

Datenschutzbeauftragter des Kantons Zug  
Tätigkeitsbericht 2011 [Nr. 13]

### Tätigkeitsbericht 2011 [Nr. 13]

Der Datenschutzbeauftragte hat dem Kantonsrat und dem Regierungsrat jährlich einen Bericht über seine Tätigkeit zu erstatten. Der Bericht ist zu veröffentlichen.<sup>1</sup>

Der vorliegende Tätigkeitsbericht Nr. 13 deckt den Zeitraum zwischen 1. Januar 2011 und 31. Dezember 2011 ab.

Er ist auch auf der Website des Datenschutzbeauftragten veröffentlicht:  
«[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)»

Zug, 12. Januar 2012

Datenschutzbeauftragter des Kantons Zug  
Dr. iur. René Huber

### Ein wichtiger Hinweis

Der Datenschutzbeauftragte des Kantons Zug befasst sich mit der Datenbearbeitung der kantonalen und gemeindlichen Zuger Verwaltung.

Für die Datenbearbeitung von privaten Unternehmen [Versicherern, Banken, privaten Arbeitgebern, Hausärzten etc.] sowie der Bundesverwaltung ist der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte<sup>2</sup> zuständig.

**ISSN 1424-4756**

#### Ein paar häufig verwendete Abkürzungen:

Abs.	Absatz
BGS	Bereinigte Gesetzesammlung [Kt. Zug]
Bst.	Buchstabe
DS	Datenschutz
DSB	Datenschutzbeauftragter
DSG	Datenschutzgesetz
EDÖB	Eidg. Datenschutz- und Öffentlichkeitsbeauftragter
E-DSG	Eidg. Datenschutzgesetz
GVP	Gerichts- und Verwaltungspraxis des Kantons Zug
IT	Informatik-, Informationstechnologie
SR	Systematische Sammlung des Bundesrechts
TB	Tätigkeitsbericht

<sup>1</sup> § 19 Abs. 1 Bst. h Datenschutzgesetz des Kantons Zug.

<sup>2</sup> Eidg. Datenschutz- und Öffentlichkeitsbeauftragter  
Feldeggweg 1  
3003 Bern  
Telefon 031 322 43 95  
«[www.edoeb.admin.ch](http://www.edoeb.admin.ch)».

#### Datenschutzstelle des Kantons Zug

Regierungsgebäude, Seestrasse 2  
Postfach 156, 6301 Zug  
Tel. 041 728 31 47, Fax 041 728 37 01  
[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)

# Inhaltsverzeichnis

---

Neu – das Recht auf Vergessen	2
Sie sind in Eile? – Das Wichtigste des Jahres 2011	3

---

<b>I. Grundlegende Themen und Projekte</b>	<b>4</b>
1. facebook, twitter & Co. – bald auch in der Zuger Verwaltung?	4
2. Datenschutzbeauftragter muss den Kantonsrat besser informieren	4
3. Datenschutz im Spital	5
4. Die Finanzkontrolle überprüft die Datenschutzstelle	6
5. Weiterbildung des Zuger Kaders	6
6. Wichtiges zur Datensicherheit	7

---

<b>II. Fälle aus unserer Beratungspraxis</b>	<b>9</b>
1. Übersicht	9
2. Personalrecht	10
3. Schule	13
4. Sicherheit	14
5. Kanton	15
6. Gemeinden	18

---

<b>III. Unsere Öffentlichkeitsarbeit</b>	<b>19</b>
1. Website	19
2. Newsletter	19
3. Tätigkeitsbericht 2010	20
4. «Gerichts- und Verwaltungspraxis des Kantons Zug»	20
5. «Schulinfo Zug»	21
6. «Personalzeitung»	21
7. In der Zeitung – die Kolumne «Ratgeber Datenschutz»	21
8. Zuger Datenschutz in den Medien	21

---

<b>IV. Mitarbeit bei der Gesetzgebung</b>	<b>22</b>
1. Vernehmlassungen	22
2. Unsere Mitarbeit bei ausgewählten Rechtserlassen	23

