiten.[27]

3. Online-Umfrage

Wir haben auf unserer Internetseite in der Zeit vom 25. Mai bis 14. Juni 2009 erstmals eine Umfrage[28] durchgeführt. Ziel war es u.a. Rückmeldungen zum allgemeinen Verständnis zum Datenschutz zu erhalten. Wesentlich war uns aber auch, herauszufinden, ob und in welchen Bereichen ein verstärkter Informationsbedarf besteht. Insgesamt wurden vier Fragenblöcke zu den Bereichen *Allgemeines – Information – Vertrauen – Verhalten* gestellt. Die Umfrage wurde auch von den Medien aufgegriffen.

Wie sich herausgestellt hat, fühlte sich eine überwiegende Anzahl an Teilnehmern *nicht ausreichend* über ihre Datenschutzrechte *informiert*. Beim Wunsch nach mehr Information zu Datenschutzthemen rangierte der *Datenschutz im Internet* an erster Stelle, dicht gefolgt von den Themen Datenschutz am Arbeitsplatz und Datenschutz als Bürger.

Die Frage nach der *Bedeutung des Schutzes* der persönlichen Daten durch Unternehmen, die Daten speichern, beantworteten nahezu alle Teilnehmer mit *sehr wichtig*.

Das *geringste Vertrauen* in die richtige Verwendung der persönlichen Daten durch Unternehmen haben die Teilnehmer in die *Kaufhäuser*. Relativ *hohes Vertrauen* wird den Banken und der *Polizei* entgegengebracht. Auffallend war die *hohe Zahl* jener Personen, die, ihrem Wissen zufolge, bereits einmal von einem *Missbrauch ihrer Daten betroffen* waren. Zur Frage des persönlichen Verhaltens schätzt die überwiegende Anzahl der Teilnehmer ihren eigenen Umgang mit deren persönlichen Daten als *kritisch oder sehr kritisch* ein.

Information (Wissen) – Vertrauen – Verhalten gehören offensichtlich *zusammen*. So wurde die Frage, ob sich die Teilnehmer über ihre Datenschutzrechte ausreichend informiert fühlen, durch eine überwiegende Anzahl von Antworten klar verneint. Nur wer seine Rechte und Pflichten kennt, möchte auch, dass diese von anderen geschützt und richtig verwendet werden. Daraus leitet sich sowohl ein kritischer Umgang mit den eigenen persönlichen Daten als auch mit dem Umgang persönlicher Daten anderer ab.

4. Volkszählung

2010 wird erneut eine *Volkszählung* stattfinden, die erste seit zehn Jahren und die erste seit Inkrafttreten des DSG. Ändert sich etwas an der Volkszählung, weil es nun das DSG gibt? Grundsätzlich nicht. Volkszählungen gibt es auch in den anderen europäischen Ländern, die schon länger ein DSG kennen, als dies in Liechtenstein der Fall ist. Die Informationen, die sich aus Volkszählungen ergeben, stellen ein wichtiges *Steuerungsinstrument* für den Landtag und die Regierung dar.[29] Es werden zahlreiche Daten erhoben, wobei bei dieser Volkszählung nicht mehr alle Daten *direkt bei den Betroffenen* erhoben, sondern *teils auch aus Registern* bezogen werden.

Gewiss entsteht bei der Teilnahme ein *Persönlichkeitsprofil* der Teilnehmer. Doch Sinn der Volkszählung ist die statistische Auswertung. Diese Daten werden auch nur für statistische Zwecke verwendet. Das *Statistikgeheimnis*, das zur Geheimhaltung von in Erfahrung gebrachten Daten dient, gilt nach wie vor. Wir wurden bei verschiedenen Aspekten der kommenden Volkszählung *aktiv* durch das Amt für Statistik einbezogen und begrüssen diesen Umstand. Denn somit können allfällige Fragen *frühzeitig* aufgegriffen werden.

Unabhängig von der Volkszählung wurden wir vereinzelt mit der Frage konfrontiert, ob es rechtmässig sei, dass durch das Amt für Statistik angefragte

27. Vgl. III. 3.
28. http://www.dss.llv.li. S. Fragen und Auswertung im Anhang.
29. http://www.llv.li/amtsstellen/llv-as-volkszaehlung.htm.

Stellen personenbezogene Daten an dasselbe bekanntgeben. Diesbezüglich ist festzuhalten, dass das DSG eine *Spezialregelung* vorsieht. Danach dürfen Daten durch Behörden für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeitet werden, vor allem wenn die Daten anonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt und die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.[30] Auch die Volkszählung wird *namensbezogen* durchgeführt. Das war bei der letzten Volkszählung im Jahr 2000 der Fall und ist auch z.B. in der Schweiz Praxis, von wo die Fragebogen übernommen wurden.

Gerade der Umstand, dass ein Teil der Volkszählung *neu registergestützt* durchgeführt wird, setzt voraus, dass der *andere Teil namensbezogen* stattfindet. Sonst könnten die beiden Teile nicht zu einem Ganzen zusammengeführt werden. Bekanntermassen gibt es auch in der Schweiz Datenschutzregelungen, die eingehalten werden müssen. Mit anderen Worten steht aus *Datenschutzsicht* dem Vorhaben einer erneuten Volkszählung unter Namensnennung der Beteiligten *nichts entgegen*, wenn die gesetzlichen Vorschriften *(Statistikgeheimnis)* eingehalten werden. Wir werden unsere Zusammenarbeit mit dem Amt für Statistik vor der Durchführung der Volkszählung fortsetzen und unseren Beitrag dazu leisten, damit diese das von Regierung und Landtag gewünschte Steuerungsinstrument bleibt.

30. Art. 26 DSG.

III. BERICHTERSTATTUNG 2009

Die Zahl der Anfragen, die an uns gerichtet werden, nehmen weiterhin zu. Im vergangenen Jahr wurden *so viele Anfragen wie noch nie* an uns gestellt.[31] Im Berichtsjahr gingen insgesamt 431 Anfragen ein, was gegenüber dem Vorjahr eine Zunahme um 115 Anfragen bedeutet. Dies kann gewiss auf ein *steigendes Bewusstsein* für den Schutz der Privatsphäre zurückgeführt werden.

Es würde den Rahmen dieses Berichtes 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. Datenschutz allgemein

1.1.1. Allgemeine datenschutzrechtliche Fragen

Schwarze Listen (englisch *blacklist*) haben einen negativen Touch. Bei solchen Listen geht es um *Personen*, die in irgendeiner Form *nicht gewünscht* sind: Personen mit Zutrittsverbot zu Fussballstadien, Diskotheken, Wirtshäusern, die *„no-fly"* Liste der USA oder Listen von Pädophilen und dergleichen sind nur einige Beispiele. Wenn jemand auf einer solchen Liste geführt wird, geschieht dies kaum zum eigenen Vorteil.[32]

Sind diese Negativlisten aus datenschutzrechtlicher Sicht aber grundsätzlich schlecht?

Das Führen einer solchen Liste nach dem DSG ist zulässig, wenn die *Einwilligung der betroffenen Personen* vorliegt, ein *Gesetz dies erlaubt* oder wenn ein *überwiegendes privates oder öffentliches Interesse* vorliegt. Da Schwarze Listen nicht zum Vorteil der betroffenen Personen und meistens ohne deren Wissen geführt werden, dürfte die Einwilligung in den meisten Fällen von vorneherein nicht in Betracht kommen. Oftmals wird die Zulässigkeit entweder auf eine gesetzliche Grundlage oder das überwiegende private oder öffentliche Interesse abzustützen sein, z.B. zur Vermeidung von Sachbeschädigungen. Bei einer Negativliste von einfachen Personendaten,[33] die aus *allgemein zugänglichen* Quellen, wie beispielsweise aus den Medien, gesammelt wurden, wird in der Regel ein überwiegendes Interesse des Inhabers der Datensammlung *angenommen*, sodass eine entsprechende *Datenbearbeitung zulässig* sein dürfte.

Die *Art. 29 Datenschutzgruppe*[34] hat eine ausführliche *Stellungnahme* zu Schwarzen Listen[35] abgegeben, in der unter anderem auch auf die in diesem Kontext kritischen Punkte eingegangen wird, wie insbesondere *Richtigkeit* der Daten (Fehler bei der Identifizierung), *Aktualisierungspflicht*, Wahrnehmung des *Auskunftsrechts* der betroffenen Personen, *Speicherdauer* oder Pflicht zur *Löschung nach Zweckerreichung*. Die Realisierung der auch hier bestehenden Rechte der betroffenen Personen auf Information und Auskunft bzw. Berichtigung und Löschung dürfte den Inhaber einer Schwarzen Liste in der Praxis vor Probleme stellen, da es für die Negativlisten ja gerade das *typische Merkmal* ist, dass die betroffenen Personen *keine* Kenntnis von dieser Datensammlung haben sollten.[36]

Gerade bei *Schuldnerverzeichnissen* und *Informationsdiensten über Zahlungsfähigkeit und Kreditwürdigkeit* ist es aber zentral, dass eine betroffene

31. 431 gegenüber 316 im Vorjahr; vgl. dazu Details im Anhang.
32. Bei einer Schwarzen Liste werden bestimmte Daten über eine bestimmte Gruppe von Personen erhoben und verbreitet. Die Kriterien richten sich nach der Art der jeweiligen Schwarzen Liste. Die Aufnahme in die Liste ist für die erfassten Personen mit negativen und nachteiligen Folgen verbunden. Beispielsweise wird ihnen dadurch der Zugang zu einer bestimmten Dienstleistung verweigert oder ihr Ruf geschädigt.
33. Einfache Personendaten sind zum Beispiel Name oder Geburtsdatum einer Person. Davon zu unterscheiden sind die Begriffe Persönlichkeitsprofile oder besonders schützenswerte Personendaten. Im Zusammenhang mit Negativlisten sind dies beispielsweise Daten über Verfolgungen und Verurteilungen von Justizbehörden, über Disziplinarverfahren, administrativer Führerausweis-Entzug oder Daten betreffend den Strafvollzug. Auch Sanktionsentscheide von privaten Verbänden und Vereinen gelten als besonders schützenswerte Daten. Daten über die Einkommens- und Vermögensverhältnisse gelten hingegen nicht als besonders schützenswert, auch wenn sie durch das Banken- oder Steuergeheimnis geschützt sind; vgl. dazu auch Tätigkeitsbericht 2008, 2.3.
34. Vgl. III. 4.1.
35. Arbeitspapier über Schwarze Listen, angenommen am 03. Oktober 2002 (WP 65), abzurufen unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp65_de.pdf.
36. Vgl. auch Erläuterungen zum Thema „Schwarze Listen" des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB): http://www.edoeb.admin.ch/themen/00794/00819/01158/index.html?lang=de.

Person ihre Rechte wahrnehmen kann. Um zu wissen, welche Daten von wem bearbeitet werden, muss die betroffene Person zunächst Auskunft verlangen. Denn erst dann, wenn die betroffene Person weiss, welche Informationen von wem über sie gesammelt wurden, kann sie effektiv ihr Recht durchsetzen, falsche oder veraltete Daten berichtigen bzw. löschen zu lassen. Die Inhaber einer Schwarzen Liste dürfen die Auskunft nicht einfach mit dem Hinweis darauf verweigern, dass es sich bei einer Negativliste um eine interne, vertrauliche Datensammlung handle. Eine Auskunftsverweigerung oder –einschränkung ist auch hier nur unter den gesetzlichen Voraussetzungen des DSG[37] zulässig.

Einer **Veröffentlichung von anonymisierten Daten** steht aus Datenschutzsicht *nichts entgegen*.[38] Denn *Personendaten* sind Daten, die sich auf eine *bestimmte oder bestimmbare* Person beziehen. Anonymisierte Daten beziehen sich jedoch eben *gerade* nicht auf eine bestimmte oder bestimmbare Person. Als anonymisierte Daten gelten anonyme Daten, die sich zuvor auf eine bestimmbare Person bezogen haben, die jedoch *nicht mehr identifizierbar ist.*[39]

1.1.2. Gesetzliche Rechte

Das **Recht auf Achtung der Privatsphäre**, und damit auf Datenschutz, wird oft auch mit dem Begriff der *„informationellen Selbstbestimmung"* gleichgesetzt. Bei letzterem geht es darum, dass eine Person wissen können soll, *wer was wann und bei welcher Gelegenheit über sie weiss*.[40] Nur wenn diese Transparenz vorhanden ist, kann sich diese Person dagegen wehren, dass falsche oder zu viele Angaben über sie bearbeitet werden. Das Gesetz sieht in diesem Sinn vor, dass eine betroffene Person gewisse *Informationen im Voraus* erhalten muss. Dies geschieht oft in Allgemeinen Geschäftsbedingungen. Ist sie mit dieser Information einverstanden, kann sie zu einer Datenbearbeitung ihre *Einwilligung* geben. Möchte sie (später) erfahren, was für Angaben über sie genau bearbeitet werden, woher sie stammen, usw., steht ihr das gesetzliche *Auskunftsrecht* zu. Ist sie mit der Antwort nicht einverstanden, kann sie die Daten *berichtigen, löschen oder sperren* lassen.[41]

Wenn eine betroffene Person also der Ansicht ist, dass eine nicht erlaubte Datenbearbeitung vorliegt, stehen ihr nach dem DSG verschiedene Wege offen. So kann die betroffene Person bei Vorliegen eines schutzwürdigen Interesses der Datenbearbeitung widersprechen oder die Berichtigung oder Löschung falscher bzw. veralteter Daten von der *verantwortlichen Stelle* verlangen. Ausserdem kann verlangt werden, dass die verantwortliche Stelle das widerrechtliche Bearbeiten von Personendaten unterlässt, die Folgen des widerrechtlichen Bearbeitens beseitigt und/oder die Widerrechtlichkeit des Bearbeitens feststellt. Gegen behördliche Verfügungen kann ausserdem direkt Beschwerde bei der Datenschutzkommission eingelegt werden. In allen Fällen aber können sich die betroffenen Personen jederzeit an uns wenden.

Um die Geltendmachung dieser Rechte ging es in folgenden Fällen:

- Ein Internetnutzer ersuchte uns um Unterstützung bei der **Löschung von verschiedenen Forenbeiträgen**, die er über mehrere Jahre in Internet-Foren geschrieben oder auf anderen Plattformen veröffentlicht hatte. Um sich von den gemachten Aussagen und Äusserungen distanzieren zu können, versuchte der Nutzer zuerst bei den jeweiligen *Forenbetreibern direkt* die Löschung der

37. Art. 12 DSG.
38. Vgl. auch Tätigkeitsbericht 2008, 5.
39. Vgl. hierzu die Stellungnahme der Art. 29 Arbeitsgruppe zum Begriff der Personendaten, S. 24: http://www.llv.li/pdf-llv-li-stellungnahme_4_2007_zum_begriff_personenbezogene_daten-2.pdf.
40. Vgl. hierzu auch Tätigkeitsberichte 2004 bis 2006, 3.2.
41. Der Europäische Gerichtshof (EuGH) hat in einem Urteil die Bedeutung des Auskunftsrechts betont, da es erforderlich ist, um der betroffenen Person die Wahrnehmung weiterer Rechte zu ermöglichen. Entspricht die Verarbeitung ihrer Daten nicht den gesetzlichen Bestimmungen, kann sie deren Berichtigung, Löschung oder Sperrung durch den für die Verarbeitung Verantwortlichen verlangen. Sie kann ihn auch verpflichten, diese Berichtigung, Löschung oder Sperrung dem Dritten, an den diese Daten übermittelt worden sind, mitzuteilen, sofern sich dies nicht als unmöglich erweist und kein unverhältnismässiger Aufwand damit verbunden ist. Vgl. College van burgemeester en wethouders van Rotterdam gegen M. E. E. Rijkeboer, Urteil vom 07. Mai 2009, Erwägung 51: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62007J0553:DE:HTML.

entsprechenden Beiträge zu erwirken. Diese Ersuchen wurden jedoch *nicht in jedem Fall berücksichtigt*. Die Ursachen für eine fehlende Mitwirkung können dabei *vielfältig* sein: z.B. fehlende Zuständigkeiten bei den Plattformbetreibern, veraltete Kontaktdaten, ungepflegte Internetauftritte und Foren oder technisch aufwändig zu lösende Abhängigkeiten sind möglich. Wenn sich der entsprechende Server im Ausland befindet, ist zu berücksichtigen, dass eine unterschiedliche Rechtslage wahrscheinlich ist, wobei sich das Problem vergrössert, wenn der Server in einem Land steht, das keinen angemessenen Datenschutz aufweist. Möglicherweise kommen Verständigungsschwierigkeiten aufgrund einer anderen Sprache hinzu. Allgemein kann gesagt werden, dass aus diesen Gründen einmal geäusserte Meinungen in Foren oder geschriebene Beiträge auf anderen Internet-Auftritten ohne Mitwirkung des Plattformbetreibers kaum *dauerhaft entfernt* werden können.[42]

In weiterer Folge wandte sich der Nutzer an Anbieter von Suchmaschinen, wie z.B. Google, Bing oder Yahoo!, um dort die Unterdrückung bzw. Filterung der noch im Internet verfügbaren und durch den jeweiligen Plattformbetreiber nicht gelöschten Forenbeiträge in den Suchtrefferlisten durchzusetzen. Suchmaschinen erfassen ausschliesslich die Inhalte im öffentlich verfügbaren Internet und liefern auf Suchanfrage Verweise auf diese Webauftritte mit entsprechenden Inhalten als Antwort. Eine *Filterung* der *Suchresultate und Suchtrefferlisten* ist *in der Regel nicht vorgesehen*. Durch den regelmässigen wiederholten Besuch der im Suchindex erfassten Seiten im Internet, werden Änderungen durch die Suchmaschinenbetreiber erkannt und der Suchindex entsprechend angepasst. Im gegenständlichen Zusammenhang weist z.B. Google darauf hin, dass die öffentlich verfügbaren Informationen im Internet zuerst auf den entsprechenden Webseiten angepasst oder entfernt werden müssen, bevor diese in den Suchtrefferlisten nicht mehr ausgegeben werden. Eine Filterung konkreter Inhalte sei nicht möglich.[43]

- **Adresshandel** führt zu *Werbung*, die auch unerwünscht sein kann. Um den *Adresshandel* zu *unterbinden*, hat der Gesetzgeber eine *spezielle Norm* geschaffen. Demzufolge ist die von der *Direktwerbung* betroffene Person vorab zu informieren und auf das ihr *zustehende unentgeltliche und sofort wirksame Widerspruchsrecht*[44] hinzuweisen. Adresshandel gibt es auch in Liechtenstein. Da die Person, die sich an uns gewendet hat, offenbar nicht im Voraus informiert wurde, möglicherweise weil sie im Ausland wohnt, machten wir darauf aufmerksam, dass jeder Person das gesetzlich garantierte Auskunfts- und danach auch das Löschrecht zusteht. Dieses kann durch Verwendung eines Musterschreibens auf unserer Internetseite geltend gemacht werden.[45] Mit der Geltendmachung des Auskunftsrechtes kann insbesondere in Erfahrung gebracht werden, *welche* Daten vorhanden sind und *woher* sie stammen. Wünscht eine betroffene Person, dass die Daten beispielsweise durch ein Adresshandelsunternehmen nicht bearbeitet werden sollen, steht ihr das gesetzliche Recht zu, die Daten *löschen* zu lassen. Grundsätzlich sind Datensammlungen, von denen die betroffenen Personen *keine Kenntnis* haben, bei uns zu *registrieren*.[46] Mit Hilfe des von uns geführten Registers der Datensammlungen kann herausgefunden werden, welche Datensammlungen bestehen. In Bezug auf diese Datensammlungen können dann die gesetzlichen Rechte geltend gemacht werden.

