Tätigkeitsbericht 2012

Datenschutzbeauftragter
des Kantons Luzern

KANTON LUZERN

Datenschutzbeauftragter | datenschutz.lu.ch

Inhalt

Vorwort

Der Datenschutzbeauftragte hat gemäss § 23 Abs. 1 lit. k DSG[1] dem Regierungsrat jährlich Bericht über seine Tätigkeit zu erstatten und stellt der Aufsichts- und Kontrollkommission des Kantonsrates eine Kopie zu; der Bericht wird öffentlich zugänglich gemacht.

Der vorliegende Bericht erstreckt sich über den Zeitraum vom 1. Januar 2012 bis 31. Dezember 2012. Das Berichtsjahr war – bei unverändert sehr angespannten Personalressourcen – durch eine im Vergleich zum Vorjahr sehr starke Erhöhung der Geschäftsfälle gekennzeichnet (+63%). Die äusserst knappe Ressourcensituation (90% Stellenprozent, aufgeteilt auf zwei Personen) führt weiterhin zu einer nicht optimalen Erreichbarkeit der Datenschutzstelle. Dies wirkt sich negativ auf die Niederschwelligkeit des Angebotes aus. Verunsicherte Personen zögern oftmals, sehr intime Informationen per E-Mail mitzuteilen oder auf einem Telefonbeantworter abzulegen. Zudem konnten die gesetzlichen Aufgaben des DSB erneut nicht vollumfänglich wahrgenommen werden. Dies ist auch im Hinblick auf die internationalen Verpflichtungen der Schweiz im Bereich des Datenschutzes weiterhin kritisch.

Das Berichtsjahr war geprägt durch die Beratung und Begleitung verschiedener Projekte wie der elektronischen Rechnungskontrolle, dem Pilotprojekt Microsoft O365 an der Kantonsschule Alpenquai, der Liste der säumigen Prämienzahler (LSP), der Stipendiengesetzrevision (elektronisches Abrufverfahren), dem BMI-Monitoring, der Erarbeitung eines Datenschutzmuster-

[1] Gesetz über den Schutz von Personendaten (Datenschutzgesetz) vom 2. Juli 1990, SRL Nr. 38

reglements für Gemeinden in Zusammenarbeit mit dem VLG, der Umsetzung der E-Government-Strategie Luzern, der Vorbereitung der SAP-Ausschreibung und der Erarbeitung einer Stellungnahme zum Thema Cloud-Computing für die Dienststelle Informatik sowie verschiedenen weiteren Projekten und Vorhaben.

Es lässt sich positiv festhalten, dass das Interesse am Datenschutz in den vielen kantonalen Dienststellen, in den Gemeinden und in der Bevölkerung stetig zunimmt und die Sensibilisierung für die Thematik des Datenschutzes in den letzten Jahren Früchte trägt; entsprechend gelangten diese kantonalen und kommunalen Verwaltungsstellen sowie Bürgerinnen und Bürger mit zahlreichen Anfragen an den Datenschutzbeauftragten (+53% gegenüber Vorjahr). Eine proaktive Sensibilisierung und Schulung wäre dennoch weiterhin notwendig bzw. als steter Prozess zu institutionalisieren, um die grundrechtlich und gesetzlich verankerten Anliegen des Datenschutzes sowie der Informationssicherheit angemessen zu thematisieren und zu berücksichtigen. Dies im Zuge der ganz allgemein immer komplexeren Informatik, welche auch die Kommunikation in der Verwaltung erfasst (E-Mail, Voice-over-IP-Telefonie, Smartphone etc.), sowie im Speziellen nicht zuletzt auch im Hinblick auf die laufende Umsetzung der E-Government-Strategie Luzern mit entsprechenden Webportalen, über welche grösstenteils Personendaten ausgetauscht werden sollen. Aufgrund der herrschenden Ressourcenknappheit lässt sich die erforderliche proaktive Sensibilisierung und Schulung jedoch nicht umsetzen.

Im nachfolgenden Text werden die beiden Begriffe *Datenschutzbeauftragter* und *Datenschutzgesetz des Kantons Luzern* oft verwendet. Damit der Text aufgrund dieser häufigen Begriffsverwendungen nicht unnötig in die Länge gezogen wird, sind die Begriffe «Datenschutzbeauftragter» mit DSB und «Datenschutzgesetz des Kantons Luzern» mit DSG abgekürzt.

Dr. iur. Reto Fanger, Rechtsanwalt
Datenschutzbeauftragter des Kantons Luzern

A. Gesetzlicher Auftrag

Der Auftrag und die Aufgaben des DSB sind in den §§ 22 f. DSG verankert. Diese lauten wie folgt:

§ 22 Aufsicht

1 Der Regierungsrat wählt als kantonale Aufsichtsstelle einen Beauftragten für den Datenschutz. Die Wahl bedarf der Genehmigung durch den Kantonsrat.

2 Der Beauftragte ist fachlich selbständig und unabhängig; administrativ ist er der Staatskanzlei zugeordnet.

3 Die dem Gesetz unterstellten Gemeinwesen können eine eigene Aufsichtsstelle schaffen. Der Beauftragte für den Datenschutz übt in diesem Fall die Oberaufsicht aus.

§ 23 Aufgaben

1 Der Beauftragte für den Datenschutz

a. überwacht die Einhaltung der Vorschriften über den Datenschutz,

b. berät die verantwortlichen Organe in Fragen des Datenschutzes und der Datensicherung,

c. erteilt den betroffenen Personen Auskunft über ihre Rechte,

d. vermittelt zwischen Organen und Personen in allen Anständen über den Datenschutz, namentlich bei Begehren um Auskunft, Berichtigung und Unterlassung,

e. reicht in hängigen Verfahren auf Ersuchen von entscheidenden Organen oder Rechtsmittelbehörden Stellungnahmen zu Datenschutzfragen ein,

f. orientiert die Organe über wesentliche Anliegen des Datenschutzes,

g. sorgt für die Instruktion der Mitarbeiter von Organen über den Datenschutz,

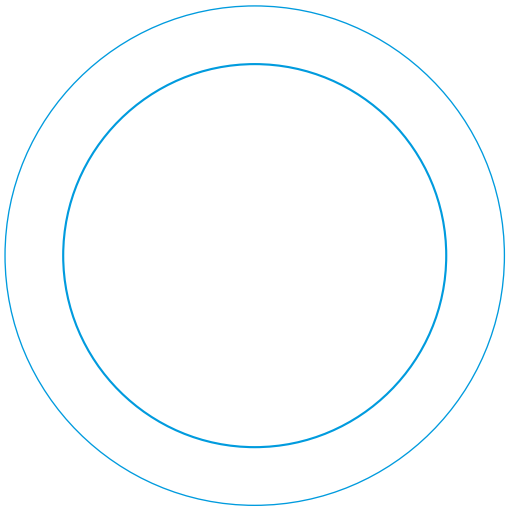
h. kontrolliert im Voraus Bearbeitungsmethoden, welche die Persönlichkeit einer grösseren Anzahl von Personen verletzen könnten,

i. veröffentlicht Stellungnahmen,

j. arbeitet mit den Kontrollorganen der anderen Kantone, des Bundes und des Auslandes zusammen,

k. erstattet dem Regierungsrat jährlich Bericht über seine Tätigkeit und stellt gleichzeitig der Aufsichts- und Kontrollkommission des Kantonsrats eine Kopie zu; der Bericht wird öffentlich zugänglich gemacht.