---

<b>V. Register der Datensammlungen</b>	<b>27</b>
--	-----------

---

<b>VI. Weiterbildung</b>	<b>28</b>
--------------------------	-----------

---

<b>VII. Zusammenarbeit der Datenschutzbeauftragten</b>	<b>29</b>
--	-----------

---

<b>VIII. Wir über uns</b>	<b>30</b>
---------------------------	-----------

---

Dank	31
Sachregister	32
Nützliche Adressen	33

## Neu – das Recht auf Vergessen

Liebe Leserin  
Lieber Leser

Es wird Sie nicht erstaunen: Über uns alle werden immer mehr Daten gesammelt, verarbeitet, weitergegeben und – gespeichert. Gespeichert werden Daten in aller Regel für immer und ewig. Wer einmal Daten über uns hat, gibt sie nicht mehr her. Das scheint fast schon ein Naturgesetz zu sein. Wir werden nicht gefragt, ob uns das passt, auch nicht, ob die Daten über uns überhaupt noch aktuell und richtig sind. Wird mit falschen Daten über uns gearbeitet, haben jedoch wir den Schaden.

Ewiges Speichern? Das will die EU nun ändern. Im soeben vorgelegten Entwurf zu einem neuen und in der ganzen EU direkt anwendbaren Datenschutzerlass<sup>3</sup> ist das «Recht auf Vergessenwerden und auf Löschung» verankert.<sup>4</sup> Was sprachlich etwas sperrig daherkommt, will sagen: Es soll ein Recht auf Löschung der persönlichen Daten geben. Damit will die EU die Privatsphäre des Einzelnen gegenüber Staat und Wirtschaft deutlich stärken.

Beabsichtigt ist dabei ganz bewusst auch eine Beeinflussung der technischen Entwicklung, bezieht sich der Löschanpruch doch ausdrücklich auch auf Daten, die im Internet veröffentlicht wurden.

Wir sollen bezüglich der Nutzung unserer Daten zukünftig somit nicht mehr schutzlos Staat und Wirtschaft ausgeliefert sein. Damit ist ein wichtiges und erfreuliches Zeichen für die Stärkung unserer Privatsphäre gesetzt.

Dieser Entwicklung werden sich auch Bund und Kantone in Zukunft nicht entziehen können.

Dr. iur. René Huber  
Datenschutzbeauftragter des Kantons Zug

<sup>3</sup> Zurzeit ist der Datenschutz in einer EU-Richtlinie geregelt. Richtlinien müssen in jedem Mitgliedsstaat noch im Rahmen der nationalen Gesetzgebung umgesetzt werden. Sie überlassen den einzelnen Staaten einen gewissen Spielraum. Deshalb gibt es in der EU eine datenschutzrechtliche Vielfalt. Neu wird die EU den Datenschutz im Rahmen einer EU-Verordnung regeln. In der schweizerischen Terminologie handelt es sich dabei um ein formelles Gesetz, das direkt und zwingend in allen Mitgliedsstaaten anzuwenden ist. Damit wird eine EU-weite Harmonisierung erreicht.

<sup>4</sup> Art. 17 des Vorschlags betreffend «Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [Datenschutz-Grundverordnung] vom 25. Januar 2012.

# Sie sind in Eile? – Das Wichtigste des Jahres 2011

## Was ist Datenschutz? – 20 Fälle aus unserer Praxis

Damit Sie sehen, worum es beim Datenschutz konkret geht, stellen wir Ihnen 20 Beispiele aus unserer Beratungspraxis vor. Alle Fälle auf einen Blick – in der Übersichtstabelle am Anfang.

[Näheres S. 9](#)

## Grundlegendes

Wie sieht es mit facebook & Co. in der Zuger Verwaltung aus? Wie soll der Datenschutzbeauftragte zukünftig den Kantonsrat besser über den Datenschutz informieren? Was ergab die Revision der Finanzkontrolle beim Datenschutzbeauftragten? Wie ist der Datenschutz im Spital geregelt? Wie soll zukünftig das Kader der Zuger Verwaltung bezüglich Datenschutz ausgebildet werden?

[Näheres S. 4](#)

## 1492 Zuger Datensammlungen!

Wer bearbeitet welche Daten wozu und über wen? Das zeigt Ihnen das Register über alle Datensammlungen, die bei der kantonalen und gemeindlichen Verwaltung vorhanden sind. Wir führen dieses Register. Zurzeit sind 1492 Datensammlungen bei uns registriert. Das Register steht Ihnen auf unserer Website zur Verfügung.

[Näheres S. 27](#)

## Aktuelles zur Datensicherheit

Die Themen: Datensicherheit beim Kopiergerät, Schulung der Mitarbeitenden bezüglich Datenschutz und Datensicherheit und die Rolle des DSB bezüglich der IT-Sicherheit.