- Die Versendung von elektronischen **Werbemails** ist grundsätzlich nicht mehr erlaubt.[47] Mit der Schaffung des Kommunikationsgesetzes wurde

42. Siehe dazu Digma, Heft 4, Dezember 2007, „Wie schütze ich mein virtuelles Ich? – Von den (begrenzten) rechtlichen Möglichkeiten, Daten über die eigene Person im Internet zu kontrollieren."
43. http://www.google.com/support/webmasters/bin/answer.py?hl=de&answer=156094.
44. Art. 14 Abs. 3 DSG.
45. http://www.llv.li/form-llv-dss-musterschreiben.
46. Diesbezüglich ist anzuführen, dass diese Firma ihre Datensammlung bei uns nicht angemeldet hat, obwohl sie dazu verpflichtet gewesen wäre. Denn seit der letzten Teilrevision des DSG gilt auch für private Personen eine grundsätzliche Pflicht zur Anmeldung zum Register der Datensammlungen. Mit dieser Anpassung ist man einer Forderung der Europäischen Aufsichtsbehörde (ESA) nachgekommen. Waren bisher Datensammlungen privater Personen nur dann unter bestimmten zusätzlichen Voraussetzungen zum Register anzumelden, wenn sie besonders schützenswerte Daten oder Persönlichkeitsprofile enthielten, besteht neu eine generelle Anmeldepflicht. Weitere Ausnahmen von dieser Anmeldepflicht sind abschliessend in der DSV geregelt. Damit besteht von wenigen Ausnahmen abgesehen nunmehr für Behörden und private Personen gleichermassen die Pflicht zur Anmeldung ihrer Datensammlungen zum Register.
47. Art. 18b DSV.

vom sogenannten *Opt-out* zum *Opt-in* gewechselt. Vielmehr ist bloss eine *einmalige Anfrage* eines Unternehmens erlaubt. In dieser Anfrage muss danach gefragt werden, ob eine betroffene Person wünscht, Werbung zu erhalten. Nur wenn dies bejaht wird (Opt-in), ist die Zusendung von Werbemails gesetzlich gestattet. Bis heute ist diese Gesetzesänderung offenbar in der Praxis noch nicht bei allen Beteiligten bekannt. Deshalb soll dies hier erwähnt werden.

- Die **Veröffentlichung von Fotos auf Internetseiten** kommt auch bei Behörden immer wieder vor. Dabei handelt es sich um ein sogenanntes *elektronisches Abrufverfahren. Behörden oder Schulen* dürfen Personendaten, wie Namen, Geschäftsadresse, geschäftliche Telefonnummer oder E-Mailadresse von Mitarbeitern mit solchen Abrufverfahren bekannt geben.[48] Bei weiter gehenden Daten, wie z.B. der Veröffentlichung eines Fotos, muss die betroffene Person *im Voraus* auf die geplante Veröffentlichung aufmerksam gemacht werden und die Einwilligung geben. Wurde die betroffene Person nicht vorab informiert und liegt auch keine Einwilligung vor, ist z.B. die Veröffentlichung eines Fotos bei Behörden *nicht erlaubt*. Eine Person kann somit die *Löschung* ihres Fotos von der in Frage stehenden Internetseite *verlangen*.

- Gleiches gilt bei einem **Intranet**. Auch da kann es vorkommen, dass nicht nur Identifikationsdaten aufscheinen, sondern auch zum Beispiel Geburtsdatum oder ein Foto der betreffenden Person. Der Sinn eines Intranets ist die Erleichterung der Kontaktaufnahme mit einer bestimmten Person. Für eine solche reicht es aus, wenn die Identifikationsdaten aufscheinen (Name, Vorname, Funktion, Telefonnummer oder E-Mailadresse). Ein Foto mag zur Kontaktaufnahme praktisch sein, ist jedoch nicht notwendig. Enthält das Intranet auch andere, darüber hinaus gehende Informationen, ist deren Bekanntgabe freiwillig, d.h. sie ist bei Behörden nur mit einer Einwilligung erlaubt. In der Privatwirtschaft darf der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind.[49] Bei einem Foto in einem Intranet eines Unternehmens ist weder das eine noch das andere der Fall. Hiervon darf auch nicht mit einer Einwilligung des Arbeitnehmers abgewichen werden.[50]

- In den Gemeinden ist es üblich, dass **Adressen der Gemeindeeinwohner** an in der Gemeinde tätige **Vereine** oder andere Institutionen zu *ideellen Zwecken* bekannt gegeben werden. Dies wünschte der Gesetzgeber bei der Schaffung des DSG. Das DSG sieht aber vor, dass eine solche Bekanntgabe *gesperrt* werden kann. Eine derartige Datensperre ist jedoch[51] nur möglich, wenn *keine Rechtspflicht* zur Bekanntgabe besteht oder die Erfüllung der gesetzlichen Aufgaben der verantwortlichen Behörde nicht gefährdet wäre. Bei der Bekanntgabe an Dorfvereine gibt es keine gesetzliche Pflicht, sodass man seine Adresse sperren lassen kann. Zur leichteren Handhabung dieses Sperrrechts ist auf unserer Internetseite ein *Musterschreiben* verfügbar, mit dem das genannte *Sperrrecht*, aber auch die *anderen Rechte* für betroffene Personen, in Anspruch genommen werden können. Die Gemeinden haben ihr System demgemäss eingerichtet.

- In vielen Unternehmen erhalten die Mitarbeiter einen **Aufwandsersatz für das Mittagessen**. Eine Beschwerde betraf die Änderung einer bestehenden Abrechnung zu einer *automatisierten Form der Verrechnung*. Durch die Einführung der elektronischen Lösung sollte die Möglichkeit von Missbrauch durch anspruchsberechtigte Personen eingeschränkt werden. Es galt, eine vernünftige Balance zwischen der Benutzbarkeit der Neulösung und dem Schutz der Privatsphäre der Anspruchsberechtigten zu finden. Seit der Umstellung werden automatisiert personenbezogene Daten erfasst und für die Verrechnung ausgewertet. Dem Grundsatz der *Datensparsamkeit* und dem Schutz der Privatsphäre folgend wurden verschiedene unserer Empfehlungen, wie z.B. die

48. Vgl. Tätigkeitsbericht 2008, 11.1., Tätigkeitsbericht 2007, 3.1.
49. Art. 28a des Einzelarbeitsvertragsrechts.
50. Art. 113 des Einzelarbeitsvertragsrechts.
51. Art. 24 Abs. 2 DSG.

Einsicht und den Zugriff auf die unbedingt notwendigen Daten einzuschränken, auf die Erfassung von zusätzlichen personenbezogenen Daten zu verzichten, die Prozesse zur Bearbeitung von Beschwerden zu definieren sowie die Datenbearbeitung lückenlos zu dokumentieren, umgesetzt. Gerade bei der Ablöse bestehender Papierlösungen durch elektronische und somit automatisierte Systeme sollte auf Datensparsamkeit geachtet und nur jene Daten erfasst werden, die zur Zweckerreichung notwendig sind.

1.2. Technologischer Datenschutz

Bei einem **amtlichen Ausweis** stellte sich die Frage, ob die **Persönliche Identifikationsnummer (Personen-Identifikationsnummer, PEID)**[52] *zusätzlich zur Ausweisnummer* aufgedruckt werden soll. Wir konnten keinen *erkennbaren Mehrwert* durch den Abdruck der PEID finden, da der Ausweis ja mit einer Ausweisnummer versehen war. Diese Identität ergibt sich insbesondere durch die persönlichen Attribute wie Namen und Geburtsdatum. Hier war ein zusätzliches Merkmal aus unserer Sicht nicht notwendig. Auch als Sicherheitsmerkmal ist die PEID nicht notwendig. Vielmehr könnten dabei Bedürfnisse geweckt werden, diese Nummer auch im Privat- und Unternehmensumfeld zur Identifikation zu verwenden. Somit wäre eine *firmenübergreifende Identifizierung sowie der automatisierte Abgleich* von Informationen über die Grenzen von Datenbeständen hinweg ohne grossen Aufwand möglich. Dieser Aspekt stellt aus Sicht des Datenschutzes eine der grössten Gefahren im Zusammenhang mit der Verwendung der hier diskutierten Nummer dar. Aufgrund der oben angeführten Argumente und schwer vorhersehbaren Entwicklungen wurde aus unserer Sicht der Abdruck der PEID als *unverhältnismässig* eingestuft. Ungeachtet der angeführten Argumente wäre das Abdrucken der PEID auf dem Ausweis aufgrund der *fehlenden Rechtsgrundlage ohnehin nicht möglich* gewesen.[53]

Der Suchmaschinenbetreiber **Google Inc.** unterhält im Internet den Service **„Street View"**.[54] Mit Videotechnik ausgestatteten Fahrzeugen erfasst Google *Strassenansichten sowie öffentliche Plätze* und veröffentlicht die *Bilder* im Anschluss im Internet. Neben Gebäuden werden auch *Personen* und *Fahrzeuge* aufgezeichnet, die sich zum Aufnahmezeitpunkt im Kamerafokus befinden. Die Aufnahmen sind weltweit über das Internet zugänglich, um interessierten Nutzern einen „virtuellen Spaziergang" zu ermöglichen. Auch wenn es sich bei den Bildern nur um eine Momentaufnahme handelt, kam es in einigen Ländern bereits zu unterschiedlichen Beschwerden von Personen, die in unangenehmen Situationen oder in sensitiven Gegenden (z.B. Besuch eines Erotikshops, Spitäler, Gefängnisse etc.) aufgezeichnet wurden. Um eine eindeutige Identifizierung zu verhindern, werden Gesichter und Fahrzeugkennzeichen von Google angeblich *unkenntlich* gemacht (englisch *blurring*).

Die Reaktionen der Öffentlichkeit und der Datenschutzbehörden in *Europa* auf Street View sind sehr *unterschiedlich*. So verlangt unter anderem *Deutschland* von Google eine *Vorinformation* darüber, in welchen Ortschaften und wann genau Aufnahmen geplant sind. Auch wird die Kamera auf den Aufnahmefahrzeugen als zu hoch kritisiert. So ist es unter anderem bei der derzeitigen Aufnahmeeinstellung möglich, über Hecken und Zäune hinweg in Vorhöfe und nicht öffentliche Gärten zu blicken. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) in der *Schweiz* kam nach eingehender Prüfung von Street View zum Schluss, dass dem *Schutz der Privatsphäre* trotz zusätzlicher Massnahmen vonseiten des Anbieters *nicht in allen Fällen Genüge* getan wird. Aus diesem Grund richtete er mehrere Empfehlungen an Google Inc.[55] Da die *Empfehlungen nicht befolgt* wurden, zog der EDÖB den Fall vor das Bundesverwaltungsgericht, dessen Entscheidung noch aussteht. Neben der *Information der Öffentlichkeit* geht es vor allem um *technische Fragen*, z.B. wie die Daten geschützt und wann die Rohdaten gelöscht werden. Wir verfolgen die Entwicklungen in anderen Ländern aufmerksam, um die Einhaltung der Privatsphäre in Liechtenstein zu schützen, falls Google Aufzeichnungen in Liechtenstein machen möchte.

52. Diese Nummer wird im Zentralen Personenverzeichnis der Landesverwaltung verwendet.
53. Zur PEID, vgl. auch Tätigkeitsbericht 2008, 3.1 und 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/themen/00794/01189/index.html?lang=de.
54. http://maps.google.com/help/maps/streetview/.
55. http://www.edoeb.admin.ch/aktuell/01584/index.html?lang=de.

Die Europäische Kommission fördert[56] und fordert[57] die Entwicklung und Anwendung von **Technologien zum Schutz der Privatsphäre** (englisch *Privacy Enhancing Technologies, PETs*). Dabei handelt es sich um ein zusammenhängendes System von Information- Communication- Technology- (ICT) Massnahmen, welche die Privatsphäre durch die Reduktion und Vermeidung der Angabe von persönlichen Daten schützt, indem diese auf das notwendige Mass reduziert und/oder die unerwünschte Bearbeitung verhindert wird. Dabei geht insbesondere die *Funktionalität* des Information verarbeitenden Systems *nicht* verloren.[58] So sollten Informationsverarbeitungssysteme wenn möglich so gestaltet werden, dass keine personenbezogenen Daten für die Nutzung erhoben, gespeichert oder verarbeitet werden, wodurch eine anonyme bzw. *pseudonymisierte* Nutzung möglich wird. So besteht bei der Überwachung öffentlicher Bereiche mittels einer Videoüberwachungsanlage zwecks Beweissicherung nach sicherheitsrelevanten Vorfällen die Notwendigkeit zur Identifikation einer aufgezeichneten Person in der Regel erst dann, wenn ein konkreter Verdacht eines relevanten Sachverhalts vorliegt. So existieren z.B. Aufzeichnungssysteme, welche Personen im Kamerafokus bei der Speicherung unkenntlich machen, und die gespeicherten Bilder sich erst bei Bedarf zur Auswertung durch berechtigte Personen entschlüsseln lassen.

Privatsphäre ist nicht gleich Datensicherheit. Viele Unternehmen implementieren zahlreiche Sicherheitsmassnahmen zum Schutz ihrer Daten, wobei dies nicht zwingend bedeuten muss, dass die Privatsphäre der Mitarbeiter und anderer betroffener Personen wie z.B. Kunden ausreichend geschützt ist. Der Aufwand ist jedoch offensichtlich wesentlich geringer, die *Entstehung* von persönlichen und sensiblen Daten in verschiedenen Geschäftsprozessen zu verhindern oder auf das notwendige Mass zu beschränken (Datensparsamkeit), als das entstehende Sicherheitsrisiko bei der Datenbearbeitung *im Nachhinein* zu mindern.

Wir beobachten die Entwicklung zu PETs aufmerksam. Gerade für die Region und insbesondere für Liechtenstein könnte mit einer entsprechenden Bewusstseinsbildung und dem vermehrten Einsatz von PETs in regionalen Unternehmen ein konkreter *wirtschaftlicher Nutzen und Wettbewerbsvorteil* erzielt werden. Begleitet würde dieser Einsatz mit einer Erhöhung des Schutzes der Privatsphäre.

Im Zusammenhang mit der Weiterentwicklung und Umsetzung der **eGovernment Strategie** der Landesverwaltung wurden wir bei einem laufenden Projekt bereits in die Konzeptionsphase mit einbezogen. Datenschutzaspekte konnten auf diese Weise in einem frühen Stadium der Entwicklung dargestellt werden. Diese Vorgehensweise wird von uns begrüsst.

1.3. Telekommunikation

Die Art. 29 Datenschutzgruppe hat vor einigen Jahren beschlossen, gemeinsame **Untersuchungen** durchzuführen, um zu einer **möglichst einheitlichen Rechtsanwendung** in den EWR-Ländern beizutragen.[59] Als Thema wurde letztes Jahr der **Telekommunikationsbereich** ausgewählt und eine Erhebung unter den Anbietern von Telekommunikationsdienstleistungen vorbereitet.[60] Diese Erhebung betrifft die Einhaltung der nationalen gesetzlichen Vorgaben.[61] Auch Länder, die die Richtlinie zur Vorratsdatenspeicherung noch nicht umgesetzt haben, waren zur Teilnahme an der Untersuchung aufgefordert. In Liechtenstein wurde diese Richtlinie noch nicht formal umgesetzt. Allerdings gilt nach liechtensteinischem

56. Es werden derzeit verschiedenste Projekte durch die Kommission finanziell unterstützt. z.B. FIDIS ("Future of Identity in the Information Society" - http://www.fidis.net/), PRIME ("Privacy and Identity Management for Europe" - https://www.prime-project.eu/), RISEPTIS ("Research and Innovation for Security, Privacy and Trustworthiness in the Information Society" - http://www.think-trust.eu/).
57. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:DE:PDF.
58. S. Tätigkeitsbericht 2007, 3.1. Die Europäische Kommission gab im November 2008 eine Studie in Auftrag, um den wirtschaftlichen Nutzen für Unternehmen beim Einsatz von Technologien zum Schutz der Privatsphäre zu untersuchen: http://ec.europa.eu/justice_home/funding/tenders/2008_S238_315681/invitation_tender_de.pdf.
59. Im Jahr 2006 führte die Art. 29 Datenschutzgruppe erstmals eine gemeinsame und europaweite Überprüfung des Krankenversicherungssektors durch, an der wir noch nicht teilnehmen konnten, vgl. Tätigkeitsbericht 2006, 7.1.
60. Vgl. "Mandate to the Enforcement Subgroup to proceed to the 2nd joint investigation action (WP 152)", abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp152_en.pdf.
61. Insbesondere die Vorschriften des Kommunikationsgesetzes (KomG) und der Verordnung vom 3. April 2007 über elektronische Kommunikationsnetze und -dienste (VKND). Diese stützen sich auf Art. 6 und 9 der Richtlinie 2002/58/EG (ePrivacy Richtlinie) und die diese Richtlinie ergänzende Richtlinie 2006/24/EG zur Vorratsdatenspeicherung durch die nationalen Telekommunikations- und Internetserviceanbieter.