2 Er führt für den Kanton das Register über die Datensammlungen.



B. Statistische Angaben

Die Dienstleistungen des DSB können für das Berichtsjahr wie folgt zusammengefasst werden:

Dienstleistungen	2009	2010	2011	**2012**	Entwicklung (11–12)
1. Auskunft					
Anfragen Gemeinden	37	40	40	**30**	–25 %
Anfragen Kanton*				**77**	
Anfragen Private*				**122**	
Total Auskunft	139	148	150	**229**	+53 %
Anfragen ohne Ablage (einfache schriftliche Auskünfte)	108	125	133	**198**	+49 %
Anfragen mit Ablage (komplizierte Dossiers)	31	23	15	**31**	+107 %
wovon betreffend Bereich Informatik	*25*	*19*	*8*	**18**	*+125 %*
wovon betreffend Bereich Polizei	*11*	*10*	*7*	**15**	*+114 %*
*wovon betreffend Bereich Bildung**	*11*	*10*	*7*	**33**	*+371 %*
*wovon betreffend Bereich Soziales**	*11*	*10*	*7*	**34**	*+386 %*
*wovon betreffend Bereich Privat**	*11*	*10*	*7*	**19**	*+171 %*
wovon betreffend Bereich Gesundheit	*16*	*25*	*16*	**26**	*+63 %*
wovon verschiedene andere Bereiche (Diverse)	*50*	*54*	*77*	**84**	*+9 %*
2. Projekte und Weiterbildung					
Mitarbeit in Projekten	3	6	5	**20**	+400 %
Leitung von Projekten	0	0	0	**0**	–
Geleitete Ausbildungsveranstaltungen	1	0	0	**3**	+300 %
Gehaltene Vorträge	3	2	3	**0**	–300 %
Total Geschäftsfälle	146	156	158	**257**	+63 %

*neue Rubriken seit 2012

Im Berichtsjahr haben – abgesehen von der generell starken Zunahme in allen erhobenen Bereichen – vor allem die Anfragen in den Bereichen Bildung und Soziales sehr stark zugenommen. Auch die Anfragen Privater entsprechen diesem Trend und beziehen sich oft auf das Thema «Videoüberwachung». Eine sehr starke Zunahme ist überdies bei den Projektarbeiten auszumachen.

Cloud Computing für die Verwaltung

Ob geplant oder nicht, Cloud-Computing hält mit der Omnipräsenz des Internets und der wachsenden Zahl von leicht zugänglichen Angeboten auch in den Behörden zunehmend Einzug – oft ohne, dass die Nutzer sich dessen bewusst sind. Die versprochenen Vorteile sind interessant: Cloud-Computing kann einen signifikanten Beitrag zur Umsetzung der E-Government-Strategie Schweiz und Luzern leisten. Mit Cloud-Computing können potentiell die Kosten gesenkt und die Innovationsfähigkeit der Schweizer Behörden gesteigert werden. Die Behörden können durch den Cloud-Einsatz ihre Effizienz steigern, die Flexibilität ihrer IKT erhöhen, Ressourcen für das Kerngeschäft frei machen und ein zeitgemässes E-Government-Angebot einfacher und schneller aufbauen. Gerade auch kleineren Gemeinden bietet Cloud-Computing die Möglichkeit, Leistungen elektronisch medienbruchfrei anzubieten ohne selbst eine Infrastruktur aufbauen zu müssen. Damit kann E-Government besser in die Fläche gebracht werden. Den Vorteilen stehen jedoch Risiken insbesondere im Bereich der Sicherheit gegenüber, denen gebührend Rechnung zu tragen ist: Die Daten liegen beim Cloud-Anbieter – eventuell im Ausland. Die Verarbeitung wird an ihn ausgelagert. Die Antwortzeiten sind von den verfügbaren Bandbreiten abhängig. Die Komplexität der Leistungserbringungs-Strukturen nimmt zu. Es stellen sich grundsätzliche datenschutzrechtliche Fragen bezüglich Ausübung der Aufsicht und Umsetzung der Kontrollrechte Betroffener (Zugang zu Rechenzentren etc.).

Bei Privatpersonen ist die Nutzung von kostenlosen Cloud-Computing-Angeboten schon weit verbreitet. Laut einer weltweiten Umfrage in 2000 Unternehmen haben aktuell 3% ihre IT mehrheitlich in die Cloud ausgelagert. Es wird erwartet, dass diese Zahl innerhalb der nächsten 4 Jahre auf 43% anwächst. In zahlreichen Ländern laufen Aktivitäten zur Nutzung von Cloud-Computing in der öffentlichen Verwaltung. Die USA haben eine Cloud First-Strategie beschlossen. Die EU hat für 2012 ist eine Cloud-Strategie angekündigt.

In der Schweiz hat die eCH-Fachgruppe SEAC (Swiss eGovernment Architecture Community) Cloud-Computing als prüfenswerte Möglichkeit zur Unterstützung der Ziele der E-Government-Strategie Schweiz identifiziert und eine entsprechende Vorstudie erstellt. Die Vorstudie kommt zum Schluss, dass mit dem aufeinander abgestimmten Einsatz von Cloud Computing einigen der bestehenden Umsetzungsprobleme im E-Government der Schweiz begegnet werden könnte.

Die Cloud-Computing-Strategie der Schweizer Behörden ergänzt die E-Government-Strategie der Schweiz. Sie beschreibt, wie die Schweizer Behörden mit den neu entstehenden Möglichkeiten umgehen wollen und welche Massnahmen zu treffen sind, damit die mit dem Cloud-Einsatz einhergehenden Risiken minimiert und die sich damit eröffnenden Chancen insbesondere auch zur Unterstützung von E-Government genutzt werden können. Ergänzt wird sie durch einen Katalog der Umsetzungsmassnahmen.

Die Strategie ist ein Ergebnis des priorisierten E-Government-Vorhabens «B1.06 – E-Government-Architektur Schweiz» und wurde zusammen mit Experten aus Bund, Kantonen, Gemeinden, bundesnahmen Betrieben und der Wirtschaft erarbeitet. Sie richtet sich vornehmlich an Bund, Kantone, Gemeinden und bundesnahe Betriebe, in zweiter Linie an betroffene Wirtschaftskreise, insbesondere Cloud-Anbieter.

Anforderungen an den Datenschutz bei Cloud Computing

Der Eidgenössische Datenschutzbeauftragte macht in seinen Erläuterungen zu Cloud Computing klar, dass der Auftraggeber sich selber vergewissern muss, dass der Anbieter der Cloud Lösung die Datensicherheit gewährleistet. Der Cloud Nutzer bleibt letztlich gegenüber den betroffenen Personen (deren Daten er in der Cloud nutzt) selber verantwortlich für die Einhaltung der schweizerischen Datenschutz-Vorschriften und haftet sogar bei allfälligen Verletzungen.

Der Auftraggeber muss folgende Punkte sicherstellen:

- Der Datenschutz und die Datensicherheit müssen gewährleistet bleiben.
- Es darf nicht zu einem Kontrollverlust der Daten kommen.
- Ausländische Behörden sollen keinen Zugriff auf die Daten haben.
- Die Daten müssen im Falle eines Wechsels des Anbieters migriert werden können.

Art. 10 des eidgenössischen Datenschutzgesetzes (DSG-CH) bestimmt, dass das Bearbeiten von Personendaten an Dritte (z.B. Cloud-Anbieter) übertragen werden darf, solange die Daten nur so bearbeitet werden, wie der Auftraggeber (z.B. Cloud-Nutzer) selbst es tun dürfte. Der Auftraggeber muss sich vergewissern, dass der Cloud Anbieter die Datensicherheit gewährleistet.

Der Cloud-Anbieter muss dazu verpflichtet werden, sich vollumfänglich an die in der Schweiz geltenden Datenschutzbestimmungen zu halten. Dies gilt genauso für allfällige Subunternehmer (Hardware- und Softwarelieferanten, Berater, Reinigungs-Personal, Software-Wartung, Support etc.), die vom Anbieter beigezogen werden.

Art. 7 DSG-CH bestimmt, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Dabei muss sich der Cloud-Nutzer gegen folgende Risiken absichern:

- unbefugte oder zufällige Datenvernichtung
- Datenverlust
- technische Fehler
- Fälschung, Diebstahl oder widerrechtliche Verwendung
- unbefugtes Ändern, Kopieren, Zugreifen

Der Cloud-Nutzer ist dafür verantwortlich, dass der Cloud-Anbieter die Daten gegen die aufgeführten Risiken schützt. Die Massnahmen gegen diese Risiken müssen regelmässig vor Ort durch den Nutzer überprüft werden.

Der Kanton Luzern verfügt mit dem Informatikgesetz über eigene gesetzliche Grundlagen, welche die Anforderungen an zentrale Datenbanken und die Auslagerung von Informatikdienstleistungen an Dritte (z.B. Outsourcing von Datenbanken an einen Cloud-Anbieter) explizit regeln.