[Näheres S. 7](#)

## Wichtiges aus der Gesetzgebung

Neben vielen anderen Gesetzgebungsprojekten haben wir vertieft bei der Änderung des Datenschutzgesetzes und des Polizeigesetzes im Zusammenhang mit Schengen sowie bei den neuen Gesetzen bezüglich Geoinformation und Videoüberwachung mitgearbeitet. Auch die Regelung der verdeckten polizeilichen Vorermittlung war ein wichtiges Thema.

[Näheres S. 22](#)

## Elektronischer Newsletter der Datenschutzstelle

Über Aktuelles aus Datenschutz und Datensicherheit informieren wir Sie in Kurzform kostenlos per E-Mail. Im Berichtsjahr haben wir über 20 Nachrichten verschickt und über 65 Neuabonnierte gewinnen können.

[Näheres S. 19](#)

## Internationales

Der DSB hat an der Frühjahrskonferenz der europäischen Datenschutzbeauftragten in Brüssel teilgenommen.

[Hinweis: An dieser Konferenz hat der DSB in seiner Freizeit teilgenommen; für Kosten und Spesen kam er selber auf.]

[Näheres S. 29](#)

# I. Grundlegende Themen und Projekte

## 1. facebook, twitter & Co. – bald auch in der Zuger Verwaltung?

Für die Verwaltung stellen sich bezüglich der sozialen Netzwerke [oder «Social Media»] zwei Fragen: Sollen die Mitarbeitenden diese Dienste während der Arbeitszeit für private Zwecke nutzen dürfen? Und: Soll die Verwaltung über diese Kanäle Informationen verbreiten? Hier befassen wir uns nur mit dem zweiten Thema.<sup>5</sup>

Bis anhin stellte der Kanton der Öffentlichkeit insbesondere via Website Informationen zur Verfügung. Dieser Kommunikationskanal ist «einspurig». Im Gegensatz dazu sind die sozialen Netzwerke meist «zweispurig», es kann zwischen Bevölkerung und Verwaltung eine Kommunikation entstehen. Verschiedene Verwaltungen in der Schweiz nehmen deshalb hier aktiv teil. Wie sieht es in der Zuger Verwaltung aus?

Der Regierungsrat hat bereits im Juni 2010 entschieden, einen allfälligen Einsatz von Social Media in der kantonalen Verwaltung vorerst von einer Studiengruppe von Master-Studierenden der Universität Lugano bis Ende 2011 untersuchen zu lassen. Gestützt darauf hat die Fachgruppe Kommunikation dem Regierungsrat Bericht und Antrag zu stellen.

Die Studiengruppe befragte verschiedene Exponenten der Verwaltung, darunter auch den DSB. Im Sommer organisierte sie einen halbtägigen Workshop, an dem auch der DSB teilnahm. Im November hat die Fachgruppe Kommunikation den DSB eingeladen, in grundsätzlicher Weise über Datenschutz und Datensicherheit bei sozialen Netzwerken zu informieren. Wir machten insbesondere auf Folgendes aufmerksam:

- Da alle Publikationen in Social Media öffentlich sind, dürfen hier keine Personendaten veröffentlicht werden.
- Die meisten Anbieter sind private US-Firmen, die Datenbearbeitung findet in aller Regel in den USA statt, der Kanton verliert mit der Veröffentlichung von Daten praktisch die

Herrschaft darüber. Die Firmen haben keinen Sitz in der Schweiz, gegen Vertragsänderungen und Vertragsverletzungen – etwa: bei Löschung von Daten oder Sperren des Kontos – stehen keinerlei Mittel zur Verfügung.

- Bei facebook handelt es sich nicht um eine Wohltätigkeitsveranstaltung. Die Nutzung aller Dienste ist zwar kostenlos – bezahlt wird jedoch mit den Daten. Die Dienste sammeln, verwalten und verkaufen die Daten über die User. So insbesondere über ihr Surfverhalten, ihre Vorlieben, ihre Vernetzung und alle ihre persönlichen Angaben und Bilder. Verschiedene Dienste sind deshalb datenschutzrechtlich sehr umstritten, so etwa die Nutzung des «like-buttons» von facebook. Der Staat darf unzulässige Dienstleistungen nicht nutzen. Er darf aber auch nicht Private dazu verleiten, dass deren Daten missbraucht werden. Deshalb hat etwa der Datenschutzbeauftragte von Schleswig-Holstein der Landesverwaltung unter Strafandrohung untersagt, facebook zu nutzen.<sup>6</sup>
- Es wird sorgfältig zu prüfen sein, ob und unter welchen Bedingungen die Nutzung welcher Dienste gemäss schweizerischem und zugerischem Recht zulässig ist.