Recht schon jetzt eine *sechsmonatige Vorratsdatenspeicherung für Verkehrsdaten*.[62] Eine Speicherung erfolgt auch bei vergeblichen Anrufversuchen. Das vorrangige Ziel dieser europaweit durchgeführten Untersuchung ist es, zu analysieren, ob und wie die Anforderungen des Datenschutzes bei der Vorratsdatenspeicherung – Sicherheitsmassnahmen, Vorkehrungen gegen Datenmissbrauch sowie die Begrenzung der Speicherdauer – im Telekommunikationsbereich der einzelnen Mitgliedstaaten erfüllt bzw. berücksichtigt werden. Die Fragen konzentrieren sich auf zehn Bereiche, die für die Speicherung und die Sicherheit von Verkehrsdaten im Telekommunikationsbereich relevant sind.[63]

Zur Beantwortung dieser Fragen haben wir eine Untersuchung durchgeführt. Die von den ausgewählten Unternehmen erteilten Antworten werden in Form eines *nationalen Berichts* zusammengefasst und ausgewertet. Die Art. 29 Datenschutzgruppe wird die Öffentlichkeit über die Ergebnisse informieren.

Die Frage, ob ein **Telefonanbieter die Kundendaten zu Werbezwecken weitergeben** darf, ist wie folgt zu beantworten: Grundsätzlich gilt das Kommunikationsgesetz.[64] Danach ist jeder Anbieter verpflichtet, seine Teilnehmer bzw. seine Nutzer in *geeigneter Form ausreichend* darüber zu informieren, *welche* Daten er bearbeiten wird, auf *welcher Rechtsgrundlage* und für welche Zwecke dies erfolgt, für wie lange die Daten aufgezeichnet oder gespeichert und für welche *Nutzungsmöglichkeiten* diese allenfalls zugänglich gemacht werden. Diese Information hat spätestens bei Beginn der vertraglichen Beziehung zu erfolgen. Da auch über Nutzungsmöglichkeiten informiert werden muss, ist eine *Bekanntgabe zu Werbezwecken grundsätzlich erlaubt*. Der Nutzer ist jedoch vor der Bearbeitung von Daten zu Werbezwecken zu informieren. Er kann *jederzeit kostenlos* sein *Widerspruchsrecht* geltend machen.[65] Die Information erfolgt normalerweise in den Allgemeinen Geschäftsbedingungen. Diese sind so zu verfassen, dass der Kunde die Einwilligung für den konkreten Fall und in Kenntnis der Sachlage geben kann.[66]

1.4. Gesundheit und Soziales

Im Zusammenhang mit der **Einwilligung der Patienten im Krankenversicherungsbereich**[67] ist eine Beschwerde zu sehen, wonach die von einer Krankenversicherung verwendete formularmässige Einwilligungserklärung sowie *Entbindung vom Arztgeheimnis* angeblich nicht den datenschutzrechtlichen Bestimmungen genügt. Die *Anforderungen* sind in diesem Zusammenhang *hoch* anzusetzen, da es um besonders schützenswerte Daten geht. Die Einwilligung der betroffenen Patienten muss *freiwillig* und aufgrund *ausführlicher Information* seitens des Krankenversicherers in Kenntnis der konkreten und umfassenden Verhältnisse abgegeben worden sein. Pauschale Erklärungen für eine Vielzahl von verschiedenen Fällen entsprechen diesen Voraussetzungen in der Regel nicht. Insbesondere hat der Patient ein Recht darauf zu wissen, an wen seine Gesundheitsdaten gegebenenfalls weitergegeben werden sollen und zu *welchem Zweck*. Nur dann kann eine Einwilligung auch wirksam erteilt werden.

Das **Arztgeheimnis** ist wohl eines der ältesten Berufsgeheimnisse. Es wird jedoch nicht ausnahmslos geschützt. Die Gesetzgebung sieht vor, dass ein Arzt in bestimmten Fällen dazu *berechtigt*, wenn nicht gar verpflichtet wird, Informationen, die auch Gesundheitsangaben umfassen können, an andere bekannt zu geben. In der Praxis stellt sich immer wieder die Frage, wann das Arztgeheimnis *durchbrochen* wird. Die Frage der Ausnahmen von diesem Geheimnis sind insbesondere deshalb wichtig, da eine Verletzung

62. Vgl. Art. 52 Abs. 2 KomG; vgl. ausführlich hierzu Tätigkeitsbericht 2008, 4. Vgl. Legaldefinition in Art. 3 Abs. 1 Ziffer 46 KomG: Verkehrsdaten sind alle Daten, die vor allem zum Zwecke der Weiterleitung einer Nachricht verarbeitet werden, wie insbesondere Teilnehmerdaten, Anrufbeginn, -ende und -dauer.
63. Diese Bereiche umfassen die Speicherung der Verkehrsdaten, die IT-Sicherheit, den logischen Schutz – einschliesslich Authentifizierung und/oder Autorisierung der Prozesse, Protokolldateien, Kryptographie, Zugriffs- und Übergabe-Protokolle, Arbeitsplatzsicherheit – und den physischen Schutz sowie „backup/disaster recovery"-Abläufe.
64. Art. 49 Abs. 4 KomG.
65. Art. 14 Abs. 3 DSG.
66. Ausführlich zur Einwilligung: Dr. Philipp Mittelberger, Die Einwilligung als zentrales Element des Datenschutzrechts, in: Liechtensteinische Juristenzeitung (LJZ) 4/06, S. 136 ff. Für die elektronisch übermittelte Direktwerbung gilt ausserdem die Spezialvorschrift von Art. 50 KomG. Vgl. zu unerwünschter Direktwerbung per E-Mail oben, III., 1.1.2. und Tätigkeitsbericht 2007, 3.1.
67. Vgl. Tätigkeitsbericht 2007, 7.1.

des Berufsgeheimnisses unter Strafe gestellt wird.[68] Da es immer wieder Fragen zu den Ausnahmen des Arztgeheimnisses gegeben hat, haben wir ein *Rechtsgutachten* erstellen lassen. Dieses berücksichtigt verschiedene Gesetze[69] und kommt zum Schluss, dass es folgende Ausnahmen gibt:

- Gemäss Ärztegesetz sowie auch aufgrund des DSG ist eine *Einwilligung* des Patienten zu berücksichtigen, wenn es um Gesundheitsdaten geht, wobei die Einwilligung ausdrücklich sein muss.[70]

- Wiederum gemäss Ärztegesetz liegt eine weitere Ausnahme vor, wenn ein Gesetz dies ausdrücklich vorsieht.[71]

- Als dritte Ausnahme wird der Fall erwähnt, dass es um ein *öffentliches oder berechtigtes privates* Interesse geht. Dabei ist zu berücksichtigen, dass das öffentliche Interesse in der Regel mit einer entsprechenden Gesetzesbestimmung einhergeht. Demgegenüber ist das private Interesse eines Arztes dann zu berücksichtigen, wenn sich ein Arzt in einem Straf- oder Disziplinarverfahren fachgerecht verteidigen oder eine Honorarforderung auf dem Klagesweg durchsetzen soll.

In einem gemeinsamen Schreiben mit der Ärztekammer sowie der Patientenorganisation gelangten wir an die Regierung mit dem Anliegen, dass die **Schaffung eines eigenen Patientengesetzes** in Liechtenstein geprüft wird. Anders als in Liechtenstein kennt etwa der Kanton Zürich ein eigenes Patientengesetz, das beispielsweise die Aufklärung und Information, die Patientendokumentation oder die Einwilligung zur Behandlung regelt. Zwar ist der eine oder andere Tatbestand auch in Liechtenstein in unterschiedlichen Gesetzen geregelt (Ärztegesetz, KVG, etc.), ein einheitliches Gesetz fehlt bislang jedoch. Die Schaffung eines solchen Gesetzes, das auch wichtige datenschutzrechtliche Belange umfasst, wäre bestimmt auch aus Sicht des Patienten zu begrüssen.

1.5. Polizei, Sicherheit und Justiz

Kann ein potenzieller Arbeitgeber einen **Strafregisterauszug** über einen Bewerber beantragen? Dieses Ansinnen ist abzulehnen: Einen Antrag auf einen Strafregisterauszug darf allein die *betreffende Person selbst* – im konkreten Fall also nur der Bewerber – stellen. Ebenso erfolgt eine Zustellung nur an den Antragsteller persönlich. Dies gilt selbst dann, wenn die betreffende Person *ausdrücklich damit einverstanden wäre*, dass wie hier zum Beispiel der zukünftige Arbeitgeber zur Beschleunigung des Bewerbungsverfahrens den Strafregisterauszug selbst anfordern wollte. Auch in diesem Fall darf das Landgericht, dem die Führung des Strafregisters obliegt,[72] den Auszug nur auf Antrag des Bewerbers diesem *persönlich zustellen*. Dass der Bewerber den Strafregisterauszug dann später an den potenziellen Arbeitgeber oder andere Dritte weitergibt, ist datenschutzrechtlich unproblematisch, wenn dies im ausdrücklichen Einverständnis der betroffenen Person geschieht. Umso brisanter ist die Frage, wenn die Person, die den Strafregisterauszug wünscht, in den USA wohnt. Die USA weisen keinen, zum EWR-Raum angemessenen, Datenschutz auf.[73]

Mit *Inkrafttreten der Teilrevision des DSG zum 1. Juli 2009* wurde eine klare **Rechtsgrundlage für die Videoüberwachung im öffentlichen Raum** geschaffen. Grund dafür war, dass die DSK unsere Ansicht im Fall der Videoüberwachung der Fussgängerzone in Vaduz gestützt hatte, wonach eine klare gesetzliche Regelung zu schaffen ist. Die Videoüberwachung im öffentlich zugänglichen Raum ist nunmehr nur nach den abschliessenden Voraussetzungen des Art. 6a DSG zulässig,[74] wobei der Einsatz einer Videoüberwachung durch uns *bewilligt* werden muss. Für bestehende Videoüberwachungsanlagen galt eine gesetzliche Übergangsfrist von sechs Monaten. Während dieser Zeit waren die entsprechenden Anträge auf Genehmigung der Anlagen bei uns ein-

68. § 121 Strafgesetzbuch (StGB).
69. Ärztegesetz, Strafgesetzbuch, Datenschutzgesetz, Krankenversicherungsgesetz, Invalidenversicherungsgesetz, etc.
70. Philipp Mittelberger, Die Einwilligung als zentrales Element des Datenschutzrechts, in: LJZ 4/06, S. 135 ff, FN 37. Dies heisst jedoch wiederum nicht, dass die Einwilligung schriftlich erfolgen muss; eine mündliche Einwilligung genügt.
71. Das Gutachten erwähnt in diesem Zusammenhang wohl als Hauptbeispiele das Krankenversicherungsgesetz, das Invalidenversicherungsgesetz, das Schweizerische Epidemiengesetz und die Schweizerische Meldeverordnung sowie das Strassenverkehrsgesetz.
72. Art. 1 Abs. 2 des Gesetzes vom 2. Juli 1974 über das Strafregister und die Tilgung gerichtlicher Verurteilungen.
73. Zum Datenschutz in den USA im Verhältnis zu Liechtenstein: http://www.llv.li/amtsstellen/llv-dss-datentransfer_ins_ausland/llv-dss-ausland-angemessenheit-ds.htm; und allgemein unter: http://ec.europa.eu/justice_home /fsj/privacy/thridcountries/index_de.htm.
74. Ausgenommen hiervon sind lediglich spezialgesetzliche Bestimmungen, wie zum Beispiel Art. 33 und 34 Polizeigesetz oder Art. 27 der Vorlage zum neuen Geldspielgesetz, vgl. Bericht und Antrag zur Schaffung eines Geldspielgesetzes Nr. 3/2010.

zureichen. Allgemein gingen innerhalb der gesetzlichen Übergangsfrist nicht so viele Anträge ein, wie zu erwarten war. Dies, obwohl wir verschiedene Massnahmen getroffen hatten, um auf dieses Anliegen des Gesetzgebers hinzuweisen.

Die für eine Genehmigungspflicht entscheidenden Kriterien können wie folgt zusammengefasst werden:

- *Erstens* muss die Videoüberwachung einen *öffentlich zugänglichen Raum* betreffen. Öffentlich zugänglich ist ein Raum dann, wenn sich seine Zugänglichkeit nach allgemeinen Merkmalen bestimmt, die von jeder beliebigen Person erfüllt werden können.

- *Zweitens* besteht eine Bewilligungspflicht nur dann, wenn die von der Videoüberwachung gewonnenen Daten Personen *bestimmbar* machen, wenn also über die Bildaufzeichnungen konkrete Personen erkennbar und identifizierbar sind oder über spezifische Merkmale bestimmt werden können.

- *Drittens* muss eine Videoüberwachung *erforderlich*, also geeignet und notwendig sein (Grundsatz der Verhältnismässigkeit). Eine Videoüberwachung in der Nacht ist beispielsweise nur dann geeignet, wenn die technische Ausstattung der Kamera tatsächlich auch verwertbare Bilder in der Dunkelheit machen kann. Notwendigkeit heisst in diesem Sinne, dass die konkrete Videoüberwachung zur Zweckerreichung, z.B. um Vandalismus vorzubeugen, *tatsächlich erforderlich* ist. Insbesondere ist hierbei zu überprüfen, ob nicht andere, *weniger eingreifende* Massnahmen ebenfalls zum Ziel führen würden.

  Eine Videoüberwachungsanlage darf also nur installiert werden, wenn keine anderen Mittel zur Erreichung des Zwecks möglich sind: In einem bestimmten Fall wurde beispielsweise vorgeschlagen, die Videokamera abzubauen und stattdessen eine verbesserte Beleuchtung zu installieren. Dadurch konnte der Schutz des Eigentums bzw. das Schutzempfinden sogar verbessert werden. Auch mit einer örtlichen und/oder zeitlichen Einschränkung von Videoaufzeichnungen kann die Beeinträchtigung in den öffentlichen Bereich merklich reduziert und gleichzeitig dem Schutzbedürfnis entsprechend Rechnung getragen werden.

Umgekehrt bedeuten die oben genannten Voraussetzungen, dass grundsätzlich folgende Videoaufnahmen *nicht* genehmigungspflichtig sind:

- Videoüberwachung für ausschliesslich private oder familiäre Zwecke,

- Bildübermittlungen in Echtzeit ohne Aufzeichnungs- oder weitere Bearbeitungsmöglichkeit,

- Webcams, die ausschliesslich im Rahmen einer privaten Telekommunikation zur Anwendung kommen (z.B. Videotelefonie), und

- Webcams, die als Panorama-, Wetter-, Schnee- oder Objekt-Kameras zwar einen bestimmten Bereich erfassen, durch deren Aufnahmen aber keine Personen bestimmbar sind.

Der Antrag auf Genehmigung einer Videoüberwachungsanlage kann auf unserer Internetseite gestellt werden, wo auch eine *ausführliche Wegleitung als Ausfüllhilfe* verfügbar ist.[75]

Der Gesetzgeber stellt hohe Anforderungen an die Zulässigkeit einer Videoüberwachung, die jeweils im konkreten Fall im Rahmen des Genehmigungsverfahrens von uns zu prüfen sind. Denn die Durchführung einer Videoüberwachung des öffentlichen Raums dient vor allem der Sicherheit. Da sie aber auf eine Vielzahl von unbestimmten Personen ausgerichtet ist, die sich im überwachten Raum bewegen, handelt es sich um einen schweren Eingriff in die persönliche Freiheit. Deshalb können die Rechte auf Achtung der Privatsphäre, der Bewegungs-, Meinungs- und Versammlungsfreiheit nur unter klar festgelegten Voraussetzungen im überwiegenden Interesse der Allgemeinheit eingeschränkt werden.
Der Schwerpunkt der Prüfung auf Zulässigkeit liegt in der Fragestellung der *Notwendigkeit* und *Geeignetheit* zur Erreichung eines bestimmten durch den

75. http://www.llv.li/amtsstellen/llv-dss-videoueberwachung.htm.

Betreiber angestrebten Zwecks sowie der *Prüfung allfälliger alternativer Massnahmen*, bei welchen der Eingriff in die Persönlichkeitsrechte des Betroffenen geringer wiegt. Um gewisse stichhaltige Anhaltspunkte zu haben, ist es bei dieser Beurteilung sehr hilfreich, wenn Protokolle vergangener Vorfälle vorgelegt werden können. Oftmals berufen sich die Antragsteller auf Vorfälle in der Vergangenheit, ohne jedoch eine entsprechende Dokumentation zum Nachweis vorlegen zu können. Die DSK hält jedoch in ihrer Entscheidung zur Videoüberwachung in der Fussgängerzone Vaduz fest, dass es wichtig ist, „detaillierte Aufzeichnungen über strafrechtsrelevante Ereignisse… zu führen, um dadurch die Verhältnismässigkeit der Überwachung und eine allfällige Einschränkung oder Ausweitung der Überwachung darlegen zu können".[76] Solche Aufzeichnungen über Sachbeschädigungen oder andere Vorfälle erleichtern uns die Erteilung einer Bewilligung.

Öffentliche Bereiche, in denen Personen erfahrungsgemäss besonderen Gefahren ausgesetzt sind oder in denen sich Gegenstände von besonderem Wert befinden, dürfen in der Regel videoüberwacht werden. Hierzu zählen beispielsweise Räume mit Schliessfächern, Kassenautomaten, Schalterräume in Banken oder Parkgaragen. Allerdings muss auch hier in jedem Einzelfall die Zulässigkeit im Rahmen des Genehmigungsverfahrens geprüft werden.