C. Anfragen und Gesuche

Nachfolgend werden exemplarisch bestimmte Anfragen, Gesuche und Projekte erwähnt, die im Verlaufe des Berichtsjahres behandelt wurden:

1. Bereich Polizei

• Betrunkener Taxifahrer erwischt

Ein Taxifahrer, der mit einer Blutalkoholkonzentration von 1.03 Promille arbeitete, gerät in eine Polizeikontrolle (NLZ vom 20.12.2011). Ein Taxichauffeur ist verantwortlich für die Sicherheit seiner Fahrgäste. Wer ein Taxi besteigt, vertraut denn auch darauf, dass der Taxifahrer sein Möglichstes tut, um seinen Gast sicher von A nach B zu bringen. Gemäss Artikel 6 des Taxireglements der Stadt Luzern wird die Taxibetriebsbewilligung entzogen, wenn die Inhaberin oder der Inhaber in schwerer Weise oder wiederholt gegen Verkehrsvorschriften oder gegen Bestimmungen dieses Reglements verstossen hat, zu solchen angestiftet oder solche geduldet hat.

Die Frage stellt sich nun, ob die Stadt über die Gesetzesverstösse der Taxifahrer von der Luzerner Polizei informiert werden darf. Hat ein Taxifahrer ausserkantonal delinquiert, erfährt dies die Stadt nicht.

Zunächst ist zu klären, was mit dem Begriff «Gesetzesverstösse» gemeint ist. Soweit damit auch laufende Strafverfahren gemeint sind, ist das Datenschutzgesetz gemäss § 3 Abs. 2 lit. a DSG nicht anwendbar: Die Zulässigkeit allfälliger Auskünfte ist nach den einschlägigen Bestimmungen der eidgenössischen Strafprozessordnung (StPO) zu beurteilen. Folglich beziehen sich die nachstehenden Ausführungen lediglich auf rechtskräftige Verurteilungen, die unter das kantonale Datenschutzgesetz fallen.

Bei Informationen über rechtskräftige Verurteilungen handelt es sich um besonders schützenwerte Daten im Sinne von § 2 Abs. 2 DSG.

Gemäss § 5 Abs. 2 DSG bedarf die Bearbeitung besonders schützenswerter Personendaten einer gesetzlichen Grundlage im formellen Sinn (lit. a) oder die Bearbeitung muss für die Erfüllung einer in einem formellen Gesetz vorgesehenen Aufgabe unentbehrlich sein (lit. b).

Eine ausdrückliche formelle gesetzliche Grundlage für eine Datenbekanntgabe liegt mit § 4 Abs. 2 PolG grundsätzlich zwar vor:

2 Sie kann Daten im Rahmen der Zusammenarbeit mit Polizeiorganen anderer Gemeinwesen und mit staatlichen Institutionen erheben, bearbeiten und weitergeben. Daten dürfen nur weitergegeben werden, wenn dies zur Erfüllung der gesetzlichen Aufgaben der Informationsempfängerinnen und -empfänger erforderlich ist.

Die in Satz 2 dieser Bestimmung vorausgesetzte Erforderlichkeit der Datenherausgabe für die Aufgabenerfüllung durch die Stadt Luzern ist aber vorliegend nicht gegeben. So vermag die Stadt Luzern die Voraussetzungen zur Lizenzerteilung bzw. -aufrechterhaltung auch durch die (regelmässige) Einforderung von Strafregisterauszügen bei den gesuchstellenden Taxihaltern und Taxiunternehmen zu prüfen. Ob die entsprechende Möglichkeit, von den Gesuchstellern regelmässig die Einreichung von Strafregisterauszügen zu verlangen, im Taxireglement vorgesehen ist, spielt für die vorliegende Beurteilung keine Rolle. Sofern dies nicht ausdrücklich vorgesehen wäre, müsste die Stadt Luzern die gesetzlichen Grundlagen und somit ihr Taxireglement entsprechend anpassen. Dies alleine berechtigt die Luzerner Polizei im vorliegenden Fall dennoch nicht zur Datenbekanntgabe.

Die Voraussetzungen von § 5 Abs. 2 lit. b DSG sind – soweit ersichtlich – ebenfalls nicht erfüllt, zumal die in § 1 Abs. 1 PolG statuierten Aufgabe der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie der Prävention nicht von der vorliegend interessierenden Datenbekanntgabe abhängen bzw. keine unmittelbare Gefahren im Sinne von § 1 Abs. 2 lit. a PolG drohen.

Zusammenfassend ist keine genügende Rechtsgrundlage für die Information der Stadt Luzern über rechtskräftige Verurteilungen von Taxifahren durch die Luzerner Polizei vorhanden.

2. Bereich Gemeinden

- Herausgabe von Adressen

Eine Luzerner Gemeinde erhielt die Anfrage einer Bank, ob sie eine Adressliste aller 14- bis 16-jährigen Einwohner erhalten könnte. Die Bank würde die Daten für die folgenden Zwecke benötigen:

- Zustellung eines Gutscheines
- Informationen zur Jugendverschuldung
- Werbung für die Eröffnung eines Kontos

Voraussetzung der oben erwähnten Datenbekanntgabe gemäss § 11 Abs. 1 DSG ist das Glaubhaftmachen eines schutzwürdigen Interesses.

Zwar gibt die Bank nicht nur wirtschaftliche Zwecke an (Zustellung eines Gutscheins und Werbung für die Eröffnung eines Jugendkontos als Marketingmassnahmen), sondern verfolgt mit der Information über die Jugendverschuldung durchaus auch schutzwürdige Interessen. Es ist allerdings aufgrund dieser Angaben nicht ersichtlich, in welchem Umfang die Werbe- bzw. Marketingmassnahmen zu den Informationsabsichten über die Jugendverschuldung stehen. Es ist aber – da die Bank ein gewinnorientiertes Unternehmen ist und die erwähnten Massnahmen in erster Linie der Neukundengewinnung dienen werden – davon auszugehen, dass die wirtschaftlichen Absichten in diesem Fall überwiegen. Somit spricht eine Interessenabwägung in diesem Fall gegen die Herausgabe der Adressen.

3. Bereich Bildung

- Einsatz von Microsoft Office 365 im Kanton Luzern (Cloud-Computing)

Seit Oktober 2011 läuft an der Kantonsschule Alpenquai in Luzern das Pilotprojekt «Office 365». Nach der Pilot-Phase wird eine vertiefte datenschutzrechtliche Beurteilung vorzunehmen sein.

Zu berücksichtigen sind dabei das DSG und die dazugehörige Verordnung, das Informatikgesetz und die Sicherheitsverordnung.

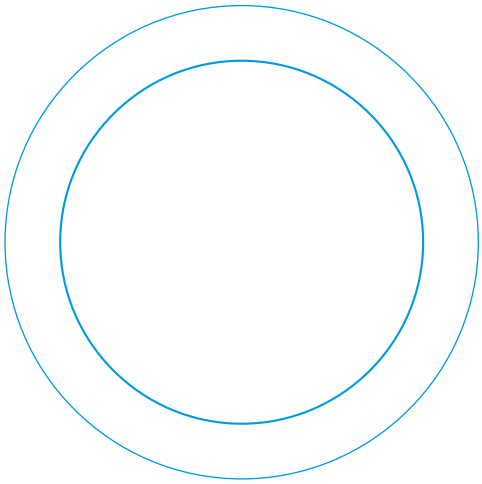
Neue Technologien wie Cloud Computing bedingen neue risikoorientierte Ansätze zum Schutz der Persönlichkeitsrechte. Cloud Computing verändert insbesondere die Art und Weise der Datenbearbeitung, wobei aus datenschutzrechtlicher Sicht diese unter die Bestimmungen der Datenverarbeitungen durch Dritte zu subsumieren sind.

Cloud Computing sollte sich somit an die bestehenden Regeln für Outsourcing orientieren. Es stellen sich dabei grundsätzliche datenschutzrechtliche Fragen bezüglich Ausübung der Aufsicht und Umsetzung der Kontrollrechte Betroffener (Zugang zu Rechenzentren etc.), die für jedes Cloud Computing-Projekt gesondert zu beantworten sind.

4. Bereich Gesundheit

- BMI-Monitoring im Kanton Luzern

In den letzten zehn bis zwanzig Jahren hat der Anteil übergewichtiger Menschen stark zugenommen. Vor diesem



Hintergrund erklärte die Gesundheitsförderung Schweiz die Förderung eines «Gesunden Körpergewichts» – insbesondere bei Kindern und Jugendlichen – zu einer ihrer drei strategischen Zielsetzungen.