Der Regierungsrat wird im ersten Quartal des Jahres 2012 über das weitere Vorgehen bezüglich facebook & Co. entscheiden. Über Aktuelles werden wir Sie in unserem Newsletter informieren.<sup>7</sup>

## 2. Datenschutzbeauftragter muss den Kantonsrat besser informieren

Im Zusammenhang mit der Beratung der gesetzlichen Regelung der polizeilichen verdeckten Vorermittlung<sup>8</sup> stellte die Kommission des Kantonsrates fest, dass ihr die Hinweise des Datenschutzbeauftragten nicht bekannt waren. Kurzfristig stellte der DSB der Kommission seine

5 «Online-Dienste wie interaktive Medien, SMS, Chatrooms, Newsgroups und dergleichen sind zur privaten Nutzung verboten» – so lautet ausdrücklich § 9 der Verordnung über die Benutzung von elektronischen Geräten und elektronischen Kommunikationsmitteln im Arbeitsverhältnis [BGS 154.28].

6 Als problematisch werden insbesondere erachtet: «like-button», Auswertung der Fotos mit Gesichtserkennungssoftware, häufige und einseitige Änderung der Vertragsbedingungen seitens der Anbieter. Vgl. das aufschlussreiche Dossier unter: «www.datenschutz-zentrum.de».

7 Siehe dazu hinten S. 19.

8 Näheres zu dieser Gesetzesrevision siehe hinten S. 24.

Stellungnahme zu, es fand ein Gespräch zwischen dem Kommissionspräsidenten und dem Datenschutzbeauftragten statt und ebenfalls kurzfristig lud die Kommission den DSB ein, seine Überlegungen anlässlich der Kommissionssitzung zu präsentieren.<sup>9</sup>

Dass Kommissionen des Kantonsrats über datenschutzrechtliche Probleme nicht genügend informiert wurden, ist verschiedentlich auch schon früher vorgekommen. Der Grund lag darin, dass die entsprechenden Berichte des Regierungsrates an den Kantonsrat auf früher abgegebene Stellungnahmen des DSB nicht oder nur rudimentär eingingen.

Das Büro des Kantonsrates lud den Datenschutzbeauftragten deshalb am 26. Mai 2011 zu einer Besprechung ein, an der beschlossen wurde, dass der Datenschutzbeauftragte in Zukunft die entsprechenden Kommissionen, Fraktionen oder auch den Gesamtrat von sich aus, somit proaktiv, zu informieren hat, falls aus seiner Sicht Informationsbedarf bezüglich Datenschutz/Datensicherheit besteht. Damit wurde eine klare Regelung getroffen, die den Informationsfluss verbessert. Im Berichtsjahr hat der DSB in zwei weiteren Fällen den entsprechenden Kommissionen Stellungnahmen zugestellt.<sup>10</sup> Bei der Beratung des Geoinformationsgesetzes hat die Kommission den DSB in der Folge zu einer Fragerunde anlässlich ihrer Beratung eingeladen.

Fazit: Es ist klargestellt, dass es am Datenschutzbeauftragten liegt, Kommissionen des Kantonsrats oder auch den Gesamtrat über wesentliche Anliegen des Datenschutzes zu informieren.

Ohne Weiteres können Rats- und Kommissionsmitglieder auch jederzeit von sich aus Dienstleistungen des Datenschutzbeauftragten beanspruchen.

### 3. Datenschutz im Spital

Die grundlegenden Änderungen im Gesundheitswesen – Stichwort Fallpauschale/«SwissDRG» –, die ab dem 1. Januar 2012 in Kraft getreten sind, haben auch Auswirkungen auf die Datenbearbeitung im Spital. Im Rahmen der Vernehmlassung der «Spitalliste 2012» machten wir die Gesundheitsdirektion auf Folgendes aufmerksam:

1. Alle Spitäler – somit auch Privatspitäler –, die Leistungen im Rahmen der obligatorischen Krankenversicherung erbringen, unterstehen diesbezüglich dem kantonalen Datenschutzrecht des jeweiligen Standortkantons. Aufsichtsorgan bezüglich der Datenbearbeitungen ist die kantonale Datenschutzaufsichtsstelle des Standortkantons des Spitals. Für Zuger Spitäler kommt demnach das Datenschutzrecht des Kantons Zug zur Anwendung, Aufsichtsbehörde ist der Zuger Datenschutzbeauftragte. Darauf sind die entsprechenden Spitäler ausdrücklich aufmerksam zu machen.
2. Der Kanton darf nur solche Spitäler auf die Spitalliste nehmen, welche die Vorgaben bezüglich Datenschutz und Datensicherheit einhalten beziehungsweise sich ausdrücklich dazu verpflichten.
3. Bei der Genehmigung der Tarifverträge durch den Regierungsrat wird dieser zu überprüfen haben, ob die Datenbekanntgabe insbesondere bezüglich der Rechnungsstellung zwischen Leistungserbringer und Versicherer rechtmässig – somit insbesondere: verhältnismässig –, ausdrücklich und detailliert geregelt ist.<sup>11</sup>

Damit ist Grundlegendes bezüglich der Datenbearbeitung in den Zuger Spitälern geklärt. Die Umsetzung der kantonalen Vorgaben in den Bereichen Datenschutz und Datensicherheit liegt in der Verantwortung der jeweiligen Spitäler. Die Aufsicht steht in erster Linie der Gesundheitsdirektion zu, aber auch der DSB hat hier Aufsichtsfunktionen. Er steht daneben allen verantwortlichen Stellen auch für Beratung und Unterstützung zur Verfügung.

9 Was leider nicht möglich war, da der DSB zu diesem Zeitpunkt an der Konferenz der europäischen Datenschutzbeauftragten in Brüssel teilnahm [s. dazu hinten S. 29].

10 Bei der Beratung des Einführungsgesetzes zum ZGB [Vorlage Nr. 2036.1 - 13731] und bezüglich dem Geoinformationsgesetz [Vorlage Nr. 2068.1 - 13848], siehe dazu hinten S. 25.

11 Gestützt auf § 7 Abs. 2 des Spitalgesetzes [BGS 826.11, am 1. 1. 2012 in Kraft getreten].

## 4. Die Finanzkontrolle überprüft die Datenschutzstelle

Im Berichtsjahr hat sich die Finanzkontrolle beim Datenschutzbeauftragten für eine sogenannte «Amtsrevision» der Datenschutzstelle angekündigt. Dazu ist vorweg zu bemerken, dass die Datenschutzstelle kein «Amt» ist. Die Datenschutzstelle ist vollständig unabhängig, nicht hierarchisch in die Verwaltung eingegliedert<sup>12</sup> und sie verfügt über ein eigenes Budget, das direkt durch den Kantonsrat beschlossen wird.

Es stellt sich deshalb die Frage, welche Kontrollbefugnisse der Finanzkontrolle im Einzelnen gegenüber der Datenschutzstelle zustehen. Diese Frage stellt sich noch akzentuierter, wenn der Datenschutzbeauftragte – wie die Ombudsfrau – durch den Kantonsrat gewählt wird. Im Rahmen der laufenden Revision des Datenschutzgesetzes wird dieser Problembereich voraussichtlich noch geklärt werden. Unbestritten dürfte sein, dass die Finanzkontrolle die buchhalterische Korrektheit des Rechnungswesens überprüfen kann.

Unabhängig von diesen Überlegungen kann gesagt werden, dass der DSB über die Revision sehr erfreut war, ist es doch für unabhängige Organe besonders wichtig, dass das Rechnungswesen korrekt, rechtmässig und in jeder Beziehung einwandfrei geführt wird und dies auch durch eine externe Stelle geprüft wird. Der Besuch des Revisors war somit – anders als bei Gogol – sehr erwünscht.

Der Prüfungsbereich bezog sich auf den Personal- und Sachaufwand der Jahresrechnung 2010 und, soweit im Oktober 2011 bereits verbucht, der Jahresrechnung 2011 auf der Basis von Stichproben. Das Revisionsergebnis der Finanzkontrolle vom 18. Oktober 2011 lautete: «Im Rahmen unserer stichprobenweise durchgeführten Revision haben wir in den Bereichen Rechnungsführung, Personalaufwand, Arbeitszeit- und Ferienkontrolle sowie Sachaufwand im geprüften Zeitraum Ordnungsmässigkeit festgestellt.»