Als *generell unzulässig* wird eine Videoüberwachung in Gaststätten, Restaurants oder Cafeterias anzusehen sein, da man sich dort *nicht* nur für eine *kurze Zeit* aufhält. An diesen Orten halten sich Menschen hauptsächlich zur Erholung und zum Konsum von Speisen sowie Getränken auf. Im Allgemeinen wird dort wesentlich lockerer miteinander umgegangen, als das etwa bei beruflichen Tätigkeiten oder privaten Besorgungen der Fall ist. Diese Bereiche sind in der Regel keine Orte, die man nur kurz wegen einer geschäftlichen Tätigkeit aufsucht. Die Menschen haben hier ein besonders schutzwürdiges Interesse daran, dass ihr Verhalten während ihres Aufenthalts in einem Restaurant nicht permanent aufgezeichnet und nachfolgend für eine unbestimmte Zeit vorgehalten wird. Die Interessen der Besucher sind in diesen Fällen in der Regel höher zu bewerten als das Interesse des Antragstellers an einer Videoüberwachung.[77]

Differenziert zu betrachten ist eine Videoüberwachung in der Nachbarschaft. Grundsätzlich unterliegt eine Videoüberwachung im privaten bzw. familiären Bereich zwar keiner Genehmigungspflicht. Die Grenzen sind hier allerdings fliessend, wenn und soweit die Kameras auch den öffentlichen Strassenbereich erfassen. Im Zweifel sollte ein Antrag auf Genehmigung gestellt werden. Ein besonderer Fall liegt insbesondere dann vor, wenn es sich um ein Mehrfamilienhaus handelt, das möglicherweise im Miteigentum mehrerer Personen steht. Hier bedarf es für die Zulässigkeit einer Videoüberwachung den Mehrheitsbeschluss der Miteigentümerversammlung und der Einwilligung aller Mieter.[78]

Wichtig ist es, auf die Videoüberwachung *erkennbar hinzuweisen*. Sollten die Videokameras nicht auf den ersten Blick für alle betroffenen Personen sichtbar sein, müssen entsprechende Hinweisschilder angebracht werden. Tafeln mit einem Hinweis auf die Verantwortlichkeit und den Betreiber dienen einerseits der Abschreckung und geben den Betroffenen andererseits die Möglichkeit, deren Auskunftsrecht beim Betreiber wahrzunehmen. Eine Videoüberwachung kann nur dann sinnvoller Weise von einem widerrechtlichen Handeln abhalten, wenn diese durch die betroffenen Personen auch als solche klar erkennbar ist. Zur leichteren Erkennbarkeit von Fällen der Videoüberwachung im öffentlichen Raum ist ein *offizielles Piktogramm* verfügbar, das bei Erteilung einer Genehmigung verwendet werden darf. Der Vorteil eines solchen Piktogramms besteht insbesondere darin, dass sichtbar ist, dass eine gesetzlich notwendige Bewilligung erteilt wurde. Leider ist ein solches Piktogramm *nicht vorgeschrieben*, sodass es bisher, wohl aus Kostengründen, nicht den erwünschten Anklang gefunden hat.

76. http://www.llv.li/entscheidung_der_datenschutzkommission_zur_videoueberwachung_in_der_fussgaengerzone_in__ vaduz.pdf.
77. Vgl. http://www.saechsdsb.de/informationen-noeb/kontrollpraxis-noeb/82-videoueberwachung-in-gaststaetten.
78. Gesetzliche Grundlage für die Stockwerkeigentümer ist vorwiegend das Sachenrecht (Art. 170g Abs. 1 i.V.m. Art. 26c f. SR) und für die Mieter das Mietrecht (§ 1090 f. ABGB) sowie das Personenrecht (Art. 39 ff PGR).

1.6. Wirtschaft und Finanzen

Mit der letzten Revision des DSG fiel auch der **Vorbehalt des Sorgfaltspflichtgesetzes (SPG)** weg. Bis zum 30. Juni 2009 fand das DSG *keine Anwendung auf Personendaten*, die aufgrund des SPG *anzulegen* waren.[79] Der Wegfall der Ausnahmebestimmung führt dazu, dass im Einzelfall zu prüfen ist, ob eine Datenbearbeitung im Rahmen des SPG mit den Bestimmungen des DSG konform geht. Relevant wird diese Frage zum Beispiel im Zusammenhang mit der Pflicht der Sorgfaltspflichtigen, unter bestimmten Voraussetzungen ein *Geschäftsprofil* zu erstellen oder eine *risikoadäquate Überwachung* einer Geschäftsbeziehung durchzuführen.[80] Hieraus ergibt sich die Frage, welcher Zeitraum abgedeckt werden muss, ob eine entsprechende Datenbearbeitung nur bei Bestehen einer Geschäftsbeziehung, schon bei *Anbahnung* derselben oder sogar unabhängig hiervon allein im Hinblick auf die blosse *Möglichkeit* des Abschlusses einer Geschäftsbeziehung bereits zulässig ist. Die ersten beiden Varianten sind grundsätzlich zu bejahen. Die Bearbeitung von Personendaten eines Vertragspartners in unmittelbarem *Zusammenhang* mit dem Abschluss oder der Abwicklung eines Vertrages ist zulässig.[81] Demgegenüber wird es bei der vagen Möglichkeit, wenn also nichts Konkretes vorliegt, entscheidend von den konkreten Einzelheiten des jeweiligen Falls abhängen.

Die FMA als Aufsichtsbehörde von **Versicherungsunternehmen** kann diese nach Rücksprache mit uns **vom Versicherungsgeheimnis entbinden**.[82] Eine Entbindung ist bei einem näher definierten berechtigten Interesse möglich. Hierzu hatten wir mehrere Anträge datenschutzrechtlich zu überprüfen. Allen Fällen gemeinsam war der *Auslandsbezug*. Es sollten aufgrund grenzüberschreitender Versicherungsverträge jeweils dem Versicherungsgeheimnis unterliegende Personendaten ins Ausland bekannt gegeben werden. Im Gegensatz zum sehr hohen Schutz des Versicherungsgeheimnisses in Liechtenstein besteht je nach Gesetzeslage in anderen Ländern die Gefahr, dass die betreffenden Daten dort *nicht dem selben Schutzniveau* unterliegen. Möglicherweise können die Personendaten, sobald sie einmal im Verfügungsbereich des Empfängerlandes wären, dort zu *verschiedenen Zwecken* weiterverwendet werden. Hier gilt es, eine Abwägung zwischen den Interessen des liechtensteinischen Versicherungsnehmers an einer Entbindung vom Versicherungsgeheimnis, dem Interesse des Versicherungsunternehmens und dem Zweck der infrage stehenden Regelung vorzunehmen.

1.7. Arbeitsbereich

Am Arbeitsplatz können **Interessen** des **Arbeitnehmers** mit Interessen des Arbeitgebers **kollidieren**: zum einen das *Persönlichkeitsrecht und die Treuepflicht* der Beschäftigten, zum anderen insbesondere notwendige Leistungskontrollen, Korruptionsbekämpfung oder Sicherung von Betriebsgeheimnissen.[83] Der Begriff *„Arbeitnehmerdatenschutz"*, der meist verwendet wird, greift unseres Erachtens zu kurz. Es geht nicht um den Schutz des Arbeitnehmers an sich, sondern um den Schutz im Vergleich zu den Interessen des Arbeitgebers. Beim Arbeitnehmerdatenschutz geht es letztendlich also um einen *Ausgleich* zwischen den einschlägigen *Arbeitnehmer- und Arbeitgeberrechten und -interessen*. Der Schutz der Privatsphäre am Arbeitsplatz ist von zentraler Bedeutung für die Identifikation der Mitarbeiter mit ihrem Unternehmen und damit auch für das Betriebsklima. Es ist bekannt, dass die grösste Sicherheitslücke in Unternehmen von Angestellten ausgeht. Dies hat oft mit der Unzufriedenheit von Angestellten zu tun. Um eine solche zu vermeiden, und eben um ein gutes Betriebsklima zu schaffen, ist es wichtig, die *„goldene Mitte"* zu finden.

Europaweit gibt es *kein einheitliches Regelwerk* zum Schutz der Privatsphäre am Arbeitsplatz. Bestrebungen, eine Europäische Arbeitnehmer-Datenschutzrichtlinie auf den Weg zu bringen, liegen seit einer ersten Anhörung des Entwurfs im Jahr 2002 brach.

79. Vgl. Art. 2 Abs. 3 Bst. g DSG. S. auch Tätigkeitsbericht 2008, 2.1.
80. Vgl. Art. 8 ff. SPG.
81. Art. 17 Abs. 2 lit. a DSG.
82. Gemäss Art. 44 Abs. 4 Versicherungsaufsichtsgesetz.
83. Vgl. auch Richtlinien über Internet- und E-Mail-Überwachung am Arbeitsplatz für öffentliche Verwaltungen und Privatwirtschaft:http://www.llv.li/richtlinien_ueber_internet-_und_e-mail-ueberwachung_am_arbeitsplatz.pdf.

In Liechtenstein gibt es kein eigenes Gesetz, die Bestimmungen finden sich verteilt in mehreren Gesetzen.[84] Dies macht es für die Betroffenen in der Praxis mitunter recht schwierig, ihre Rechte zu kennen und entsprechend auszuüben. Wir haben daher damit begonnen, das Thema „*Datenschutz im Arbeitsbereich*" grundsätzlich aufzuarbeiten. Einer der Schwerpunkte wird voraussichtlich die *Überwachung am Arbeitsplatz* sein.

Belange, die den Arbeitsplatz betreffen, sind jedoch nicht nur für uns relevant. Auch dem Amt für Volkswirtschaft obliegen gesetzliche Aufgaben, die datenschutzrechtliche Aspekte tangieren. Während z.B. die Videoüberwachung an öffentlich zugänglichen Orten allein in unsere Zuständigkeit fällt, ist dies bei einem (öffentlich zugänglichen) Arbeitsplatz nicht so. Hier überschneiden sich die Zuständigkeiten. Gemeinsam mit dem Amt für Volkswirtschaft werden wir Berührungspunkte definieren und Merkblätter erarbeiten. Allfällige Kontrollen sollen ebenfalls in Zusammenarbeit erfolgen.

Wie lange ein Unternehmen die **Bewerbungsunterlagen potenzieller Arbeitnehmer aufbewahren** darf, ist nicht präzise geregelt. Dem Arbeitgeber ist es gestattet, Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind.[85] Darüber hinaus wird auf das DSG verwiesen. Der Begriff „Arbeitnehmer" ist *extensiv* auszulegen und umfasst auch potenzielle Arbeitnehmer, also Bewerber. Mangels expliziter Bestimmungen oder Fristen im DSG gilt der allgemeine Grundsatz der *Zweckbindung*, wonach Personendaten „nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde". Konkret bedeutet das, dass die Bewerberdaten so lange aufbewahrt werden dürfen, solange dies für die Erreichung des Zwecks, für den sie behoben wurden, erforderlich ist. Danach sind sie zu *vernichten*[86] oder *zurückzuschicken*.

Der **widerrechtliche Zugriff auf ein Computersystem** oder das missbräuchliche Abfangen von Daten stellen strafrechtliche Tatbestände dar, die in Umsetzung der Cybercrime Convention neu in das liechtensteinische Strafgesetzbuch aufgenommen wurden.[87] Ein Arbeitgeber hatte heimlich am Computer eines Angestellten nach Informationen gesucht, die für letzteren schädlich waren und zur Entlassung des Angestellten führten.[88]

Unternehmen zeichnen manchmal **geschäftliche Telefongespräche** zu Beweissicherungszwecken auf. Bei solchen Praktiken ist es aus Sicht der Privatsphäre wichtig, dass sowohl der Kunde als auch der Mitarbeiter hierüber informiert werden müssen. Der Kunde kann dann allenfalls das Telefongespräch abbrechen, falls er die Aufzeichnung nicht wünscht. In Bezug auf die Mitarbeiter kann auf unsere *Richtlinien zum Thema Internet- und E-Mail-Überwachung am Arbeitsplatz* verwiesen werden.[89] Während ein *Nutzungsreglement*, welches die Nutzung von Internet und Telefon regelt, fakultativ ist, ist ein *Überwachungsreglement* obligatorisch. Der Arbeitgeber sollte darin definieren, zu welchen Zwecken die Überwachung stattfindet. Wesentlich ist zudem eine Trennung von privaten und geschäftlichen Gesprächen. Beispielsweise könnten private Gespräche am Telefon mit einer anderen Vorwahltaste als geschäftliche Gespräche geführt werden. Was die *Einwilligung* von Mitarbeitern angeht, ist diese im *Einzelarbeitsvertragsrecht irrelevant*, da der Arbeitnehmer in einer *schwächeren* Position ist.[90] Genau eine solche Einwilligung der Beteiligten ist aber paradoxerwei-

84. Insbesondere Art. 27 Abs. 1 (allgemeiner Persönlichkeitsschutz) und Art. 28a des Einzelarbeitsvertragsrechts (Datenbearbeitung im Arbeitsverhältnis); Art. 62 ff. ArGV I (Datenbearbeitung durch Aufsichtsbehörde); Art. 8 Abs. 1, Art. 59 der Verordnung über die Sicherheit und den Gesundheitsschutz der Arbeitnehmer am Arbeitsplatz (Überwachung am Arbeitsplatz).
85. Nach Art. 28a des Einzelarbeitsvertragsrechts.
86. Art. 19a DSG sieht vor, dass Personendaten zu vernichten sind, wenn sie nach Erreichung der Zwecke, für die sie bearbeitet wurden, nicht mehr benötigt werden.
87. Vgl. III. 4.5.
88. Das revidierte StGB ist seit September in Kraft. Vgl. dazu den Vernehmlassungsbericht: http://www.llv.li/pdf-llv-rk_vernehml_2008_abaenderung_stgb_cyber_crime.pdf, auf Seite 13 ff.
89. http://www.llv.li/richtlinien_ueber_internet-_und_e-mail-ueberwachung_am_arbeitsplatz.pdf.
90. Art. 28a des Einzelarbeitsvertragsrechts nach § 1173a ABGB.

se notwendig, wenn ein fremdes, nicht-öffentliches Gespräch mit einem Abhörgerät abgehört oder auf einem Tonträger aufgenommen wird.[91] Zu beachten ist ausserdem, dass der Arbeitgeber einen *konkreten Zweck* definiert, dass die *Daten sicher aufbewahrt* bzw. *beschränkt zugänglich* sind und dass es *nicht zu einer Verhaltensüberwachung* kommt.

1.8. Datenbekanntgabe im Inland

Bei der **Bekanntgabe von Personendaten zwischen Behörden** ist einerseits das *Amtsgeheimnis* und andererseits die *Amtshilfe* zu berücksichtigen. Vereinfacht ausgedrückt besteht der Sinn der Amtshilfe darin, Informationen an eine andere Amtsstelle zu geben, um deren Arbeit zu erleichtern. Voraussetzung ist die gesetzliche Erlaubnis hierfür. Behörden dürfen grundsätzlich nur das tun, wozu sie gesetzlich befugt sind.[92] Dieses *Gesetzmässigkeitsprinzip* führt dazu, dass es sehr viele Bestimmungen gibt, die entweder eine Schweigepflicht, eine Datenbearbeitung, eine Datenbekanntgabe oder, allgemein formuliert, eine Amtshilfe vorsehen.[93] Doch was gilt, wenn sich eine Behörde auf eine Amtshilfe- oder Datenbekanntgabebestimmung beruft, die andere dagegen auf eine ausdrückliche Schweigepflicht? Wie ist die allgemeine Amtshilfebestimmung[94] zu interpretieren? Solchen Fragen wurde in einem *Rechtsgutachten* nachgegangen, das wir in Auftrag gegeben hatten.

Die Idee des Datenschutzes besteht darin, dass ein Schutz nur dort greifen soll, wo er gerechtfertigt ist. Mit anderen Worten sollen Daten fliessen, wenn dies notwendig ist. Das Rechtsgutachten ging auch der Frage nach, unter welchen Umständen die Bekanntgabe von besonders schützenswerten Personendaten möglich ist. Wir haben die Erkenntnisse des Gutachtens noch nicht ausgewertet, werden dies aber sobald wie möglich tun.

Die **Übermittlung von Fotos** eines Jahrgängertreffens an die Presse zur Publikation kann mit der Bekanntgabe von *vereinsinternen Mitgliederlisten* verglichen werden.[95] Die betroffenen Personen sollten auf diesen Umstand aufmerksam gemacht werden, sodass sie einwilligen können.

1.9. Datenbekanntgabe mit Auslandsbezug

Inwieweit **liechtensteinische Unternehmen gegenüber ausländischen Behörden** zur Auskunft verpflichtet sind (z.B. über Mitarbeiter), hängt vom konkreten Fall ab. Problematisch ist diese Fallkonstellation vor allem in den Fällen, in denen das ausländische mit dem inländischen Recht kollidiert. Auch wenn aufgrund der ausländischen Gesetzeslage eine Pflicht zur Auskunftserteilung bestünde (z.B. im Steuerrecht des betreffenden Staates), heisst das umgekehrt noch nicht, dass dem auch nach liechten-

91. Art. 1 des Gesetzes über den strafrechtlichen Schutz des persönlichen Geheimbereichs. Vgl. auch Art. 179bis des Schweizer Strafgesetzbuches. Zum Ganzen: Erläuterungen zur Telefonüberwachung am Arbeitsplatz des Eidgenössischen Datenschutzbeauftragten, S. 4: http://www.edoeb.admin.ch/themen/00794/00917/index.html?lang=de&download=M3wBP gDB/8ull6Du36WenojQ1NTTjaXZnqWfVpzLhmfhnapmmc7Zi6rZnqCkkIN0fXaEbKbXrZ6lhuDZz8mMps2gpKfo.
92. Grundsätzlich dürfen Behörden also nur dann Personendaten bekannt geben, wenn dafür eine Rechtsgrundlage besteht. Hier stellt sich die Frage, wie diese Rechtsgrundlage ausgestaltet sein muss. Bei einfachen Personendaten, wie z. B. Name oder Geburtsdatum, genügt das Vorliegen eines Gesetzes im materiellen Sinn (Es ist zu unterscheiden zwischen einem materiellen und einem formellen Gesetz. Ein Gesetz im materiellen Sinn ist im Rang niedriger als ein formelles Gesetz. Ein Gesetz im materiellen Sinn kann zum Beispiel eine von der Regierung erlassene Verordnung sein, während sich ein Gesetz im formellen Sinn dadurch auszeichnet, dass es vom Landtag verabschiedet worden sein muss. Diesen Unterschied in der Wertigkeit übernimmt das DSG im Zusammenhang mit der Bekanntgabe von Personendaten von Behörden.) Bei einer Bekanntgabe von besonders schützenswerten Personendaten und Persönlichkeitsprofilen, zu denen insbesondere Gesundheitsdaten zählen, ist hingegen ein Gesetz im formellen Sinn Voraussetzung für eine zulässige Datenbekanntgabe (Vgl. III. 1.1.1 und 1.4.). Dass es einer ausdrücklichen gesetzlichen Grundlage bedarf, vertritt auch das vorgehend zitierte Rechtsgutachten zum Amtsgeheimnis. Aus datenschutzrechtlicher Sicht genügt daher der Abschluss einer Verwaltungsvereinbarung beispielsweise, also eines einfachen Vertrags zwischen Behörden, nicht den Anforderungen an ein formelles Gesetz. Darüber hinaus müssen Behörden gemäss Art. 14 des Informationsgesetzes die Öffentlichkeit über Tätigkeiten von allgemeinem Interesse informieren, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen. Welche Tätigkeiten im konkreten Fall hierunter fallen, ist nicht immer einfach zu entscheiden, da auch das Amtsgeheimnis und die Bestimmungen des Datenschutzes gelten. Vor allem wenn es um Einzelfallentscheidungen im Rahmen verwaltungsrechtlicher Verfahren geht, die für bis dahin unbeteiligte Dritte von Bedeutung sein könnten, ist zu hinterfragen, wer neben den unmittelbar Beteiligten ausserdem informiert werden darf oder sogar muss. Mitunter geben spezialgesetzliche Regelungen im Einzelnen vor, welche Stellen in Kenntnis zu setzen sind. Gibt es solche Vorschriften nicht, ist auf die allgemeinen Grundsätze zurückzugreifen. Hier ist dann von Fall zu Fall zu entscheiden, ob zum Beispiel ein anderes Amt, Nachbarn oder gegebenenfalls auch ein Anzeigeerstatter zu informieren ist.
93. Die Amtshilfe ist in Art. 25 des Landesverwaltungs-Pflegegesetzes (LVG) geregelt; das Amtsgeheimnis dagegen in Art. 38 des Staatspersonalgesetzes (StPG); ausdrückliche gesetzliche Schweigepflichten sind z.B. im Sozialhilfegesetz oder im Invalidenversicherungsgesetz (IVG) zu finden.
94. Art. 25 LVG.
95. Vgl. dazu auch Tätigkeitsbericht 2008, 2.2.