Seit 2008 führt in diesem Rahmen die Dienststelle Gesundheit das Luzerner Aktionsprogramm «Gesundes Körpergewicht» durch. Ziel des Programms ist, dass sich Kinder und Jugendliche mehr bewegen und ausgewogen ernähren. Bisher verfügt der Kanton Luzern über kein systematisches Monitoring des Übergewichtsproblems in seiner Bevölkerung, sondern nur über einmalige Erhebungen oder Befragungen. Dabei ist erwiesen, dass Befragungsdaten die Übergewichtsproblematik unterschätzen. Um das Aktionsprogramm besser zu steuern, sind zuverlässige Angaben zum Body-Mass-Index (BMI) von Kindern und Jugendlichen zentral. Verschiedene Kantone und Städten nehmen deshalb an einem nationalen BMI-Monitoring teil. Diese nationale Studie wird von Gesundheitsförderung Schweiz koordiniert. Die Dienststelle Gesundheit möchte ein eigenes BMI-Monitoring aufbauen und sich an der nationalen BMI-Studie beteiligen.

Im Kanton Luzern werden Schülerinnen und Schüler im Kindergarten, im 4. und 8. Schuljahr ärztlich untersucht. Ihre Angaben werden auf einer ärztlichen Schülerkarte festgehalten und vertraulich behandelt. Die Schüler- und Schülerinnenkarten werden in der Schule oder in der Praxis des Schularztes aufbewahrt.

Folgende Daten werden erfasst:

- Geburtstag
- Zeitpunkt der Untersuchung
- Geschlecht
- Körpergewicht
- Körpergrösse
- PLZ und Ort
- Angaben aus früheren Untersuchungen

Auf die Erfassung der Nationalität der Schülerinnen und Schüler wird auf Intervention des DSB verzichtet und die Dienststelle Gesundheit unterzeichnete ein entsprechendes Datenschutz-Revers.

• Pflegefinanzierung und Spitex

Die Elektronische Rechnungsstellung wird auf den 1.1.2013 eingeführt. Alle Organisationen, welche dem Administrativvertrag beigetreten sind, müssen spätestens an diesem Stichtag auf die elektronische Abrechnung umstellen.

Eine private Spitex-Organisation im Kanton Luzern mit staatlichem Leistungsauftrag stellte uns im Zusammenhang mit der neuen elektronischen Rechnungsstellung die Frage, ob Name, Vorname und Sozialversicherungsnummer der Klienten aufgeführt werden dürfen, damit die Gemeinde die Rechnung mit der Kostengutsprache vergleichen kann.

Für den Kanton Luzern bestimmt § 44 Abs. 3 des Gesundheitsgesetzes (SRL Nr. 800), dass für die Finanzierung der Pflegeleistungen im Sinne von Art. 25a KVG das kantonale Pflegefinanzierungsgesetz (SRL Nr. 867) gilt.

§ 44

1 Die Gemeinden sorgen für eine angemessene Krankenpflege und Hilfe zu Hause (Spitex) sowie für einen angemessenen Mahlzeitendienst.13
2 Sie können diese Aufgaben privaten oder öffentlich-rechtlichen Institutionen übertragen.
3 Die Gemeinden regeln die Finanzierung und tragen die Kosten, soweit sie insbesondere nicht durch Vergütungen der betreuten Personen und der Versicherer

gedeckt sind. Für die Finanzierung der Pflegeleistungen im Sinn von Artikel 25a des Bundesgesetzes über die Krankenversicherung14 gilt das Pflegefinanzierungsgesetz vom 13. September 201015.16

Gemäss § 4 des Pflegefinanzierungsgesetzes (SRL Nr. 867) werden die Grundsätze für die Rechnungsstellung durch die Leistungserbringer mittels Verordnung (SRL Nr. 867a) des Regierungsrates geregelt.

§ 4 Grundsätze der Rechnungstellung

Der Regierungsrat legt die Grundsätze für die Rechnungstellung durch die Leistungserbringer durch Verordnung fest.

Die Pflegefinanzierungsverordnung (SRL Nr. 867a) hält fest, dass die Rechnung der Leistungserbringer generell alle Angaben zu enthalten hat, die benötigt werden, um die Berechnung der Vergütung der Leistung überprüfen zu können (§ 1 Abs. 1) und eine direkte Rechnungsstellung an die Wohnsitzgemeinde bei Vorliegen einer Vollmacht der anspruchsberechtigten Person zulässig ist (§ 1 Abs. 2).

§ 1 Grundsätze

1 Die Leistungserbringer stellen der anspruchsberechtigten Person eine detaillierte und verständliche Rechnung zu. Diese hat alle Angaben zu enthalten, die benötigt werden, um die Berechnung der Vergütung der Leistung überprüfen zu können.

2 Bei Vorliegen einer Vollmacht der anspruchsberechtigten Person können die Leistungserbringer der Wohnsitzgemeinde für den Beitrag an die Pflegekosten direkt Rechnung stellen. Der anspruchsberechtigten Person ist auf Verlangen eine Kopie der Rechnung zuzustellen. Die Leistungserbringer können der Wohnsitzgemeinde für mehrere anspruchsberechtigte Personen mit Sammelrechnung Rechnung stellen.

Die Zulässigkeit der Verwendung der AHV-Versichertennummer ergibt sich aus § 17 Abs. 1 des kantonalen Registergesetzes (SRL Nr. 25) in Verbindung mit Art. 83 KVG.

§ 17 Systematische Verwendung

1 Die vom Bundesrecht ermächtigten Stellen und Institutionen, die mit dem Vollzug von kantonalem Recht betraut sind, dürfen die AHV-Versichertennummer für die Erfüllung ihrer gesetzlichen Aufgaben systematisch verwenden.

2 Folgende Stellen und Institutionen, die mit dem Vollzug von kantonalem Recht betraut und nicht unter Absatz 1 genannt sind, dürfen die AHV-Versichertennummer für die Erfüllung ihrer gesetzlichen Aufgaben systematisch verwenden:

a. Luzerner Polizei7,
b. Strassenverkehrsamt,
c. Grundbuchämter,
d. Gebäudeversicherung Luzern8,
e. Kantonsärztliche Dienste,
f. Kollektivhaushalte, die gemäss Bundesrecht an die Einwohnerregister Daten liefern müssen.

3 Andere Stellen und Institutionen dürfen die AHV-Versichertennummer zur Erfüllung ihrer gesetzlichen Aufgaben nur dann systematisch verwenden, wenn ein Gesetz dies vorsieht.

Art. 83 Versichertennummer der AHV

Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Versichertennummer der AHV nach den Bestimmungen des Bundesgesetzes vom 20. Dezember 1946181 über die Alters- und Hinterlasse-

nenversicherung für die Erfüllung ihrer gesetzlichen Aufgaben systematisch zu verwenden.

Zusammenfassend ergibt sich Folgendes: Vorausgesetzt die erwähnte Vollmacht für die direkte Rechnungsstellung liegt vor, ist die Angabe von Name, Vorname und Sozialversicherungsnummer auf den Rechnungen an die Gemeinde für die Berechnung der Vergütung der Leistung zulässig.

5. Bereich Soziales

- Sozialhilfebetreuerin verlangt Kontoauszüge

Eine Sozialhilfebetreuerin einer Luzerner Gemeinde ersucht einen Sozialhilfebezüger die Bankkontoauszüge der letzten drei Monate zur Überprüfung der Unterstützung einzureichen.

Gemäss § 11 Abs. 1 des kantonalen Sozialhilfegesetzes (SHG) haben Hilfsbedürftige über ihre wirtschaftlichen Verhältnisse vollständig und wahrheitsgetreu Auskunft zu geben und die dazu erforderlichen Unterlagen einzureichen.

§ 11 Auskunfts- und Meldepflicht

1 Der Hilfebedürftige hat bei der wirtschaftlichen Sozialhilfe, der Inkassohilfe, der Bevorschussung und der Mutterschaftsbeihilfe über seine wirtschaftlichen Verhältnisse vollständig und wahrheitsgetreu Auskunft zu geben und die zur Abklärung erforderlichen Unterlagen beizubringen.