## 5. Weiterbildung des Zuger Kaders

Im Herbst entwickelten Finanzdirektion und Personalamt ein Weiterbildungskonzept [WBK] für Führungspersonen. Das Kader der Verwaltung besteht, mit Einbezug der Stellvertretenden, aus rund 200 Personen und setzt sich in etwa wie folgt zusammen: 80 Personen des unteren, 60 des mittleren und 60 des obersten Kaders.

Der DSB wurde eingeladen, sich zum Konzeptentwurf zu äussern. Wir begrüssten das Konzept sehr und beantragten, Kurse in Datenschutz und Datensicherheit für das gesamte Kader vorzusehen, stellen wir doch immer wieder fest, dass vielen Führungspersonen nicht bekannt ist, welche Vorgaben das Datenschutzrecht und das Datensicherheitsrecht machen. Für viele Aufgabenbereiche sind grundlegende diesbezügliche Rechtskenntnisse jedoch wichtig.

Ende Berichtsjahr hat der Regierungsrat das neue Weiterbildungskonzept für Führungspersonen in erster Lesung beraten.<sup>13</sup> Wir werden einen Grundkurs und einen darauf aufbauenden Kurs für alle Personen des Kaders anbieten. Die beiden je halbtägigen Kurse haben folgenden geplanten Inhalt:

«BASIS-Kurs Datenschutz Teil 1»: Sensibilisierung bezüglich Schutz der Privatsphäre, Vorstellen der wichtigsten Rechtsgrundlagen und der datenschutzrechtlichen Grundprinzipien, Rechte der EinwohnerInnen, Konzept des Registers der Datensammlungen, Grundsätze der Datensicherheit.

«AUFBAU-Kurs Datenschutz Teil 2»: Regelung der Datenbearbeitung bei Gesetzesprojekten, Datensicherheit bei IT-Projekten, Datenschutz bei Outsourcing und Leistungsvereinbarungen, Erstellen des Massnahmenplans Datensicherheit, Online-Zugriffe auf Datenbestände Dritter.

Wir freuen uns sehr, diese Kurse zu konzipieren und durchzuführen und auch auf die Zusammenarbeit in dieser Form mit den Führungspersonen der Verwaltung.

12 Sie ist der Staatskanzlei nur administrativ zugeordnet [§ 18 Abs. 3 DSG].

13 Der Regierungsrat hat das WBK bei den Personalverbänden in die Vernehmlassung gegeben [Frist: 31. März 2012].

## 6. Wichtiges zur Datensicherheit

### Rolle und Aufgaben des DSB bei der IT-Sicherheit?

Im Berichtsjahr überprüfte der Regierungsrat die Sicherheitsstrategie und das Sicherheitskonzept der kantonalen Behörden. Dabei geht es grundsätzlich um alle Aspekte der Sicherheit, die sich in der Verwaltung stellen: Betriebs-/Gebäudesicherheit, Arbeitssicherheit und Gesundheitsschutz, IT-Sicherheit, Notfall- und Ereignismanagement, Krisenmanagement etc.

Bei der IT-Security stellten sich Fragen bezüglich der Verantwortung und der Rolle des Datenschutzbeauftragten. Zwischen Regierungsrat, der kantonalen Informatik/AIO, der Fachstelle Sicherheit und dem Datenschutzbeauftragten konnte klargestellt werden, dass die Verantwortlichkeiten wie folgt geregelt sind:

- Für den Schutz der IT-Grundstruktur<sup>14</sup> ist die kantonale Informatik/AIO zuständig und verantwortlich. Der Datenschutzbeauftragte unterstützt diese mit seinem Dienstleistungsangebot.
- Für die übrigen Datensicherheitsaspekte am Arbeitsplatz sind die Organe zuständig und verantwortlich.<sup>15</sup> Der Datenschutzbeauftragte unterstützt die Organe mit seinem Dienstleistungsangebot.

Der DSB ist in den verschiedenen diesbezüglichen Gremien vertreten.<sup>16</sup>

### Ist ein Kopierer einfach ein Kopierer?

Nein, dem ist bereits seit einigen Jahren nicht mehr so. Ein moderner Geschäftskopierer mag zwar im Gewande des Druckers, Scanners und Fax daherkommen – wir lassen uns aber nicht täuschen und erahnen es: In erster Linie handelt es sich um einen Computer mit einer grossen Festplatte, der alles, was er zu sehen bekommt, abspeichert. Via Netzwerk ist er mit dem Internet und damit mit der ganzen Welt verbunden.