steinischem Recht so wäre. Möglicherweise unterliegen die infrage stehenden Informationen nach liechtensteinischem Recht einer Geheimhaltungspflicht wie z.B. dem Versicherungsgeheimnis und die Privatsphäre des betroffenen Arbeitnehmers würde bei einer Bekanntgabe verletzt. Diese Prüfung können die angefragten Unternehmen in der Regel kaum selbst vornehmen. Daher ist in diesen Fällen den Unternehmen zu raten, die *ausländischen Behörden auf den Amts- oder Rechtshilfeweg zu verweisen*. Dann müssten die in Liechtenstein zuständige Aufsichtsbehörde oder das zuständige Gericht zunächst die Zulässigkeit des Ansuchens nach nationalem Recht beurteilen. Nur wenn diese zu bejahen ist, wären die betroffenen Unternehmen in dem vorgegebenen Umfang zur Auskunftserteilung verpflichtet, ohne dass sie dabei Gefahr liefen, etwaige Geheimhaltungs- oder Datenschutzrechte zu verletzen.

Für international tätige Konzerne, die regelmässig grenzüberschreitend Personendaten bearbeiten, ist der **Abschluss von einzelvertraglichen Datenschutzvereinbarungen oder verbindlichen unternehmensinternen Datenschutzregelungen**[96] eine zu empfehlende Regelung, um eine angemessene und einheitliche Datenbearbeitung zu gewährleisten. Werden diese Vereinbarungen getroffen, um Datentransfers in sogenannte Drittländer zu regeln, so müssen diese seit Inkrafttreten der letzten Teilrevision des DSG von der Regierung vorab genehmigt werden.[97] Im Rahmen dieses Genehmigungsverfahrens fordert uns das Ressort Justiz auf, innerhalb einer Frist von 30 Tagen eine Stellungnahme abzugeben, ob die Garantien oder einheitlichen Datenschutzregelungen einen angemessenen Schutz im Sinne des liechtensteinischen DSG gewährleisten. Die Genehmigung hat für den Datentransfer in das betreffende Drittland konstitutive Wirkung, das heisst, erst mit Vorliegen der Genehmigung dürfen die Personendaten zulässiger Weise in das betreffende Drittland bekannt gegeben werden.

Die Bekanntgabe von **Autohalterdaten an ausländische Behörden** ist kein neues Thema.[98] Es ist bekannt, dass liechtensteinische Autohalter bei *Verkehrswidrigkeiten Bussen aus der Schweiz direkt* zugeschickt bekommen. Dies hat unter anderem damit zu tun, dass *liechtensteinische* und *Schweizer Bundesbehörden teils mit denselben Datenbanken* arbeiten. Generell ist eine solche Bekanntgabe zulässig, wenn und soweit sie entsprechend gesetzlich vorgesehen wird: Eine Bekanntgabe von Daten liechtensteinischer Fahrzeughalter zum Beispiel in die Schweiz wird in verschiedenen Gesetzen geregelt.[99]

In diesem Zusammenhang ist eine neue Entwicklung zu beobachten. *Ausländische Behörden* in der EU gehen dazu über, *private Firmen im Ausland* mit der Zustellung und Betreibung von *Verkehrsbussen* zu beauftragen.[100] Die MFK erhielt insofern wiederholte Anfragen aus dem Ausland, dass sie Adressen von betroffenen Personen an ein solches Unternehmen bekannt geben sollte, damit letztere diesen einen Bussgeldbescheid zustellen können. Grundsätzlich sieht das liechtensteinische Strassenverkehrsgesetz vor, dass die MFK einer Person, die ein *hinreichendes Interesse glaubhaft* machen kann, die Namen von Fahrzeughaltern und ihre Versicherer bekannt geben muss.[101] Es obliegt der Prüfung der *MFK*, ob ein hinreichendes Interesse vorliegt. Ausserdem sollte bei der Prüfung berücksichtigt werden, ob die anfragende Stelle aufgrund einer *ordnungsgemässen Vollmacht* der zuständigen nationalen Behörden überhaupt bevollmächtigt ist und ob die eigentlich zuständigen Behörden aufgrund eines Gesetzes berechtigt sind, die Halterdaten anzufragen.

96. Grundsätzliche Ausführungen zu verbindlichen unternehmensinternen Datenschutzregelungen (Binding Corporate Rules, BCR) s. Tätigkeitsbericht 2008, 2.3. und 10.2.1.
97. Art. 8 Abs. 2 Bst. a und Art. 8 Abs. 3 DSG. Zuständig für die Erteilung der Genehmigung ist das Ressort Justiz, Art. 6 Abs. 1 DSV.
98. Tätigkeitsbericht 2007, 4.1., zur Bekanntgabe von liechtensteinischen Autohalterdaten an österreichische Behörden.
99. Als mögliche Rechtsgrundlagen können unter anderem in Betracht kommen: Art. 4 Abs. 4 Bst. a und Art. 6 des trilateralen Polizeikooperationsvertrags (vgl. dazu auch BuA Nr. 77/2000, S. 17 zu Art. 6); Art. 10 des Internationalen Kraftfahrübereinkommens (Pariser Abkommen) von 1926, LGBl. 1931 Nr. 9; Art. 104a CH-SVG (SR 741.01) bzw. Art. 99 Abs. 10 und Art. 99b FL-SVG (LGBl. 1978 Nr. 18) in Verbindung mit der Verwaltungsvereinbarung zwischen Liechtenstein und der Schweiz über die Beteiligung Liechtensteins an der Führung und Nutzung von automatisierten schweizerischen Registern im Strassenverkehrsbereich, LGBl. 2006 Nr. 209 (LR 0.741.531.910.13).
100. Vgl. dazu auch Tätigkeitsbericht 2008, 2.3.
101. Art. 99b Abs. 4 SVG.

2. Öffentlichkeitsarbeit

Die Sensibilisierung der Öffentlichkeit für Themen rund um den Schutz der Privatsphäre gehört zu unseren **Kernaufgaben**. Nicht zuletzt unsere Online-Umfrage[102] vom vergangenen Jahr hat gezeigt, dass der Informationsbedarf gemeinhin nach wie vor gross ist. Um möglichst weite Kreise der Bevölkerung zu erreichen, nutzen wir *unterschiedliche Kanäle* und setzen auf ein *Bündel von Massnahmen*. Neben Veranstaltungen, Schulungen, Publikationen und unserer Internetseite gehört auch der gegenständliche Tätigkeitsbericht zu den zentralen Informationsmassnahmen.[103]

2.1. Veranstaltungen

Am 28. Januar, dem Europäischen Datenschutztag, veranstalteten wir in Zusammenarbeit mit dem Institut für Wirtschaftsinformatik der Hochschule Liechtenstein erstmals eine öffentliche Veranstaltung unter dem Titel **„Denn sie wissen nicht, was sie tun?! - Soziale Netzwerke unter der Lupe"**.[104] Ziel war es, auf die Privatsphäre im Zusammenhang mit der Nutzung sozialer Netzwerke aufmerksam zu machen: Das Internet ist mit einer Revolution vergleichbar, es hat das Alltagsleben stark verändert. Auch Freizeittätigkeiten werden von den Möglichkeiten teils stark beeinflusst und können sich von der realen in eine virtuelle Welt verlagern. Zum Beispiel vereinfachen soziale Netzwerke, wie *facebook*[105], *Xing*[106], *LinkedIn*[107] , *studiVZ*[108] *oder MySpace*[109], die Vernetzung und den Austausch von Informationen. Soziale Netzwerke sind sehr beliebt, was durch stark steigende Nutzerzahlen verdeutlicht wird.[110]

Da Anbieter *sozialer Netzwerkedienste* (englisch *social network services*) in der Regel keine Gebühren für die Nutzung des Dienstes verlangen, sind die Profil- und somit die persönlichen Nutzerdaten das einzige Kapital. Die technische Infrastruktur sowie die Programmierer der Dienste müssen bezahlt werden. Hier hat sich die gebräuchliche Art der Finanzierung mittels zielgerichteter Werbung und Verkauf der Nutzerdaten offensichtlich durchgesetzt. Die Nutzung sozialer Netzwerke ist *nicht kostenlos*. Die Nutzer *bezahlen mit ihrer Privatsphäre bzw. ihren persönlichen Daten*. Daher ist eine sparsame und zurückhaltende Bekanntgabe persönlicher Informationen geboten. Ein informeller Umgangston zwischen „Freunden" sowie einfache Möglichkeiten der Vernetzung vermitteln den Eindruck von Privatsphäre – „Das wissen *nur* meine Freunde!". In sozialen Netzwerken gibt es jedoch keine zur Gänze abgeschlossenen Gemeinschaften, die mit der Realwelt vergleichbar wären. Sämtliche Fotos und Inhalte werden durch den Plattformbetreiber in den USA, der primär amerikanischem Recht unterstellt ist, verwertet und können unter Umständen nach Belieben im Internet öffentlich zugänglich gemacht werden.

Die Verwendung eines *Pseudonyms sowie die Verfremdung des eigenen Fotos* sind keine Zeichen von Unhöflichkeit. Durch die Verwendung verschiedener E-Mail-Adressen bei der Anmeldung zu sozialen Netzwerkdiensten wird das Verknüpfen der jeweiligen Profile erschwert. Für die jeweilige Plattform kann auf diese Weise durch den Nutzer eine soziale Rolle festgelegt und die Inhalte entsprechend gestaltet werden (z.B. StudiVZ als Student und bei LinkedIn als Angestellter).

Soziale Netzwerke lassen die „*reale Welt*" mit der „*virtuellen Welt*" verschmelzen, wodurch neue Gefahren für die Privatsphäre entstehen. Wir beobachten die Entwicklungen laufend und informieren auch direkt auf Facebook[111] über aktuelle Themen rund um diese Thematik.

Ebenfalls an der Hochschule informierten wir Studenten des Master-Studiengangs **Business Process Engineering** der Wirtschaftsinformatik. Neben einer

102. Vgl. unter II.3.
103. Gemäss Art. 31 DSG.
104. http://www.llv.li/amtsstellen/llv-dss-datenschutztag/llv-dss-datenschutztag-archiv.htm.
105. http://www.facebook.com/.
106. http://www.xing.com.
107. http://www.linkedin.com.
108. http://www.studivz.net/.
109. http://www.myspace.com.
110. http://www.facebakers.com/countries-with-facebook/.
111. http://www.facebook.com/pages/Vaduz/Datenschutzstelle-Liechtenstein/364340615234.

juristischen Einleitung und der 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.

Die Videoüberwachung im öffentlichen Raum wird in Liechtenstein immer wieder diskutiert. Der Verein Sicheres Liechtenstein (VSL)[112] veranstaltete eine Podiumsdiskussion zum Thema **„Freiheit vs. Sicherheit?"**, auf der wir die Anliegen der Privatsphäre darstellten. Der Charme Liechtensteins ist eng mit der Gestaltung des öffentlichen Raums verknüpft. Zahlreiche Strassen und Plätze prägen mit unterschiedlichen sozialen Qualitäten das Gesicht des Landes. Frei zugänglich für alle, bieten diese öffentlichen Bereiche Raum für Aufenthalt, Begegnung, Bewegung und Erholung. Niemand würde sich generell gegen Vorschläge zur *Förderung der Sicherheit im öffentlichen Raum* wenden. Die Sicherheit hat auch etwas mit intelligenter Planung, psychologisch richtiger Gestaltung, Nutzungsmischung, Nachbarschaftsförderung, Ordnung, Wohlbefinden, Sauberkeit und Pflege zu tun. *Sicherheitsfragen* können möglicherweise nur zum Teil mit gestalterischen Mitteln gelöst werden. Auf der anderen Seite wird die Überwachung des öffentlichen Raums mit Videokameras in zahlreichen Städten ausgebaut. Nicht nur in Vaduz wird über den vermehrten Einsatz von Videokameras im öffentlichen Raum zum *Schutz vor Vandalismus und Gewalt* gesprochen. Der Einsatz von Videokameras im öffentlichen Raum ist aber umstritten. Sowohl die Sicherheit, als auch der Datenschutz und das subjektive Sicherheitsempfinden spielen in Liechtenstein in vielen Lebensbereichen eine bedeutende Rolle. Im Rahmen einer *Podiumsdiskussion* mit Vertretern der Hochschule Liechtenstein, der Gemeinde Vaduz und der DSS wurde aufgezeigt, wie in Liechtenstein ein qualitatives Nebeneinander zwischen gestalterischen Möglichkeiten und dem Ruf nach mehr Überwachung funktionieren kann.

2.2. Neuigkeiten auf der Internetseite

Auf unserer **Internetseite** „www.dss.llv.li" informieren wir regelmässig über aktuelle Themen, die für die Öffentlichkeit relevant sind. Dies geschieht in der Regel *einmal pro Monat*.

Wir haben beispielsweise über unsere Veranstaltung anlässlich des Datenschutztages berichtet. Nennenswert sind auch die *Online-Umfrage über Datenschutz* oder das *Inkrafttreten neuer Datenschutzbestimmungen*. Weiters haben wir *internationale Entwicklungen* thematisiert, wie die Entscheidung der belgischen Datenschutzkommission in der „*SWIFT-Affäre*". Einige Dokumente haben wir auf diese Weise einer breiten Öffentlichkeit zugänglich gemacht. Als Beispiele sind die *Stellungnahme* 1/2008 zu Datenschutzfragen im Zusammenhang mit *Suchmaschinen der Art. 29 Datenschutzgruppe*, der Tätigkeitsbericht der Gemeinsamen Kontrollinstanz Schengen über den Zeitraum Dezember 2005 bis 2008 oder der Leitfaden der Art. 29 Datenschutzgruppe für Anbieter und Nutzer sozialer Netzwerke zu nennen.

Von unseren eigenen Aktivitäten sind zwei **Mustervorlagen für Geheimhaltungs- und Datenschutzvereinbarungen** nennenswert, die neu über unsere Internetseite oder die Online-Formularlösung der Landesverwaltung[113] heruntergeladen werden können. Diese Vorlagen sind dafür gedacht, ergänzend zu den verschiedensten Verträgen herangezogen zu werden. Aus diesem Grund sind sie sehr *allgemein formuliert*; Anpassungen an den konkreten Fall sind jeweils gesondert vorzunehmen. Sinnvoll ist eine Verwendung von gesonderten Geheimhaltungs- und Datenschutzvereinbarungen vor allem dann, wenn *besonders viele oder besonders schützenswerte Daten* für eine Vertragserfüllung ausgetauscht werden müssen. Dies ist beispielsweise bei *Gutachtenaufträgen* im *Gesundheitsbereich* oder in der *Personalverwaltung* der Fall.

112. http://vsl.li/.
113. http://www.llv.li/form-llv-dss-mustervorlagen.

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 Verfahrensstadion* einbezogen werden. Insgesamt gaben wir zu 34 Gesetzesvorhaben in verschiedenen Stadien des Gesetzgebungsverfahrens eine Stellungnahme ab. Exemplarisch soll im Folgenden aufgrund besonderer datenschutzrechtlicher Relevanz nur auf ein paar wenige Gesetzesvorhaben näher eingegangen werden:

Das Vernehmlassungsverfahren betreffend die Revision des **Kommunikationsgesetzes** (KomG) nahmen wir zum Anlass, unsere grundsätzlichen Bedenken gegenüber den geltenden Bestimmungen zu den *Mitwirkungspflichten der Anbieter im Bereich der elektronischen Kommunikation*[114] zu äussern. Hierbei geht es insbesondere um *die sechsmonatige Vorratsdatenspeicherung von Verkehrsdaten*.[115] Die Regierung hat unsere Kritik, die sich teils auf ein von uns in Auftrag gegebenes Rechtsgutachten stützte,[116] zum Anlass genommen, die einschlägigen Regelungen im Interesse einer bürger- und grundrechtsfreundlichen Ausgestaltung nochmals zu überarbeiten und für den Zugriff auf bzw. die Verwertung von auf Vorrat gespeicherten Daten strenge Voraussetzungen zu normieren.[117] So ist beispielsweise vorgesehen, den *Richtervorbehalt ausnahmslos* vorzuschreiben. Ausserdem hat die Regierung nun vorgesehen,[118] dass eine umfassende *Kontrolle des Datenschutzes und der Datensicherheit* durch uns eingeführt werden soll. Die Kontrolle umfasst die Personendaten, die zum Zweck der Mitwirkung bei einer Überwachung bearbeitet werden, und soll sicherstellen, dass keine missbräuchliche Bearbeitung von Inhalts- und/oder Verkehrsdaten durch die betreffenden Anbieter oder durch die zuständigen Behörden stattfindet.[119] Die Revision war zum Ende des Berichtsjahres noch nicht abgeschlossen.