2 Der Hilfebedürftige hat Änderungen seiner wirtschaftlichen Verhältnisse sofort zu melden.

Folglich verfügt die von der Sozialhilfebetreuerin angeordnete Massnahme über eine ausreichende gesetzliche Grundlage. Da nicht sämtliche Kontoauszüge seit Eintreten der wirtschaftlichen Notlage verlangt werden, sondern nur diejenigen der letzten drei Monate, ist die Massnahme überdies auch als verhältnismässig einzustufen. Schliesslich ist auch die Zweck-Mittel-Relation gewahrt, indem die eingeforderten Kontoauszüge über die Verwendung der Einkünfte bzw. der erhaltenen Sozialgelder Informationen enthalten, so dass die beabsichtigte Überprüfung der Unterstützungsbedürftigkeit damit erreicht werden kann.

Zusammenfassend ergibt sich, dass die verlangte Herausgabe der Kontoauszüge aus datenschutzrechtlicher Sicht nicht zu beanstanden ist.

6. Bereich Privat

- WLAN mit öffentlichem Zugriff

Ein Unternehmen im Bereich Tourismus stellte uns die Frage, wie weit ein öffentlicher Zugriff auf ein Wireless-Netzwerk kostenlos mit oder ohne Registrierung möglich wäre.

Auch wenn wie für diesen Fall nicht zuständig, möchten wir diese Anfrage gerne beantworten, da sich diese Fragestellung gleich oder ähnlich auch für kantonale oder kommunale Projekte (z.B. in Schulen stellen kann).

Es können zwei Probleme entstehen:

1. Problem Trittbrettfahrer: Drittpersonen surfen auf Ihre Kosten in Ihrem WLAN, schmälern dadurch für Sie die Bandbreite und laden eventuell illegale Inhalte herunter. Je nach Inhalt verstösst der Trittbrettfahrer damit meist unerkannt gegen das Urheberrechtsgesetz oder gar gegen das Strafgesetzbuch, nicht jedoch gegen das Datenschutzgesetz.
2. Problem Hacker: Drittpersonen hören die Funkkontakte innerhalb Ihres Netzwerks ab oder schleusen sich gar direkt in Ihre Geräte, Ihren Rechner ein und lesen, manipulieren oder stehlen Ihre Daten. Hier liegt

die Verletzung der Privatsphäre und damit des Datenschutzgesetzes auf der Hand.

Aus oben genannten Gründen (IT-Sicherheit und einer möglichen Haftung) empfehlen wir für den Betrieb einer kostenlosen WLAN-Infrastruktur die folgenden Massnahmen umsetzen:

1. Bieten Sie Ihr WLAN kostenlos an, aber mit einer einfachen Registrierung
2. Schützen Sie Ihr eigenes Netzwerk vom WLAN mit einer entsprechenden Firewall

7. Diverse

- Die Feuerwehr veröffentlicht Daten und Fotos auf deren Webseite

Eine private Person hat sich bei uns beschwert, dass die Feuerwehr schon wenige Stunden nach dem Brand seines Hofes mit Textinformationen und Fotos auf der Webseite der entsprechenden Feuerwehr veröffentlich hat. Mit Recht stellt er uns die Frage, ob dies gemäss dem Datenschutzgesetz erlaubt ist.

Bei den veröffentlichten Textinformationen handelt es sich teilweise um Personendaten im Sinne von § 2 Abs. 1 DSG, da es sich mit dem Hinweis auf die Örtlichkeit der Liegenschaft und Beteiligte (Bewohner) um Daten über bestimmbare Personen handelt (unabhängig davon, ob in dieser Liegenschaft mehrere Bewohner wohnen oder nicht). Dementsprechend fallen auch einschlägige Fotos der Liegenschaft unter die Kategorie der Personendaten.

Bei einer Feuerwehr handelt es sich um ein kommunales Organ (§ 3 Abs. 1 lit. b DSG). Das DSG, welches den Schutz von Personen vor unbefugtem Bearbeiten ihrer Daten durch öffentliche Organe bezweckt (§ 1 DSG), ist daher anwendbar.

§ 10 Abs. 1 DSG verlangt für die Bekanntgabe von Personendaten durch Organe an Private (z.B. wie vorliegend im Rahmen einer Internetveröffentlichung) das Vorliegen eines Rechtssatzes (lit. a), der zu dieser Datenbekanntgabe verpflichtet oder berechtigt, oder die ausdrückliche oder nach Umständen vorauszusetzende Einwilligung des Betroffenen (lit. b). In diesem Fall lag keine ausdrückliche Einwilligung der Betroffenen Person zur Veröffentlichung dieser Personendaten (Text und Fotos) vor. Somit ist § 10 Abs. 1 lit b DSG nicht erfüllt. Zu prüfen ist daher weiter, ob ein Rechtssatz ausdrücklich zu einer solchen Veröffentlichung verpflichtet bzw. diese erlaubt.

§ 8 der Verordnung zum DSG (DSV) zählt verschiedene Kategorien von Personendaten und Veröffentlichungsmöglichkeiten auf, die aber vorliegend nicht zutreffen.

Auch das kantonale Gesetz über den Feuerschutz (FSG) enthält keine einschlägigen Bestimmungen, die eine solche Veröffentlichung erlauben.

Gemäss Art. 7 Abs. 1 der Gemeindeordnung der entsprechenden Gemeinde informiert der Gemeinderat die Öffentlichkeit über wichtige Geschäfte und Beschlüsse, während amtliche Akten, an deren Geheimhaltung überwiegende öffentliche oder private Interessen bestehen, nicht öffentlich sind. Das amtliche Publikationsorgan der Gemeinde ist nach Art. 7 Abs. 2 der Gemeindeordnung die öffentliche Anschlagstelle. Publikationen können weiter in den Printmedien und im Internet erfolgen. gestützt auf Art. 16 Abs. 3 der Organisationsverordnung der Gemeinde sind Informationen von öffentlichem Interesse in der öffentlichen Anschlagstelle, in den Printmedien und im Internet zu publizieren.

Es ist noch darauf hinzuweisen, dass die Gebäudeversicherung Luzern auf Ihrer Webseite (www.gvl.ch) unter der

Rubrik Feuerwehr auf Hinweis von uns seit dem 28. April 2010 das Merkblatt «Veröffentlichung von Einsätzen und Einsatzfotos auf Homepages» um Download zur Verfügung stellt.

Anhand der obigen Ausführungen ist nun zu prüfen, ob die kommunalen Rechtsgrundlagen für die Veröffentlichung der vorliegend beanstandeten Personendaten ausreichen. Da es sich vorliegend nicht um wichtige Geschäfte und Beschlüsse handelt, besteht keine Informationspflicht durch den Gemeinderat bzw. die Feuerwehr als zuständiges Organ. Auch besteht kein überwiegendes öffentliches Interesse daran, den Ort, Beteiligte und Ablauf des Brandes zu veröffentlichen, so dass von einem überwiegenden privaten Interesse an der Nichtveröffentlichung ausgegangen werden darf.

Von öffentlichem Interesse sind hingegen folgende Informationen, die auf der Webseite hätten veröffentlicht werden dürfen:

- dass sich zu besagtem Zeitpunkt ein Brand ereignete,
- dass die Feuerwehr im Einsatz stand,
- dass Dritte durch ihr beherztes Eingreifen weiteren Sachschaden verhindert haben und eventuell sogar
- die Veröffentlichung der Fotos (sofern diese nicht direkt oder indirekt einer Person zugeordnet werden können).

Da durch diese Informationen keine Rückschlüsse auf die Person möglich wären, könnte dies aus Sicht des Datenschutzes nicht beanstandet werden.

Zusammenfassend ist eine Veröffentlichung von Informationen zum Brandfall auf der Webseite der Feuerwehr grundsätzlich zulässig, mangels ausreichender rechtlicher Grundlagen aber nicht in der vorliegend erfolgten Form. So reichen die rechtlichen Grundlagen insbesondere nicht dazu aus, Personendaten zu veröffentlichen. Bei der vorliegenden Veröffentlichung handelt es sich daher um ein widerrechtliches Bearbeiten von Personendaten.

Selbst wenn eine ausreichende rechtliche Grundlage für die Veröffentlichung vorhanden und damit § 10 Abs. 1 lit.a DSG erfüllt wäre, müsste die Datenverarbeitung verhältnismässig sein, was vorliegend ebenfalls nicht gegeben ist, da eine Veröffentlichung in milderer Form (ohne Angabe von Personendaten) möglich gewesen wäre.