Der Ersatz eines Kopierers im Regierungsgebäude gab uns den Anlass, zusammen mit der verantwortlichen Person bei der kantonalen Informatik

und dem Lieferanten, die Datensicherheit eines Kopierers, wie er als Standard-Gerät in der Zuger Verwaltung bei rund 170 Stellen eingesetzt wird, etwas genauer unter die Lupe zu nehmen. Zum Datenhandling während der Nutzung des Geräts waren folgende Fragen zu klären:

- Wie lange wird der «Scan» [d.h. «die Aufnahme» der Kopie, des Drucks oder des Faxes] gespeichert?

Antwort: Die Festplatte hat eine Speichergrösse von 160 GB. Wenn dieser Speicher voll ist, werden alte Daten überschrieben. Voll ist der Speicher erst, wenn er Aufnahmen von etwa 300 000 A4-Seiten enthält. All diese Dokumente finden sich somit im Speicher. Bis Aufnahmen überschrieben werden, kann es daher sehr lange dauern.

- Wie lange werden die Randdaten [d.h. insbesondere: Wer hat wann welches Dokument gedruckt und wie weiterverarbeitet?] des Scans gespeichert?

Antwort: Alle Randdaten werden erfasst und gespeichert. Sie werden nicht gelöscht und stehen dem Servicetechniker für die Wartung des Kopierers zur Verfügung.

- Wer (User, Dritte im Netzwerk, Administrator AIO oder Servicefachperson des Herstellers) hat wie und wie lange Zugriff auf den Scan beziehungsweise auf die Randdaten des Scans [zudem: via Netzwerk oder nur am Gerät selber]?

Antwort: Mitarbeitende sehen an ihrem Computer den Scan des Dokuments nicht, nur die Randdaten auf der Job-Liste. Die Administratoren der kantonalen Informatik sehen die Job-Listen. Der Servicetechniker sieht die Job-Liste und kann grundsätzlich auch auf die Festplatte zugreifen.

- Wie sieht es mit der Datensicherheit beim Versenden von Dokumenten via E-Mail aus?

Antwort: Wird direkt ab Kopierer gemailt, handelt es sich um gewöhnliche, unverschlüsselte E-Mails. Der kantonsinterne Versand wird grundsätzlich als sicher beurteilt [zu beachten ist aber, dass dem Adressaten als Absender die E-Mail-Adresse des Kopiergeräts angezeigt wird,

14 Darunter fallen insbesondere die zentralen Server, die Netzwerke zu den Amtsstellen, die Arbeitsgeräte der Mitarbeitenden und die Standard-Anwendungen.

15 Schutz der Büros vor Zutritt bzw. der Geräte vor Zugriffen durch Unberechtigte etc.

16 «Arbeitsgruppe Sicherheit [gross]/AGS» sowie im «Kantonalen Führungsstab/KFS», der bei der Sicherheitsdirektion angegliederten Notorganisation.

sodass nicht klar ist, welche Person den Scan geschickt hat. Zudem kann auf eine solche E-Mail somit nicht geantwortet werden]. Der Versand von E-Mails an Externe via Internet ist dann unzulässig, wenn das Dokument Personendaten oder vertrauliche Informationen enthält. Das ist in der Praxis fast immer der Fall, sodass der Versand ab Kopiergerät via Internet unzulässig ist. Beim Versenden von E-Mails ab Kopiergerät können zudem leicht falsche Adressaten ausgewählt werden. Dokumente sind deshalb grundsätzlich nur an die eigene E-Mail-Adresse zu mailen. Ein sich selber gemailtes Dokument kann anschliessend weiterbearbeitet, allenfalls auch weiter versendet werden.

Wie sieht das Datenhandling bei Rückgabe des Geräts aus [bezüglich der Festplatte bzw. des V-RAM-Speichers]?

Antwort: Bei Rückgabe des Geräts wird die Festplatte durch einen Mitarbeiter der kantonalen Informatik ausgebaut und vollständig gelöscht. Der V-RAM-Speicher ist durch den Hersteller zu löschen.

Fazit: Man muss sich bewusst sein, dass moderne Kopiergeräte alles abspeichern. Nutzt man die Scanfunktion, ist der Scan immer an die eigene E-Mail-Adresse zu senden, nicht hingegen ab Kopiergerät an Dritte.

Ergänzend: Die Sicherheitseinstellungen werden Anfang 2012 zwischen der kantonalen Informatik und dem Datenschutzbeauftragten festgelegt.