Im Zusammenhang mit dem **Beitritt zu den Abkommen von Schengen und Dublin**[120] war seitens der Landespolizei die sogenannte *N-SIS-Verordnung* zu erstellen, bei der wir mitarbeiten konnten. Diese regelt den nationalen Teil des Schengen Informationssystems (SIS). Sie setzt den für den Betrieb des SIS notwendigen rechtlichen Rahmen, regelt die Zuständigkeiten unter den jeweiligen Behörden sowie die Rechte der Betroffenen. Gemeinsam mit den Bestimmungen des Schengen Durchführungsübereinkommens und des SIRENE[121]-Handbuchs stellt sie die Grundlage für den Betrieb des SIS in Liechtenstein dar. Zentral aus Datenschutzsicht ist dabei, dass die Rechte der betroffenen Personen gebührend berücksichtigt werden.

Wenngleich der Beitritt Liechtensteins zum Schengenraum noch nicht erfolgt ist, muss bereits im Vorfeld der sogenannten *Weiterentwicklung des Schengen-Besitzstandes* Rechnung getragen werden. Diesbezüglich ist beispielsweise die *Schwedische Initiative*[122] zu nennen, für deren Umsetzung eine Abänderung des Polizeigesetzes notwendig wurde. Der Umfang des polizeilichen Informationsaustausches soll durch die Einführung des vereinfachten Verfahrens zwischen Liechtenstein und den Schengen-Staaten gegenüber dem bisher geltenden Recht nicht verändert werden.[123] In Liechtenstein ist der Rahmenbeschluss daher spätestens bis zum Inkrafttreten der Schengen Assoziierung in das nationale Recht umzusetzen.[124]

114. Art. 51 ff KomG.
115. Bericht und Antrag Nr. 110/2009, S. 105 ff.
116. Vgl. dazu Tätigkeitsbericht 2008, 4; Dr. Hilmar Hoch: Die Regelung des staatlichen Zugriffs auf Fernmeldedaten im Kommunikationsgesetz aus grundrechtlicher Sicht, in: Liechtensteinische Juristen Zeitung (LJZ), 12/2009, S. 99 ff: http://www.juristenzeitung.li/essays/show/id/147.
117. Bericht und Antrag Nr. 110/2009, S. 113.
118. Art. 52b KomG (neu) der Vorlage gemäss BuA 110/2009.
119. Bericht und Antrag Nr. 110/2009, S. 118.
120. S. II. 2.
121. Supplementary Information Request at the National Entry.
122. Rahmenbeschluss 2006/960/JI über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden.
123. Vgl. Vernehmlassungsbericht betreffend Abänderung des Polizeigesetzes (vereinfachter Informationsaustausch), S. 23.
124. Vgl. Vernehmlassungsbericht betreffend Abänderung des Polizeigesetzes (vereinfachter Informationsaustausch), S. 6.

Weiters haben wir zu folgenden Gesetzesprojekten eine Stellungnahme abgegeben:

- Abänderung Datenschutzverordnung;
- Abänderung Statistikverordnung;
- Gesetz über die Geoinformationen;
- Gesetz über die Glücks- und Geschicklichkeitsspiele;
- Gesetz über das Hochschulwesen;
- Gesetz über den Umgang mit Organismen;
- Heimatschriftengesetz;
- Patientenverfügungsgesetz;
- Personenfreizügigkeitsgesetz;
- Polizeigesetz;
- Steuergesetz;
- Strafgesetzbuch;
- Strafprozessordnung;
- Tierschutzgesetz und Hundegesetz;
- UNO-Konvention gegen das Verschwindenlassen von Personen;
- US-Amtshilfegesetz;
- Versicherungsaufsichtsgesetz;
- Zusatzprotokoll zum Datenschutzübereinkommen.

4. Internationale Zusammenarbeit

4.1. Art. 29 Datenschutzgruppe

Die Art. 29 Datenschutzgruppe[125] beschäftigt sich mit aktuellen und *wichtigen Themen im Datenschutz*, die von allgemeiner Bedeutung sind. Von den insgesamt **elf verabschiedeten Dokumenten**[126] ist allen voran der Beitrag **„Die Zukunft des Datenschutzes"**[127] zur Konsultation der Europäischen Kommission zum Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten (WP 168) zu nennen. Diese wichtige Stellungnahme wurde gemeinsam mit der Working Party on Police and Justice[128] abgegeben. Sie geht auf elementare Aspekte des Datenschutzes ein, wie beispielsweise auf Folgende:

- Zum Thema *Globalisierung*[129] wird insbesondere festgehalten, dass in der EU der Datenschutz Verfassungsrang innehat. Zur Wahrung dieser Bedeutung auch auf globaler Ebene sollten Bestrebungen angegangen werden, diesen hohen Schutz in andere Regionen der Welt zu „exportieren", sei dies durch Überdenken des Konzeptes der Angemessenheit, der Entwicklung internationaler globaler Standards, dem Abschluss internationaler Abkommen oder auch durch verbindliche unternehmensinterne Datenschutzregeln.

- Was *technologische Änderungen* angeht, wird festgestellt, dass diese die Risiken für die Privatsphäre des Einzelnen erhöhen. Als Gegengewicht zu diesen Risiken sollte der Grundsatz *„privacy by design"* eingeführt werden, um bei der Planung von Informations- und Kommunikationstechnologien der Privatsphäre und dem Datenschutz Rechnung zu tragen.

- Weiters werden die Rollen der verschiedenen Akteure diskutiert: Die Stärkung der *Rechte der betroffenen Personen* wird z.B. im Hinblick auf das Internet gefordert oder die Möglichkeit der Stärkung der Einwilligung oder allgemein eine Verbesserung des Rechtsschutzes. Parallel dazu sollte die Verantwortung der Dateninhaber verstärkt werden, indem ein Grundsatz der Rechenschaftspflicht oder erforderliche interne Mechanismen zur Sicherstellung der Einhaltung der Grundsätze und Verpflichtungen eingeführt werden können.

- Was die *Rolle der nationalen Datenschutzbehörden* betrifft, wird festgestellt, dass es derzeit grosse Unterschiede zwischen den Mitgliedsstaaten in Bezug auf Ressourcen und Befugnisse gibt. Diesbezüglich wird im Hinblick auf einen möglichen neuen Rechtsrahmen eine strikte, einheitlichere und effektive Überwachung durch die Daten-

125. Die sogenannte Art. 29 Datenschutzgruppe ist das Gremium der unabhängigen Datenschutzbehörden des EWR, benannt nach Art. 29 der Datenschutzrichtlinie 1995/46/EG. Die DSS hat in diesem Gremium einen Beobachterstatus.
126. Die Dokumente (englisch Working Papers, WP) können über das Internet abgerufen werden unter: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_de.htm.
127. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_de.pdf.
128. Vgl. III. 4.5.
129. In diesem Sinne äusserte sich auch Christian Batliner anlässlich der Lesung des Berichts und Antrags Nr. 82/2009 betreffend das Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung, S. 1919 ff, in dem er aufgrund der zunehmenden Globalisierung eine Steigerung des grenzüberschreitenden Datentransfers und Handlungsbedarfs in Bezug auf die Harmonisierung der Zuständigkeiten der Aufsichtsbehörden und den Erlass gesetzlicher Regelungen zur Vermeidung einer Umgehung des Datenschutzes sah. Mit der Ratifikation des Zusatzprotokolls würde das vom Europarat festgelegte Datenschutzniveau eingehalten, was wiederum im Hinblick auf den bevorstehenden Schengen-Beitritt elementar ist.

schutzbehörden gefordert. Die Verhängung von Geldbussen bei Verstössen gegen das Gesetz ist ein Element.

In der Stellungnahme über die Vorschläge zur Änderung der *Datenschutzrichtlinie für die elektronische Kommunikation* (WP 159) begrüsst die Arbeitsgruppe den Vorschlag der Einführung einer Bestimmung betreffend Sicherheitsverletzungen durch Anbieter öffentlich zugänglicher Kommunikationsdienste, da derartige Meldungen zu einem wichtigen Instrument der Datenschutzbehörden werden können, um die Verpflichtung, geeignete Sicherheitsmaßnahmen zu ergreifen, besser und wirksamer durchzusetzen. Auch dies könnte sich auf die Aufgaben der Datenschutzbehörden, und somit auch auf unsere, auswirken.

Besonders hervorzuheben ist die *Stellungnahme zur Nutzung sozialer Online-Netzwerke*. Diese Stellungnahme (WP 163)[130] geht der Frage nach, wie das Betreiben sozialer Netzwerkdienste mit den Bestimmungen des Datenschutzrechts in Einklang zu bringen ist. Darin wird klar ausgedrückt, dass die Zweckentfremdung bzw. die anderweitige Nutzung von Informationen, die über soziale Netzwerkdienste verfügbar sind, zu den besorgniserregenden Sicherheitsbedenken der Art. 29 Datenschutzgruppe gehört. Die *Nutzerzahlen nehmen weiter exponentiell zu*, wobei die sozialen Netzwerkdienste einen Grossteil ihrer Einnahmen mit gerichteter Werbung finanzieren. Das gegenständliche Arbeitspapier gibt Antworten und Empfehlungen zur Verantwortlichkeit der Datenverarbeitung, für sicherheits- und datenschutzfreundliche Standardeinstellungen sowie den Informationspflichten des Dienstanbieters. Insbesondere empfiehlt die Stellungnahme den Nutzern beispielsweise, Bilder bzw. jede Information über andere Personen nur mit deren konkreten Einwilligung in ein soziales Netzwerksystem herunterzuladen oder zu veröffentlichen.

Weiters zu nennen ist die *Zweite Stellungnahme zum Schutz personenbezogener Daten von Kindern* (WP 160)[131] oder die Stellungnahmen zur Angemessenheit des Datenschutzes in Andorra (WP 166) und Israel (WP 165). Diese Stellungnahmen sind ein erster Schritt in Bezug auf eine künftige Anpassung der DSV, welche die Liste der Länder enthält, die einen angemessenen Datenschutz vorweisen.

4.2. Gemeinsame Kontrollinstanz Schengen

Die **Gemeinsame Kontrollinstanz Schengen** besteht aus Vertretern der nationalen Kontrollinstanzen.[132] Die nationale Kontrollinstanz hierfür ist in Liechtenstein die DSS. Sie überwacht, ob die Verwendung der Daten im SIS mit dem Schengen Durchführungsübereinkommen übereinstimmt. Schengen erfordert auch die Durchführung von *Kontrollen*, die teils durch die Gemeinsame Kontrollinstanz Schengen, in der die DSS den Beobachterstatus innehat, koordiniert werden. Koordinierte Kontrollen der Vergangenheit, an denen Liechtenstein noch nicht teilnehmen konnte, wurden in der Gemeinsamen Kontrollinstanz Schengen besprochen. Ein wichtiges Arbeitsmittel für solche Kontrollen stellen *Fragebögen* dar.

Wenngleich Liechtenstein noch keinen Zugriff auf die Daten hat, können durch die Mitarbeit in diesem Gremium wichtige Erkenntnisse über die Funktions- und Arbeitsweise von Schengen gewonnen werden.

Ein weiteres Projekt der Gemeinsamen Kontrollinstanz Schengen betraf die Überarbeitung des *„Best Practices"-Kataloges*. Der Katalog enthält Empfehlungen, die im Zuge des bevorstehenden Schengenbeitritts und auch danach massgebend sind. Er befasst sich mit den Ergebnissen aufgrund der Evaluierungen und stützt sich auf die Evaluierungsberichte ab. Weiters enthält er eine Zusammenfassung der Rechtsgrundlagen und Anforderungen für die nationalen Kontrollinstanzen (Personalausstattung der Instanzen, Rechte der betroffenen Personen, Grad der Unabhängigkeit, etc.). Auch zukünftige Entwicklungen, wie das SIS II, werden berücksichtigt.

Darüber hinaus hat sie einen Leitfaden betreffend das Auskunftsrecht überarbeitet. Dabei geht es um die Umsetzung des Auskunfts-, Berichtigungs- oder Löschrechts auf der Grundlage des Schengen Durchführungsübereinkommens.[133]

130. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_de.pdf.
131. Vgl. Tätigkeitsbericht 2008, 10.2.1. zur ersten Stellungnahme (WP 147).
132. Im Sinne des Art. 114 Schengen Durchführungsübereinkommens (SDÜ).
133. Vgl. Art. 109 ff SDÜ.

4.3. Eurodac Supervision Coordination Group

Wie das SIS sieht auch das Abkommen von Dublin eine Vernetzung der Ausländerbehörden vor. Kern des Abkommens ist das gemeinsame System *Eurodac*, welches die Fingerabdrücke von Asylwerbern umfasst. Mit Hilfe von Eurodac, das eine Identifizierung dieser Personen ermöglicht, soll das sogenannte Asylshopping vermieden werden. Als nationale Kontrollstelle Liechtensteins nimmt ein Vertreter der DSS an Sitzungen der **Eurodac Supervision Coordination Group** als Beobachter teil. Auch dieses Gremium koordiniert Kontrollen, an denen sich Liechtenstein nach seinem Beitritt zu den Abkommen von Schengen und Dublin beteiligen wird. Im Berichtsjahr wurde beispielsweise die Nutzung von *DubliNet* untersucht. Weiters wurde ein Bericht über die Untersuchung von *Informationen an die Betroffenen* sowie die *Feststellung des Alters von minderjährigen Asylsuchenden* fertiggestellt und veröffentlicht.[134]

4.4. Europarat

Der Datenschutzausschuss des Europarats setzte die Arbeit zum Thema „*Profiling*" fort.[135] Inzwischen war beschlossen worden, hierzu eine Empfehlung an die Mitgliedsstaaten auszuarbeiten, die sich allerdings auf den Privatrechtsbereich beschränkt. Damit bestehen zukünftig Richtlinien für den Umgang zu diesem Thema, welche allerdings rechtlich nicht verbindlich sind.[136] Der Ausschuss wird die Empfehlung voraussichtlich bei der Sitzung im kommenden Jahr finalisieren.

Die Arbeiten zur *Präzisierung der Kriterien der Unabhängigkeit und der Befugnisse einer nationalen Datenschutzbehörde*, welche im Vorjahr angegangen worden waren, wurden unterbrochen.[137] Der Grund für diese Unterbrechung der Arbeit besteht im Umstand, dass zum gegebenen Zeitpunkt ein Verfahren vor dem Europäischen Gerichtshof (EuGH) hängig war, in dem es genau um diese Frage ging. Mit anderen Worten sollte das Ergebnis dieses Verfahrens abgewartet werden, ehe die Arbeiten fortgesetzt werden.

Das Europaratsübereinkommen über die gegenseitige Amtshilfe in Steuersachen aus dem Jahr 1988 erhielt in der jüngeren Vergangenheit eine neue Dynamik in Anbetracht der Entwicklungen zum *Datenaustausch in Steuer-Angelegenheiten*. Bislang wurde es erst von vierzehn Mitgliedsstaaten des Europarats ratifiziert.[138] Dennoch soll es, auf Initiative der OECD, geändert und auch für Nicht-Mitgliedsstaaten des Europarats geöffnet werden. Die Achtung der Privatsphäre soll bei dieser Revision durch Arbeiten des Ausschusses gebührend berücksichtigt werden.

4.5. Europäische Datenschutzkonferenz

Im Rahmen der Europäischen Konferenz werden zweimal pro Jahr sogenannte **Case Handling Workshops** abgehalten. Bei diesen Workshops werden *aktuelle Themen und konkrete Fälle* behandelt, welche für die Datenschutzbehörden in Europa wichtig sind. Im Berichtsjahr nahmen wir an beiden Workshops teil, auf denen nützliche Informationen in Erfahrung gebracht werden konnten: insbesondere zur *Videoüberwachung*, welche auf beiden Workshops thematisiert wurde. Diese wertvollen Informationen aus der Praxis anderer Länder waren für uns bei der Schaffung des Genehmigungsverfahrens von Videoüberwachungsanlagen sehr hilfreich.[139]

Ausserdem waren *das Internet, die Datenbearbeitung am Arbeitsplatz, das Auskunftsrecht* und die wichtige Frage der *Rechtsdurchsetzung* weitere Themen. Anhand eines konkreten Falles wurden die einzelnen Datenschutzbehörden danach gefragt, was sie bei einer klar illegalen Datenbearbeitung unterneh-

134. Eine Zusammenfassung in deutscher Sprache kann unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/ shared/Documents/Supervision/Eurodac/09-06-24_Eurodac_report2_summary_DE.pdf abgerufen werden.
135. Vgl. Tätigkeitsbericht 2008, 10.2.2.
136. Dabei wird noch konkret zu definieren sein, wie diese Trennlinie zwischen Unternehmen und Behörden bzw. dem privaten und dem öffentlichen Sektor, aussehen wird. Diese Trennlinie, welche auf die Terminologie des Datenschutzübereinkommens des Europarats zurückgeht, hat sich im Laufe der Jahre verändert bzw. ist sie nicht mehr so klar.
137. Vgl. Tätigkeitsbericht 2008, 10.2.2.
138. Darunter kein einziges deutschsprachiges Land.
139. Vgl. III. 1.5.

men würden. Dabei stellte sich heraus, dass es teils grosse Unterschiede bei den Kompetenzen der Datenschutzbehörden gibt. So können einige die Unterlassung einer illegalen Datenbearbeitung direkt veranlassen und einige können gar das Bearbeitungssystem beschlagnahmen. Andere wiederum können Bussen und/oder Sanktionen aussprechen. Demgegenüber können wir *bloss eine Empfehlung* erlassen, die im Fall der Nichtbefolgung zur Entscheidung an die *DSK* gegeben werden kann.

Wir nahmen weiters als Beobachterin an Sitzungen der **Working Party on Police and Justice** teil. Behandelt wurden in diesem Gremium beispielsweise bestehende bilaterale Abkommen zwischen EU-Staaten und Drittstaaten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, einschliesslich des Kampfes gegen den Terrorismus oder Prüm-ähnliche bilaterale Abkommen mit Drittstaaten. Da sie hauptsächlich datenschutzrechtliche Fragen der polizeilichen und justiziellen Zusammenarbeit behandelt, sind viele Aspekte auch für den *Schengenbeitritt* relevant, beispielsweise Rechtsakte der Weiterentwicklung Schengen.[140]

Für Liechtenstein bedeutsam waren auch die Arbeiten dieses Gremiums zur Cybercrime Convention. Das Übereinkommen ist das erste internationale Rechtsinstrument zur Bekämpfung der Computer- und Internetkriminalität. Liechtenstein hatte dieses Übereinkommen 2008 unterzeichnet und zwischenzeitlich bereits entsprechende Straftatbestände neu in das Strafgesetzbuch aufgenommen. Die Working Party on Police and Justice hat unter den Mitgliedsstaaten eine Umfrage zur nationalen Umsetzung durchgeführt. Vor allem Ländern, die das Übereinkommen noch nicht ratifiziert haben, sollten die Ergebnisse dienen.