- Persönlichkeitsschutz bei Abbildungen von Grabsteininschriften

Für eine Informationsbroschüre über die verschiedenen Gräberarten auf einem Friedhof einer Luzerner Gemeinde stellte sich folgende Frage: Ist es zur Bebilderung bzw. der verschiedenen Gräberarten möglich, Grabsteine mit den lesbaren Inschriften abzubilden oder wird die Gemeinde damit allenfalls wegen einer Persönlichkeitsverletzung gegenüber der Angehörigen angreifbar?

Grundsätzlich handelt es sich bei den Grabinschriften um Personendaten und bei der geplanten Broschüre – sollten die Inschriften auf Fotos ersichtlich sein – um einen Anwendungsfall von § 10 DSG zur Datenbekanntgabe.

§ 10 Bekanntgeben an Private

1 Unter Vorbehalt besonderer Geheimhaltungspflichten darf ein Organ privaten Personen und Organisationen Personendaten bekanntgeben, wenn

a. ein Rechtssatz dazu verpflichtet oder ermächtigt oder

b. die betroffene Person eingewilligt hat oder ihre Einwilligung nach den Umständen vorausgesetzt werden kann.

2 Personendaten aus allgemein zugänglichen amtlichen Veröffentlichungen darf ein Organ auf Anfrage in dem

Umfang und in gleicher Weise bekanntgeben, wie sie veröffentlicht worden sind.

3 Der Regierungsrat regelt das Bekanntgeben von Personendaten für Adressbücher und andere Nachschlagewerke sowie für Publikationen im Zusammenhang mit andern Vorgängen von allgemeinem Interesse.

Die in § 10 Abs. 3 DSG verankerte detaillierte Regelung durch den Regierungsrat für Veröffentlichungen wurde in § 8 der kantonalen Verordnung zum DSG (DSV) umgesetzt und enthält keine auf den vorliegenden Fall anwendbare Bestimmung.

§ 8 Bekanntgeben von Personendaten zur Veröffentlichung

1 Zur Veröffentlichung von Personendaten dürfen bekanntgegeben werden:

a. für Adressbücher und ähnliche Nachschlagewerke: Name, Vorname, Titel, Firma und Adresse von Personen und Personengesellschaften sowie deren Eigentum an Grundstücken am Wohnort oder Sitz;

b. für das Verzeichnis der Fahrzeughalter10 und Schiffshalter: Name, Vorname oder Firma und Adresse von Inhabern eines Kontrollschildes;11

c. für den Staatskalender, Behördenverzeichnisse und ähnliche Nachschlagewerke: Name, Vorname, Titel, Beruf, Geburtsjahr, Adresse, Heimatort sowie Funktion von Personen, die im öffentlichen Dienst stehen oder gestanden haben;

d. für Zeitschriften und andere periodische Veröffentlichungen und Mitteilungen: Personendaten im Zusammenhang mit Geburten, Todesfällen, Verkündungen und Trauungen nach Massgabe der Verordnung über das Zivilstandswesen12.

2 Vorbehalten bleiben die Sperre von Personendaten gemäss § 11 Absatz 4 des Datenschutzgesetzes und andere rechtmässig zugelassene Ausnahmen von der Veröffentlichung.

3 Auf das Bekanntgeben der Personendaten gemäss Absatz 1 besteht kein Rechtsanspruch.

Da weder dem Friedhof- und Bestattungsreglement noch der dazugehörigen Vollzugs- und Gebührenverordnung der Gemeinde einschlägige gesetzliche Bestimmungen zu entnehmen sind, ist davon auszugehen, dass die entsprechenden gesetzliche Grundlage im Sinne § 10 Abs. 1 lit. a DSG für eine solche Veröffentlichung von Fotos mit erkennbaren Grabinschriften in einem Prospekt fehlt. Jedenfalls kann nicht davon ausgegangen werden, dass mit der Beschriftung des Grabes bzw. Grabsteins, welche öffentlich zugänglich sind, auch die Berechtigung einhergeht, diese einer breiteren Öffentlichkeit mittels Prospekten zugänglich zu machen.

Da eine Einwilligung der Angehörigen den Umständen nach in diesen Belangen nicht einfach vorausgesetzt werden kann (§ 10 Abs. 1 lit. b DSG), müsste vorgängig die Einwilligung der betroffenen Angehörigen eingeholt werden. Sind solche Einwilligungen nicht erhältlich, weil die Angehörigen nicht auffindbar sind oder diese Einwilligung explizit verweigern, müsste auf die geplanten Fotos verzichtet werden oder aber diese so aufgenommen werden, dass die Grabschriften nicht lesbar sind.

D. Vorträge zum Thema Datenschutz und Informationssicherheit

Im Berichtsjahr wurden zum Thema Datenschutz und Informationssicherheit keine Vorträge gehalten. Aufgrund der herrschenden Ressourcenknappheit liess sich die erforderliche proaktive Sensibilisierung nicht umsetzen.

E. Datenschutz- und Sicherheitstipps für Privatpersonen

Privatpersonen können die Sicherheit ihrer persönlichen Informationen schon mit ein paar einfachen Regeln erhöhen. Der DSB gibt einige grundlegende Tipps zum Umgang mit den eigenen Daten im Internet und zum Schutz von PCs und Smartphones.

Datensparsamkeit

Grundsätzlich gilt es, mit den eigenen Daten sparsam umzugehen und bewusst zu entscheiden, welchen Diensten sie anvertraut werden. Je weniger persönliche Informationen im Internet zu einer Person vorhanden sind, desto schwieriger ist es für potenzielle Betrüger, diese zu missbrauchen. Die Daten-Sparsamkeit gilt auch bei der Registrierung für Internet-Dienste. Anwender sollten nur die unbedingt notwendigen Informationen angeben. Auf die Eingabe von Namen, Adressdaten oder gar Kontoverbindungen bei angeblich kostenlosen Online-Diensten sollte daher verzichtet werden. Auch bei Gewinnspielen ist besondere Vorsicht angebracht. Im Zweifel sollte auf die Eingabe persönlicher Informationen lieber verzichtet werden. Der sparsame Umgang mit den eigenen Daten betrifft auch Smartphone-Nutzer. Sie sollten die Ortungsfunktion ihres Geräts nur aktivieren, wenn dies für den gewünschten Dienst nachvollziehbar notwendig ist.

Private Daten schützen

Die Sparsamkeit mit den eigenen Daten ist auch deshalb wichtig, weil das Internet nichts vergisst. Selbst wenn persönliche Informationen bereits gelöscht wurden, können sie als Kopien an anderer Stelle im Internet noch vorhanden sein. Daher ist es wichtig, den Zugang zu privaten Informationen, beispielsweise in sozialen Netzwerken oder auf privaten Webseiten, zu beschränken. Auch im Alltag würden die meisten Menschen Unbekannten nicht ihr gesamtes Privatleben offenbaren. Der Zugriff auf persönliche Fotos oder die Kontaktdaten sollten nur guten Bekannten zugänglich gemacht werden. Potenziell peinliche Fotos und Texte in Netzwerk-Profilen sollten konsequent gelöscht werden oder am besten gar nicht online gehen.

Benutzername

Ob Internet-Nutzer besser mit ihrem echten Namen oder einem Pseudonym (Nickname) auftreten, hängt von der Art der Web-Plattform ab. Für Einträge in Fachforen, beim Twittern oder in Verbraucherportalen empfiehlt es sich, einen Nicknamen zu verwenden. Nur wenn man leichter gefunden werden möchte, sollte der echte Name genutzt werden. Das ist bei einigen Internet-Communitys oder sozialen Netzwerken üblich.

Eigener Ruf

Jeder sollte regelmässig mit Suchmaschinen prüfen, welche Informationen im Netz über seine Person vorhanden sind. Dies gilt insbesondere für alle, die viel veröffentlichen oder in der Öffentlichkeit arbeiten. Wer einen häufigen Namen trägt, gibt Vor- und Nachnamen in Anführungszeichen ein («Max Müller») und danach etwa Wohnort, Beruf oder Sportverein. So lassen sich Ergebnisse filtern. Neben allgemeinen Suchmaschinen wie Google oder Bing können auch spezielle Suchmaschinen für Personen genutzt werden. Diese beziehen auch soziale Netzwerke in die Suche ein.

Urheber- und Persönlichkeitsrechte

Wenn jemand Ihre Fotos oder Texte unerlaubt ins Netz gestellt hat, können Sie die Löschung verlangen. Dies gilt auch, wenn Ihnen das Bild nicht gehört, Sie aber darauf zu sehen sind. Jeder hat ein »Recht am eigenen Bild». Sie dürfen bestimmen, ob und in welchem Zusammen-

hang Bilder von Ihnen veröffentlicht werden. Daher sollten auch Sie keine Fotos von anderen veröffentlichen, ohne vorher zu fragen. Im privaten Umfeld sollte eine Aufforderung zur Löschung per E-Mail oder Telefon reichen.

Passwörter und Sperrcodes

Für viele Online-Dienste müssen die Nutzer ein Passwort zur Anmeldung benutzen. Um möglichst sichere Passwörter zu erzeugen und zu verwenden, gilt es daher ein paar Tipps zu beachten:

- Verwenden Sie nicht dasselbe Passwort bei mehreren Diensten
- Je länger das Passwort, desto sicherer. Es sollte mindestens acht, besser zehn Zeichen lang sein.
- Nutzen Sie willkürlich Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen
- Das Passwort sollte sich in keinem Wörterbuch wiederfinden.

Sichere Passwörter lassen sich leicht merken, wenn man sich einen Satz ausdenkt und dann jeweils die ersten Buchstaben der Wörter sowie die Satzzeichen als Passwort verwendet. Hilfreich sind auch spezielle Programme, sogenannte Passwort-Safes. Sie können die Geheimzahlen und Passwörter sicher speichern. Der Anwender braucht sich dann nur noch das Haupt-Passwort zu merken. Zudem sollten die Passwörter gelegentlich geändert werden. Gleiches gilt auch für die PIN und gegebenenfalls den Sperrcode von Mobiltelefonen.

Verschlüsselte Verbindungen

Sensible Informationen, etwa Konto- und Kreditkartendaten, sollten nur über verschlüsselte Verbindungen übertragen werden. Ob die Verbindung sicher ist, erkennen Sie an den Buchstaben »https» vor der Internetadresse oder an einem kleinen Schlosssymbol im Internet-Programm (Browser). Zunehmend sind sichere Webseiten auch an einer grün hinterlegten Adresszeile erkennbar, wenn sich der Betreiber einer unabhängigen Prüfung unterzogen hat. Zahlungen können per Lastschrift, Kreditkarte oder Rechnung erfolgen. Es gibt auch seriöse Bezahldienste, bei denen die Bankdaten einmalig hinterlegt werden. Vorkasse per Überweisung ist verbreitet, aber riskanter.

E-Mails und Chat

Öffnen Sie nur E-Mails, die von vertrauenswürdigen Absendern stammen und bei denen Sie sich den Hintergrund des Versandes plausibel erklären können. Denn technisch versierte Betrüger können die Absenderadresse fälschen. Dubiose Mails von unbekannten Absendern möglichst sofort löschen. Schadprogramme verbergen sich oft in Grafiken oder E-Mail-Anhängen. Verdächtige Dateien auf keinen Fall öffnen! Folgen Sie auch nicht den Links in verdächtigen E-Mails, denn diese können auf verseuchte Webseiten führen. Auch bei E-Mails von Kreditinstituten ist besondere Vorsicht geboten: Banken bitten Kunden unter keinen Umständen per Mail, vertrauliche Daten, wie Transaktionsnummern (TAN), im Netz einzugeben. Auch bei Chat-Nachrichten von Unbekannten ist Vorsicht geboten. Kriminelle versenden oft Links zu Webseiten mit Viren.

Online-Banking

Beim Online-Banking sollte man die offizielle Adresse der Bank immer direkt eingeben oder aber eigene Lesezeichen (Favoriten) aufrufen. Zudem muss darauf geachtet werden, dass die Verbindung, wie bei anderen Zahlvorgängen im Web verschlüsselt (https:) ist. Für Überweisungen und andere Kundenaufträge sind Transaktionsnummern (TANs) nötig. In den Anfängen des Online-Bankings konnten die Nutzer einen dieser Codes aus einer Liste frei

wählen. Sicherer ist das iTAN-Verfahren, bei dem die Codes nummeriert sind. Ein Zufallsgenerator der Bank bestimmt, welche TAN aus der Liste eingegeben werden muss. Noch weniger Chancen haben Kriminelle beim mTAN-Verfahren. Dabei werden die Codes per Kurzmitteilung direkt auf das Mobiltelefon geschickt. Weitere Schutzverfahren sind chipTAN und HBCI, bei denen der Kunde als Zusatzgeräte einen TAN-Generator oder ein Kartenlesegerät nutzt. Wichtig: Kreditinstitute fragen niemals mehr als eine TAN gleichzeitig ab. Auf der Webseite www.ebankingabersicher.ch der Hochschule Luzern erfahren Sie alles Notwendige für einen sicheren Umgang mit E-Banking.

PC-Schutz

Viren und andere Schadprogramme beeinträchtigen nicht nur die Funktion von PCs, sondern werden zunehmend zur Ausspähung digitaler Identitäten eingesetzt. Vor der ersten Internet-Nutzung müssen ein Anti-Viren-Programm und eine Firewall installiert werden, um den PC zu schützen. Diese Schutzprogramme sowie Betriebssystem und Internet-Programm des PCs müssen regelmässig aktualisiert werden. Da Schadsoftware auch über Datenträger, wie DVDs und CDs, USB-Sticks und Speicherkarten, verbreitet wird, sollten auch diese regelmässig überprüft werden. Tipps gibt es beispielsweise unter www.bis-fuer-buerger.de.

Schutz für Smartphone-Nutzer

Schadprogramme gibt es auch für Smartphones. Um Sicherheitslücken zu schliessen, müssen die Updates der Geräte-Hersteller regelmässig installiert werden. Es ist ratsam, grundsätzlich alle Daten zu verschlüsseln. Bei Verlust des eigenen Mobiltelefons sollten die eigenen Daten aus der Ferne gelöscht werden. Für viele Smartphones ist dies kostenlos. Nutzer von Apples iPhone können sich unter www.icloud.com für den Service registrieren. Für Smartphones mit dem Microsoft Betriebssystem Windows Phone gibt es einen ähnlichen Service unter www.windowsphone.com. Auch viele Hersteller von Android-Smartphones, etwa Samsung oder Motorola, bieten die Fernlöschung des eigenen Geräts an.

Funkverbindungen

Smartphone-Nutzer sollten Funkverbindungen, wie WLAN oder Bluetooth, nur dann aktivieren, wenn diese tatsächlich benötigt werden. Potenziellen Angreifern wird dadurch der Zugriff auf das Gerät erschwert. Zudem sollten sensible Informationen nicht über ungesicherte WLAN-Netze übertragen werden. Nur Drahtlos-Netzwerke, die den Standard WPA2 verwenden, bieten ausreichend Schutz für persönliche Daten, da eine verschlüsselte Übertragung genutzt wird.

F. Interkantonale Zusammenarbeit

Der Kanton Luzern ist Mitglied des Vereins privatim. Dieser Verein bezweckt eine interkantonale Zusammenarbeit im Bereich des Datenschutzes, damit die Mitglieder (vorwiegend kantonale DSB), die allesamt über beschränkte Mittel verfügen, gewisse Arbeiten effizienter bewältigen bzw. aufteilen können.

Die Arbeitsgruppe «Schule» hat sich im Berichtsjahr mit verschiedenen datenschutzrechtlichen Themen im Bereich Schule befasst und mittels einer Umfrage direkt bei den verschiedenen Bildungsinstitutionen den Unterstützungs- und Koordinationsbedarf in den beteiligten Kantonen ermittelt. Der DSB ist Mitglied der Arbeitsgruppe «Schule».

Die Arbeitsgruppe «ICT» beschäftigte sich im Berichtsjahr mit den Themen Cloud Computing und Spitalkontrollen (Anforderungen an Klinikinformationssysteme). Der Mitarbeiter des DSB, Wolfgang Sidler, ist Mitglied der Arbeitsgruppe «ICT».

Privatim führt zwei Mal jährlich ein Plenum durch, bei dem sich die Mitglieder zwecks Besprechung von und Austausch in aktuellen Datenschutzfragen treffen. Diese Veranstaltungen werden abwechslungsweise von einzelnen Mitgliedern organisiert und fanden im Berichtsjahr in Bellinzona und Fribourg statt.