4.6. Internationale Datenschutzkonferenz

Die **„International Working Group on Data Protection in Telecommunications"**[141] wurde im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten im Jahr 1983 auf Initiative des Berliner Datenschutzbeauftragten gegründet. Seither wurden eine Vielzahl von Empfehlungen zur Verbesserung des Datenschutzes in der Telekommunikation erarbeitet. Teilnehmer sind Datenschutzbehörden, aber auch Regierungsstellen, Vertreter internationaler Organisationen und Wissenschaftler aus aller Welt. Bei dieser wurde durch uns eine Diskussionsgrundlage zum Thema Datenschutz auf *mobilen Endgeräten* (Mobiltelefone, Notebooks, usw.) eingebracht.

Mobile Geräte besitzen in der Regel eine kleine Bauform und geringes Gewicht. Hier liegen die *grössten Gefahren für die Datensicherheit im Verlust, der Manipulation und dem Diebstahl* der Daten. Während ein Verlust sofort erkennbar ist, verlangt die Erkennung einer Datenmanipulation die Implementierung geeigneter Sicherheitsmassnahmen zur Sicherung der Datenintegrität. Die Daten sind immateriell, wodurch ein möglicher Diebstahl oftmals erst dann bemerkt wird, wenn die Daten an einem anderen Ort wieder auftauchen. Basierend auf den zahlreichen Risiken der Nutzung von mobilen Geräten erarbeitet die Arbeitsgruppe Empfehlungen für die Hersteller und die Nutzer.

4.7. Privatim - Vereinigung der Schweizer Datenschutzbeauftragten

An den jährlichen Tagungen von Privatim[142] konnten wir nicht teilnehmen. In der Frühjahrestagung wurde eine *neue Arbeitsgruppe Technik (AG-ICT)* formell genehmigt. Die DSS hat einen Beobachterstatus und beteiligt sich aktiv an der Ausarbeitung von Papieren

140. Vgl. Tätigkeitsbericht 2008, 10.2.3 sowie III. 3.
141. http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt.
142. http://www.privatim.ch/.

im Zusammenhang mit Technik und Datenschutz, die für Liechtenstein von Interesse sind. Gerade der technische Datenschutz verlangt eine starke Vernetzung und einen regen Informationsaustausch.

4.8. Arbeitskreis Technik

Seit mehreren Jahren existiert unter der Leitung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Mecklenburg-Vorpommern der Arbeitskreis *„Technische und organisatorische Datenschutzfragen"* (AK Technik) als Gremium der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Er *berät* die Konferenz zu technischen Fragen des Datenschutzes und unterstützt die Beratungstätigkeit der Datenschutzbeauftragten. Zweimal im Jahr finden sich die Teilnehmer zu einer Sitzung zusammen, wobei auch wir seit 2005 zu den einzelnen Sitzungen eingeladen wurden. Bisher war jedoch mangels personeller Ressourcen eine Teilnahme nicht möglich. An der 52. Sitzung in Zürich konnte erstmalig ein Vertreter der DSS teilnehmen.

Im Berichtsjahr wurden insbesondere die Orientierungshilfen *„Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb"*[143] *sowie die „Protokollierung"*[144] *von Zugriffen* auf personenbezogene Daten behandelt. Erstere stellt klar, dass die Verarbeitung personenbezogener Daten in der Entwicklung und Testphase eines Systems nicht weniger schutzbedürftig sind als nach dessen Freigabe und Einsatz in einem Produktivumfeld. Die Regelungen des DSG und der Verordnung gelten für die Verarbeitung personenbezogener Daten ungeachtet der Frage, ob die Datenverarbeitung bereits im Produktivbetrieb oder noch in einer Projektphase erfolgt. Das zweite Papier stellt Aspekte der konkreten Ausgestaltung von Protokollierung vor. Erprobte Vorgehensweisen, die auf Basis gesetzlicher Anforderungen entwickelt wurden, werden in diesem Text als grundlegende Empfehlungen dargestellt. Weiters wurde das Thema Sicherheit von Webapplikationen aufgegriffen und diskutiert. Auf diese Weise konnten wertvolle Quellen im Zusammenhang mit dem technischen Datenschutz erschlossen werden.

5. In eigener Sache

Wie bereits erwähnt[145] wurde die *Stabsstelle für Datenschutz (SDS) in Datenschutzstelle (DSS) umbenannt* und neu dem Landtag zugeordnet.[146] Mit der Loslösung aus den Strukturen der Landesverwaltung ging eine *Leistungsvereinbarung mit der Landesverwaltung* einher.[147] Ziel dieser Leistungsvereinbarung war es, dass die technische und administrative Unterstützung durch die Landesverwaltung weiterhin gegeben ist, damit wir in nahezu allen organisatorischen Abläufen weiterhin so weit wie möglich durch die bestehende Infrastruktur profitieren können; damit wurden wir nicht in unserem gesetzlichen Auftrag eingeschränkt. Sonst wäre davon auszugehen, dass wir, zumindest in der Anfangsphase, grossteils mit organisatorischen wie dienstrechtlichen Angelegenheiten befasst gewesen wären.[148] Somit sollte eine möglichst einfache Handhabung bzw. Fortsetzung der organisatorischen Abläufe garantiert werden. Mit der Lösung aus der Landesverwaltung wurde deutlich, was für organisatorische Abläufe in der Verwaltung bestehen, die sonst eigentlich fast unbemerkt existieren. Gewiss wäre eine noch grössere organisatorische Selbstständigkeit der Abläufe möglich gewesen. Dieser Weg wurde jedoch bewusst nicht beschritten: einerseits, um Funktionierendes nicht zu hinterfragen, andererseits um Ressourcen zu sparen.

143. http://www.lfd.m-v.de/dschutz/informat/projekt/oh_projekt.pdf.
144. http://www.lfd.m-v.de/dschutz/informat/protokol/oh-proto.pdf.
145. S. dazu ausführlich im Tätigkeitsbericht 2008, 9. und 11.3.
146. Art. 28 Abs. 1 DSG.
147. Art. 28 Abs. 4 DSG: „Die Datenschutzstelle schliesst mit der Regierung eine Vereinbarung über die Besorgung organisatorischer und administrativer Geschäfte ab."
148. Stellungnahme der Regierung, Nr. 97/2008, S. 11.

Mit der Zuteilung zum Landtag war auch neu zu klären, wie das Verhältnis der DSS gegenüber der *Geschäftsprüfungskommission* des Landtags (GPK) anzusehen ist. Neben der Anhörung derselben vor der Wahl des Datenschutzbeauftragten erweisen sich der *Voranschlag* und die *Rechnungsprüfung* als Hauptberührungspunkte.[149] Zu nennen ist auch die Schaffung eines *Organisationsreglements*, bei der die GPK anzuhören ist.[150] Im Gegensatz zur Corporate Governance Vorlage erweist sich das Organisationsreglement im Sinne des DSG als rein internes Instrument, das im Wesentlichen die Verteilung der internen Aufgaben definiert. Wäre wie bei der Corporate Governance Vorlage auch das Verhältnis zur GPK Teil des Organisationsreglements, wäre die GPK gewiss nicht nur anzuhören, sondern ihr stünden darüber hinausgehende Rechte zu. Wie schon im Rahmen der Leistungsvereinbarung konnte auch bei der Schaffung des Organisationsreglements auf bestehendes Know-how der Landesverwaltung zurückgegriffen werden, um die interne Organisation der DSS zu definieren.

149. Art. 28a Abs. 1 und Art. 28c DSG.
150. Art. 28a Abs. 4 DSG.

IV. AUSBLICK

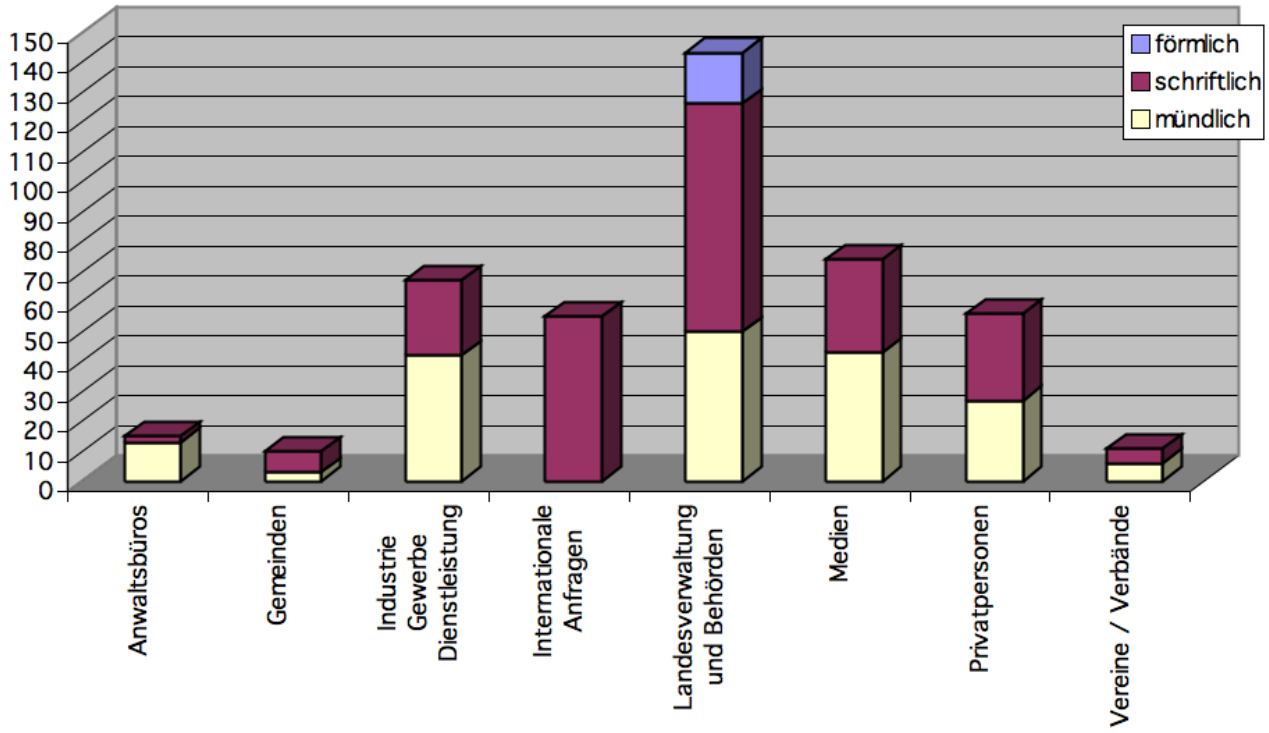
Einige wichtige Vorhaben werden wir auch kommendes Jahr weiterverfolgen: Der bevorstehende Beitritt zu „Schengen“ und „Dublin“ wird uns intensiv beschäftigen. Damit im engen Zusammenhang steht auch unser Aufgabenbereich „Aufsicht“, den wir deshalb ausbauen (müssen) und Kontrollen notwendig werden.

Die Sensibilisierung der Öffentlichkeit wird weiterhin ein zentrales Thema für uns sein. Dazu gehört insbesondere wiederum eine öffentliche Veranstaltung aus Anlass des Europäischen Datenschutztages, die regelmässig stattfindet und möglichst weite Kreise der Bevölkerung ansprechen soll.

V. ANHANG

1. Statistik: Beratung privater Personen und Behörden

Die Beratung privater Personen und Behörden ist eine Kernaufgabe. Im Berichtsjahr gingen insgesamt 431 Anfragen ein, so viele Anfragen wie nie zuvor. Gegenüber dem Vorjahr bedeutet das eine Zunahme um 115 Anfragen. Wie die nachfolgende Übersicht zeigt, stammen die meisten Anfragen nach wie vor von der Landesverwaltung.



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

Gesetzesthemen	Anwaltbüros	Gemeinden	Industrie, Gewerbe, Dienstleistungen	Internationale Gremien	Landesverwaltung und Behörden	Medien	Private Personen	Vereine/ Verbände
Datenschutz allgemein	6	1	22	6	32	44	21	4
Arbeitsbereich	1		8		1	2	3	
Datenbekanntgabe Inland		8	4		43	5	11	3
Datenbekanntgabe Auslandsbezug	5	1	11	8	7	1	1	1
Geltendmachung gesetzlicher Rechte							6	
Gesetzesvorlagen					34			
Gesundheit/Soziales					2			1
Polizei/Sicherheit	1		3	1	8	4	2	1
Register der Datensammlungen	1		7		1	1	1	
Schengen/Dublin				33	5	3		
Technologischer Datenschutz	1		2	4	2	12	8	1
Telekommunikation			4	3	1	1	2	
Umsetzung europäischen Rechts					2			
Wirtschaft/Finanzen			6		5	1	1	
TOTAL	15	10	67	55	143	74	56	11

2. Unsere Online-Umfrage

Wir haben auf unserer Homepage in der Zeit vom 25. Mai bis 14. Juni 2009 eine Umfrage durchgeführt. Deren Ziel war es u.a., Rückmeldungen zum allgemeinen Verständnis zum Datenschutz zu erhalten. Insgesamt wurden zum Thema Datenschutz vier Fragenblöcke gestellt: *Allgemeines – Information – Vertrauen – Verhalten*. Die Auswertung des Fragebogens erfolgte selbstverständlich anonym.

Die Umfrage wurde in den beiden Tageszeitungen sowie auf der Homepage angekündigt. Die Umfrage ist nicht repräsentativ, da wir sie auf unserer Homepage durchgeführt haben. 49 Personen haben teilgenommen. Bei der Auswertung der Eingaben waren daher folgende Prämissen zu berücksichtigen:

- Die teilnehmenden Personen verfügen zumindest über ein grundsätzliches Interesse für Datenschutzfragen;
- diesem Personenkreis ist die DSS bekannt;
- nur Nutzer des Internets konnten teilnehmen; wenngleich mittlerweile ein hoher Anteil der Bevölkerung mehr oder weniger regelmässig das Internet benützt, handelt es sich dabei lediglich um einen eingeschränkten Personenkreis.

2.1. Die Fragen

1. Allgemeines

a) Sind Sie der Meinung, dass Ihre Daten (und damit Ihre Privatsphäre) in Liechtenstein – im Allgemeinen – ausreichend geschützt sind?

ja 0 nein 0 weiss nicht 0

b) Kennen Sie Ihre Rechte und Pflichten im Datenschutz?

Ja 0 nein 0
teilweise 0 weiss nicht 0

2. Information

a) Fühlen Sie sich über Ihre Datenschutzrechte ausreichend informiert?

ja 0 nein 0 weiss nicht 0

b) Zu welchen Datenschutz-Themen wünschen Sie sich mehr Informationen?

Datenschutz am Arbeitsplatz 0
Datenschutz als Patient 0
Datenschutz als Konsument 0
Datenschutz im Internet 0
Datenschutz als Bürger 0
Sonstiges 0

3. Vertrauen

a) Verschiedene Unternehmen und Verwaltungen speichern Daten über Sie. Wie wichtig ist es Ihnen, dass Ihre persönlichen Daten von diesen geschützt werden?

Sehr wichtig 0 wichtig 0 weniger wichtig 0
unwichtig 0 weiss nicht 0

b) Welchen von den nachstehenden Unternehmen und Verwaltungen, die persönliche Daten gespeichert haben könnten, vertrauen Sie, dass Ihre Daten richtig verwendet werden?

Amtsstellen	ja 0 nein 0
Polizei	ja 0 nein 0
Banken	ja 0 nein 0
Kaufhäuser	ja 0 nein 0
Spitäler/Arztpraxen	ja 0 nein 0
Krankenkassen	ja 0 nein 0
Kreditkartenfirmen	ja 0 nein 0
Gemeinden	ja 0 nein 0
Telekom-Anbieter	ja 0 nein 0

c) Sind Sie – soweit Sie wissen – schon einmal von einem Missbrauch Ihrer Daten betroffen gewesen?

Ja 0 Nein 0

d) An wen würden Sie sich im Falle eines Missbrauchs Ihrer persönlichen Daten wenden? Mehrfachnennungen sind möglich (in alphabetischer Reihenfolge).

Datenschutzstelle 0
Gericht 0
Konsumentenschutz
(Amt für Handel und Transport) 0
Organisation, welche die Daten missbraucht hat 0
Polizei 0
Andere 0
Weiss nicht 0

4. Verhalten

a) Wie schätzen Sie Ihren eigenen Umgang mit Ihren persönlichen Daten ein?

Sehr kritisch 0 kritisch 0
weniger kritisch 0 sorglos 0

b) Wie schätzen Sie Ihren eigenen Umgang mit den persönlichen Daten anderer ein?

Sehr kritisch 0 kritisch 0
weniger kritisch 0 sorglos 0

2.2. Die Antworten

1. Allgemeines

Bei diesem Frageblock ging es um die Einschätzung darüber, ob der Datenschutz allgemein als ausreichend geschützt angesehen wird und im Speziellen darum, ob die Teilnehmer deren Rechte und Pflichten kennen. Gleich viele Teilnehmer bejahten und verneinten (je knapp 43 %) die Frage, ob Daten - und damit die Privatsphäre - in Liechtenstein im Allgemeinen ausreichend geschützt werden. 14 % konnten diese Fragen nicht beantworten („weiss nicht").

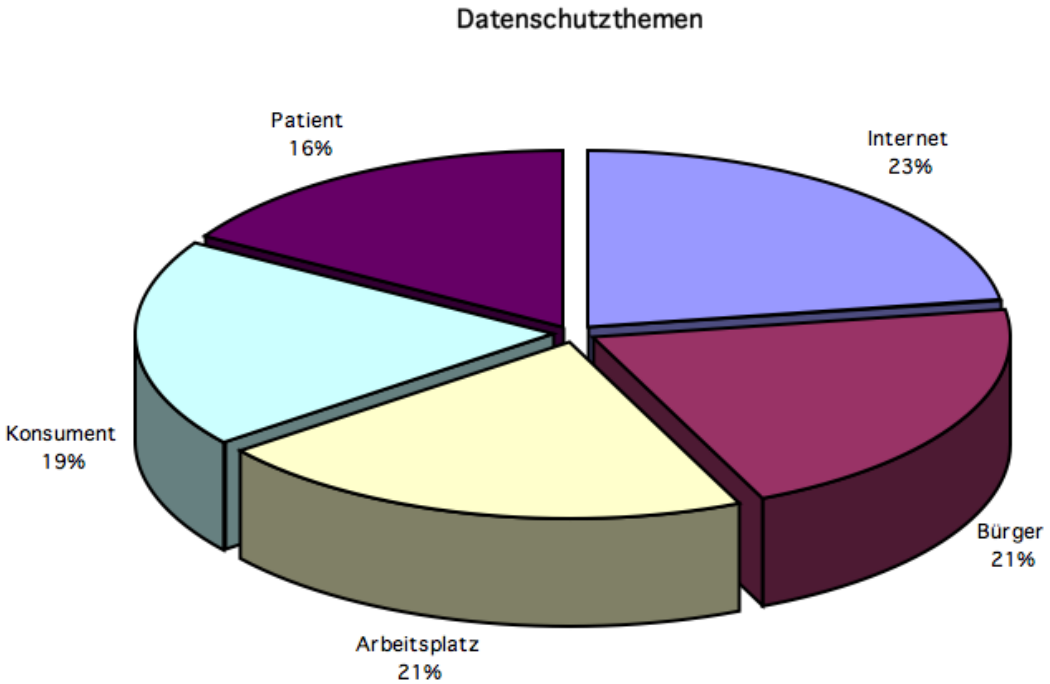
Die Frage, ob die Rechte und Pflichten im Datenschutz bekannt seien, wurde von 45 % der Teilnehmer mit „teilweise bekannt" beantwortet. 39 % bejahten ihre Kenntnis von den Rechten und Pflichten im Datenschutz. Bei diesem Ergebnis ist zu berücksichtigen, dass bei Personen, die an einer Online-Befragung auf unserer Internetseite teilnehmen, ein grundsätzliches Interesse für Datenschutzfragen besteht und sie teilweise auch über gewisse Kenntnisse in diesem Bereich verfügen.

2. Information

Die Frage, ob sich die Teilnehmer über ihre Datenschutzrechte ausreichend informiert fühlen, wurde von 57 % verneint.

Beim Wunsch nach mehr Information zu Datenschutzthemen rangierte der Datenschutz im Internet an erster Stelle, dicht gefolgt von den Themen Datenschutz am Arbeitsplatz und Datenschutz als Bürger. Bei dieser Frage waren mehrfache Antworten möglich.

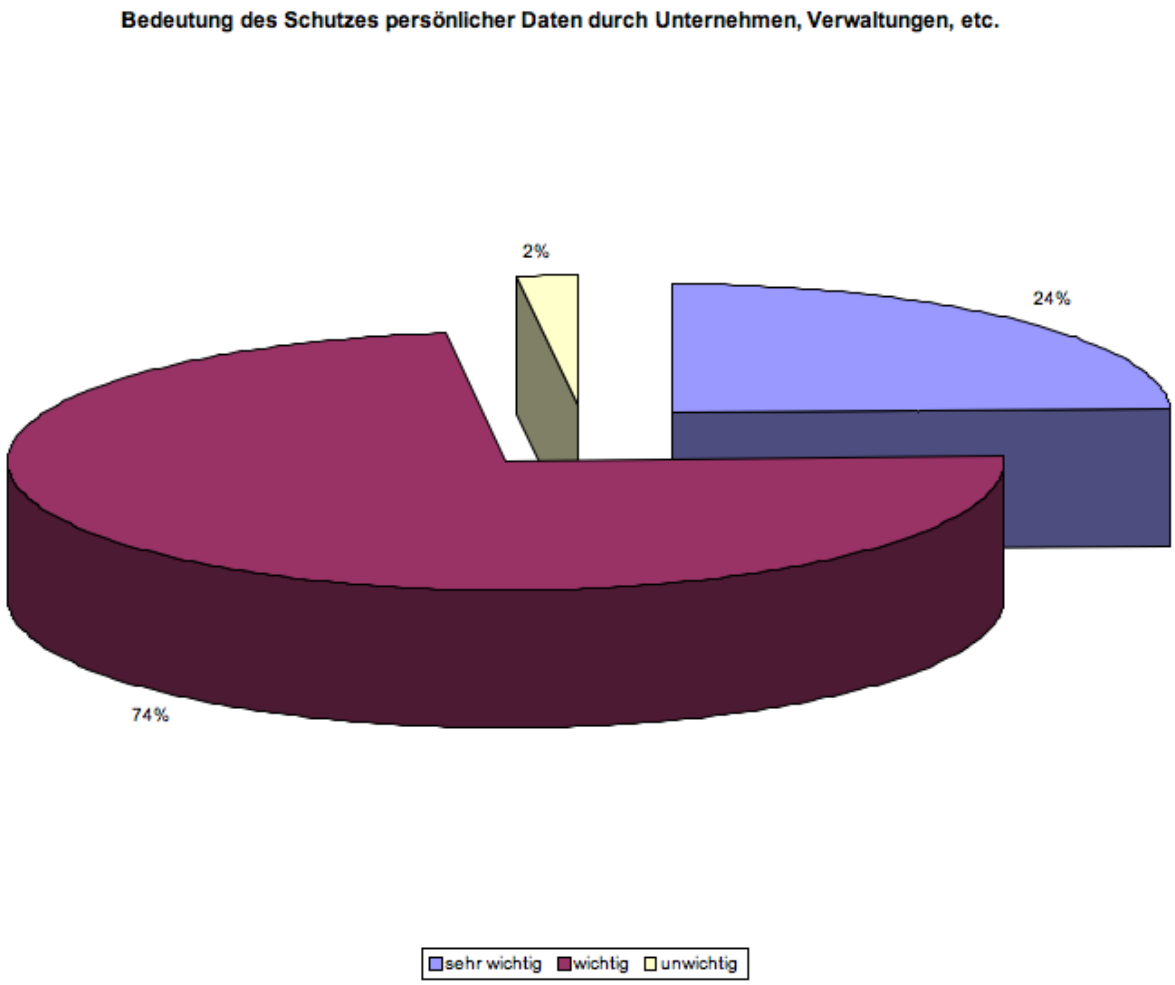
Abbildung 1: Wunsch nach mehr Informationen zu Datenschutzthemen



3. Vertrauen

Die nachstehende Grafik zur Frage „Vertrauen“ zeigt, wie wichtig dem Einzelnen die richtige Verwendung seiner persönlichen Daten durch die Verwaltungen und Unternehmen ist. Nahezu allen Befragten ist der Schutz ihrer persönlichen Daten sehr wichtig oder wichtig.

Abbildung 2: Bedeutung des Schutzes persönlicher Daten durch Unternehmen und Verwaltungen

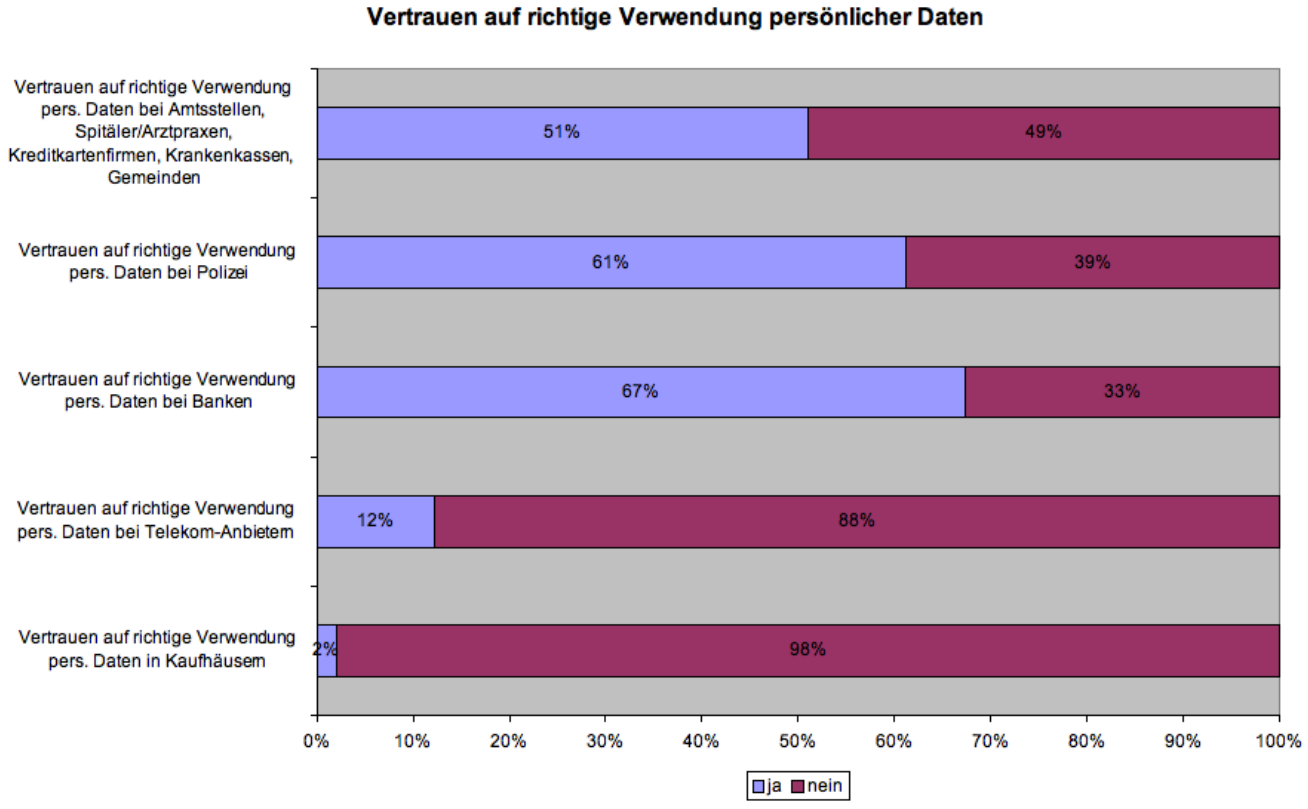


Auffallend ist die hohe Zahl jener Personen, die, ihrem Wissen zufolge, bereits einmal von einem Missbrauch ihrer Daten betroffen waren: 41 %. Dieser sehr hohe Anteil an Personen könnte dadurch erklärt werden, dass der Teilnehmerkreis bereits für Datenschutzthemen sensibilisiert ist.

Bei der Frage, an wen sich die Teilnehmer im Falle eines Missbrauchs ihrer Daten wenden würden, rangierte die DSS an erster Stelle (73,5 %). Mehrfachnennungen waren möglich. Das Ergebnis ist nicht überraschend, da die Umfrage lediglich mittels Online-Befragung auf unserer Internetseite durchgeführt wurde. Somit setzt die Teilnahme an der Befragung und die Beantwortung der Frage Bekanntheit der DSS voraus. An 2. Stelle der Antworten rangierte die Organisation, welche die Daten missbraucht hat (43 %) und auf Platz 3 die Konsumentenschutzstelle des Amtes für Handel und Transport (39 %).

In der nächsten Frage ging es um Vertrauen auf die richtige Verwendung persönlicher Daten in einzelnen Kategorien von Unternehmen, Behörden, usw. Auch bei dieser Frage waren Mehrfachnennungen möglich. Eindeutig lässt sich mangelndes Vertrauen im Umgang mit den persönlichen Daten durch Kaufhäuser und Telekom-Anbieter feststellen. Ein durchschnittliches Bild zeichnet sich bei den Amtsstellen, Spitälern/Arztpraxen, Krankenkassen, Gemeinden und Kreditkartenfirmen ab. In diese Einrichtungen hat jeweils etwa die Hälfte Vertrauen.

Abbildung 3: Vertrauen in die richtige Verwendung persönlicher Daten



4. Verhalten

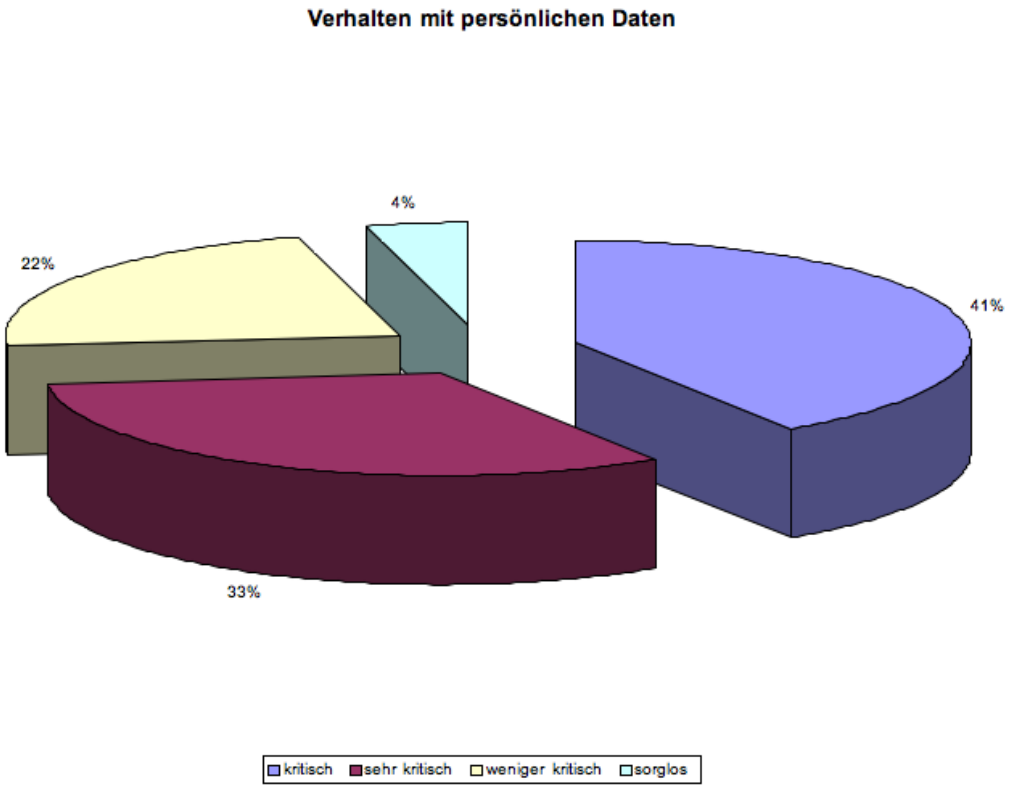
Das eigene Verhalten im Umgang mit den eigenen persönlichen Daten schätzt die überwiegende Zahl der Teilnehmer als kritisch (61 %) oder sehr kritisch (19 %) ein. Lediglich 18 % pflegen einen weniger kritischen oder gar sorglosen (2 %) Umgang.

Wie nachfolgende Grafik zeigt, pflegen dieselben Personen auch einen sehr kritischen bzw. kritischen Umgang mit den persönlichen Daten anderer.

Abbildung 4: Verhalten im Umgang mit den persönlichen Daten anderer

Zusammengefasst lassen sich aus den Ergebnissen folgende Schlüsse ziehen:

- Information (Wissen) – Vertrauen – Verhalten gehören offensichtlich zusammen. So wurde die Frage, ob sich die Teilnehmer über ihre Datenschutzrechte ausreichend informiert fühlen, durch eine überwiegende Anzahl von Antworten klar verneint.
- Nur wer seine Rechte und Pflichten kennt, möchte auch, dass diese von anderen geschützt und richtig verwendet werden. Daraus leitet sich sowohl ein kritischer Umgang mit den eigenen persönlichen Daten als auch mit dem Umgang persönlicher Daten anderer ab.
- Information und Sensibilisierung der Bevölkerung sind unerlässlich. Datenschutz wird immer wichtiger. Die hohe Anzahl an (vermeintlichen) Missbräuchen zeigt klar, dass hier verstärkt Aufklärungsarbeit zu leisten ist. Denn einmal mehr gilt auch im Datenschutz: „Nur wer seine Rechte (und Pflichten) kennt, kann sie auch schützen."



Abkürzungsverzeichnis

ABGB	Allgemeines Bürgerliches Gesetzbuch
AK	Amt für Kommunikation
ArGVI	Arbeitsgenehmigungs-verordnung
Art.	Artikel
Bst.	Buchstabe
DSB	Datenschutzbeauftragter
DSG	Datenschutzgesetz
DSK	Datenschutzkommission
DSS	Datenschutzstelle
DSV	Datenschutzverordnung
ECM	Enterprise Content Management
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDSK	Datenschutzkommission
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechts-konvention
ENISA	European Network and Information Society Agency
ESA	European Surveillance Authority
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
FAQ's	Frequently Asked Questions (oft gestellte Fragen)
FIDIS	Future of Identity in the Information Society
FMA	Finanzmarktaufsicht
GewV	Gewerbeverordnung
GPK	Geschäftsprüfungskommission
ICM	Integriertes Case Management
IP	Internet Protocol
IV	Invalidenversicherung
IVG	Invalidenversicherungsgesetz
IWGDPT	International Working Group on Data Protection in Telecommunications
KomG	Kommunikationsgesetz
KVG	Krankenversicherungsgesetz
LIZ	Liechtensteinische Juristenzeitung
LLV	Liechtensteinische Landesverwaltung
LVG	Allgemeine Landesverwaltungsrechtspflege
PEID	Personenidentifikationsnummer
PET	Privacy Enhancing Technologie (Technologie zum Schutz der Privatsphäre)
PGR	Personen- und Gesellschaftsrecht
PolG	Polizeigesetz
PRIME	Privacy and Identity Management for Europe
RISEPTIS	Research and Innovation for Security, Privacy and Trustworthiness in the Information Society
S.	Siehe; Seite
SDS	Stabsstelle für Datenschutz
SDÜ	Schengener Durchführungsübereinkommen
SIS	Schengener Informationssystem
SPG	Sicherheitspolizeigesetz
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPG	Staatspersonalgesetz
StPO	Strafprozessordnung
Vgl	Vergleiche
VKND	Verordnung über elektronische Kommunikationsnetze und Dienste
VSL	Verein Sicheres Liechtenstein
VUD	Verein Unternehmens-Datenschutz
WP	Working Papers
WPPJ	Working Party on Police and Justice
ZPV	Zentrale Personenverwaltung

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

09