G. www.datenschutz.lu.ch

Die Webseite enthält verschiedene inhaltlich gegliederte Rubriken. Sie verweist auf die wichtigsten Rechtsgrundlagen im Bundes- und kantonalen Recht. Folgende Themen werden speziell bearbeitet und in Form von Merkblättern aktualisiert: Schulen, Gesundheitswesen, Informatik, Videoüberwachung, Polizei und Diverses. Der Besucher kann auch Formulare, Checklisten und andere hilfreiche Unterlagen herunterladen. Zudem werden die Publikationen des DSB auf der Webseite veröffentlicht. Schliesslich wird auch die Möglichkeit angeboten, dem Unterzeichnenden über das Kontaktformular Fragen zu stellen.

Die Kennzahlen der Besucher Analyse zeigen auf, wie unsere Datenschutz-Webseite www.datenschutz.lu.ch besucht wurde. Die Zahlen zeigen, dass das Bedürfnis einer Datenschutz-Webseite ausgewiesen ist. Der DSB hätte zwischen Januar und Dezember 2012 nie die entsprechenden Fragen beantworten können, wenn die interessierten Personen angerufen hätten, statt auf die Webseite zu gehen. Das neue Gesetz über die Videoüberwachung wurde am häufigsten heruntergeladen, an zweiter Stelle der Tätigkeitsbericht 2010 und an dritter Stelle das Merkblatt zum Thema Amtsgeheimnis.

	2010	2011	2012	Entwicklung (11–12)
Besucher Insgesamt	3'189	2'788	2'946	+5.7%
Besucher pro Tag	8	7	8	
Seitenansichten Insgesamt	10'560	7'190	7'877	+9.5%
Seitenansichten pro Tag	28	19	21	

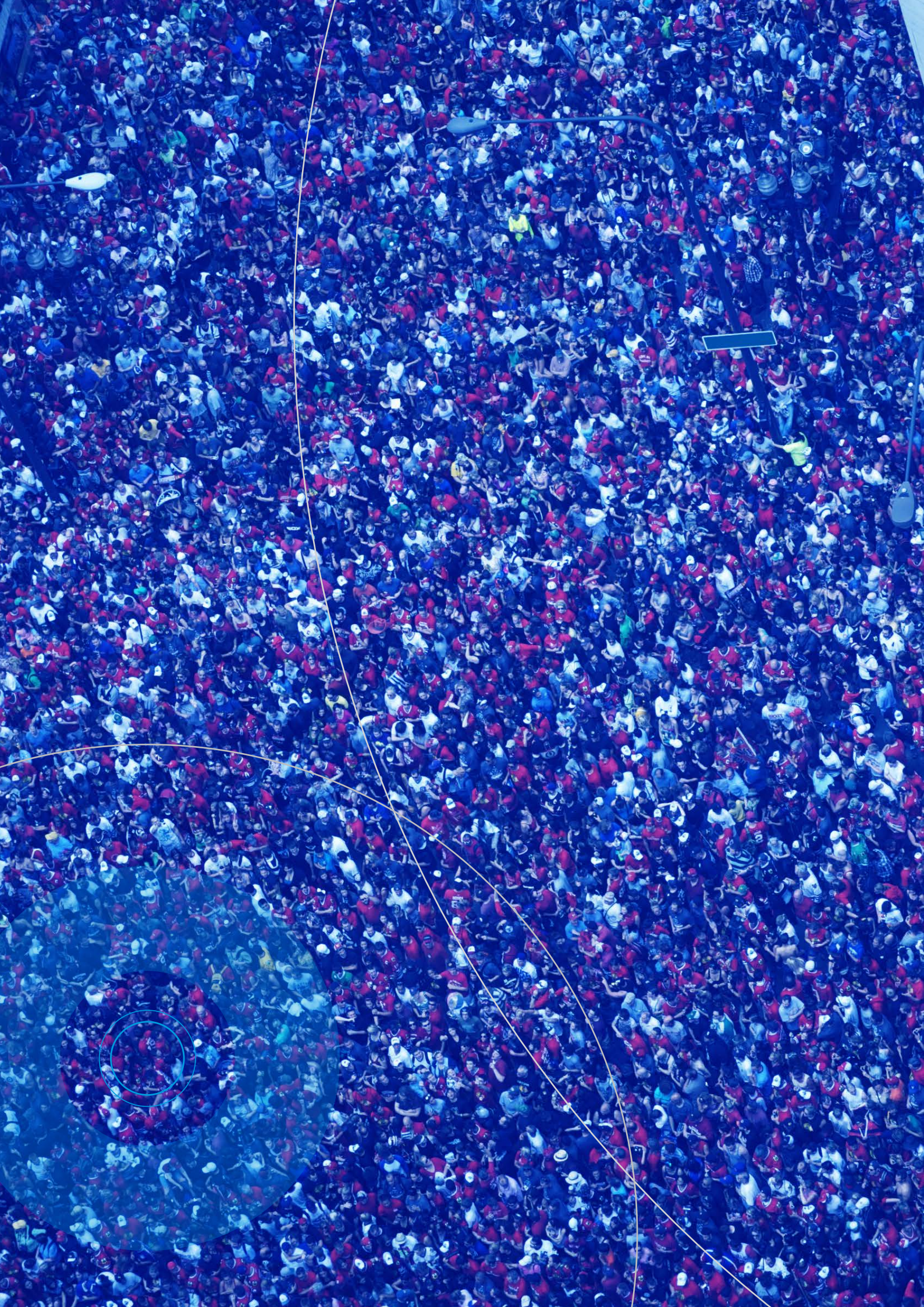
H. Medienarbeit

Aufgrund der geringen personellen Ressourcen und des grossen Arbeitsdrucks ist nicht an eine umfassende und proaktive Informationspolitik seitens des DSB zu denken. Dies ist problematisch, da die Information der Bevölkerung auch zu den Aufgaben des DSB gehört, was die europäischen Instanzen im Rahmen der Überprüfung der Datenschutztätigkeiten in der Schweiz unterstrichen und deren Umsetzung gleichzeitig bemängelt haben. Es konnte daher lediglich auf Medienanfragen reagiert werden. Solche Anfragen umfassten im Berichtsjahr hauptsächlich die Themen Veröffentlichung von Fotos bei Pyrovorfällen, potentiell gewalttätige Personen, Tablet-Computer und E-Books im Kantonsrat/Unterricht, Stimmregisterzugriff der Parteien, Datenaustausch Polizei-Caritas bei Verhaftungen von Asylbewerbern, Hotelkontrolle, Medienauskünfte von Luzerner Polizei und Kantonsspital bei Verkehrsunfällen mit Personenschaden sowie Öffentlichkeitsfahndung bei Ausschreitungen von Fussballfans.

I. Ausblick

Die bestehenden Herausforderungen wie «Cloud Computing» und «Bring Your Own Device» werden den DSB und dessen Mitarbeiter weiterhin mit interessanten Anforderungen, Projekten und Fragestellungen aktiv beschäftigen.
Im Bereich E-Government ist der DSB zur Zeit in erste Projekte involviert worden und wird mit zunehmender Umsetzung der kantonalen Strategie und laufendem Betrieb noch vermehrt datenschutzrelevante Fragen zu prüfen und beantworten haben.

Die aktuellen rechtlichen, technischen und gesellschaftlichen Entwicklungen wirken sich direkt auf die öffentlichen Verwaltungen im Kanton Luzern aus und erfordern künftig entsprechende Beratungs- Schulungs- und Kontrollkapazitäten seitens des Datenschutzes, um den gesteigerten Anforderungen von Behörden sowie Bürgerinnen und Bürgern nachkommen zu können (Zunahme der Geschäftsfälle im Berichtsjahr um 63%).



Adressen

Datenschutzbeauftragter
des Kantons Luzern
Murbacherstr. 21
6002 Luzern
Telefon 041 228 66 06
datenschutz@lu.ch
www.datenschutz.lu.ch

Eidgenössischer Datenschutz-
und Öffentlichkeitsbeauftragter
Feldeggweg 1
Postfach
3003 Bern
Tel. 031 322 43 95
www.edoeb.admin.ch

Nützliche Websites anderer Kantone oder Vereinigungen

www.baselland.ch/datenschutz
www.datenschutz-zug.ch
www.datenschutz.ch
www.privatim.ch

900145 diekonkreten.ch

KANTON LUZERN

Datenschutzbeauftragter
Murbacherstrasse 21
6002 Luzern