### **Schulung der Mitarbeitenden bezüglich Datensicherheit**

Die Daten der Zuger Bevölkerung müssen in der Verwaltung in jeder Hinsicht sicher bearbeitet und aufbewahrt werden. Dafür sorgt in erster Linie die Technik. Bekanntlich ist aber auch der Mensch entscheidend: Jede einzelne Mitarbeiterin, jeder einzelne Mitarbeiter muss wissen, wie mit Daten umzugehen ist. Die Datensicherheitsverordnung sieht deshalb vor, dass sämtliche Mitarbeitenden bezüglich Datenschutz und Datensicherheit zu schulen sind.<sup>17</sup> Der Datenschutzbeauftragte stellt Merkblätter<sup>18</sup> für die Instruktion der Mitarbeitenden zur Verfügung.<sup>19</sup>

Im Jahr 2009 hat die Finanzdirektion durch eine externe Firma ein webbasiertes E-Learning-Modul zur Datensicherheit entwickeln lassen, dessen Inhalt den Merkblättern entspricht. Damit haben die Mitarbeitenden die Möglichkeit, sich individuell an ihrem Arbeitsplatz weiterzubilden. Es wird dabei mit einem Arbeitsaufwand von etwas mehr als einer Stunde gerechnet. Der Kurs wird mit einer Abschlussprüfung abgeschlossen. Wird diese bestanden, kann eine Kurs-Bestätigung ausgedruckt werden. Im Berichtsjahr haben über 310 Mitarbeitende aus der Verwaltung von Kanton und Gemeinden diesen Kurs absolviert – was sehr erfreulich ist.

17 § 5 Abs. 2 der Datensicherheitsverordnung vom 16. Januar 2007 [DSV, BGS 157.12].

18 Gemäss § 7 Datensicherheitsverordnung.

19 Sämtliche Unterlagen finden sich auf der DSB-Website in der Rubrik «Kanton Zug/Datensicherheit».

## II. Fälle aus unserer Beratungspraxis

### 1. Übersicht

Falls Sie im Folgenden wichtige Themen vermissen, konsultieren Sie bitte die früheren Tätigkeitsberichte. Sie finden dort über 390 weitere Fallbeispiele. Die Tätigkeitsberichte 1999 bis

2011 können Sie übrigens beim DSB kostenlos bestellen [041 728 31 47]. Sie finden sie zudem auch im Internet unter: «[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)», Rubrik «Kanton Zug/Tätigkeiten». Im Bereich «Suche» können Sie übrigens Abfragen machen, die sich ausschliesslich auf die Tätigkeitsberichte beziehen.

Stichwort	Fragestellung	Fall Nr.	Seite
Abstimmungsgeheimnis	Woher weiss das Schweizer Fernsehen, wer an der Abstimmung teilgenommen hat?	16	17
Auslagern	Welche Daten darf ein privater Beauftragter erheben?	13	15
Einwohnerkontrolle	Verweigerung einer Adressanfrage trotz fehlender Datensperre?	19	18
E-Mail	Was ist bei Ferienabwesenheit bezüglich E-Mails vorzusehen?	3	10
«Fichen»	Wie und wo ist das Personaldossier zu führen?	2	10
Kantonsrat	Welche Geschäfte dürfen nicht im Internet veröffentlicht werden?	14	16
Kindeswohl	Wie geht die Familienhilfe vor, wenn sie das Kindeswohl als gefährdet erachtet?	20	18
«Moskito»	«Moskito» - oder Videoüberwachung?	11	14
Ombudsstelle	Welche Daten/Unterlagen können der Ombudsstelle bekannt gegeben werden?	15	17
Outlook-Kalender	Wer hat beim Outlook-Kalender Einsicht worauf?	5	11
Outsourcen	Welche Daten darf ein privater Beauftragter erheben?	13	15
Personaldossier	Wie und wo ist das Personaldossier zu führen?	2	10
Schule	Darf eine Lehrperson den zukünftigen Lehrbetrieb einer Schülerin informieren?	8	13
Schulpsychologischer Dienst	Wie sieht es mit der Schweigepflicht aus? Wie mit der Einsicht in Berichte?	9	13
sexuelle Belästigung	Was ist aus datenschutzrechtlicher Sicht bei der Regelung des Themas sexuelle Belästigung am Arbeitsplatz zu beachten?	6	12
Sperrrecht	Kann die Einwohnerkontrolle eine Adressanfrage verweigern, auch wenn die Adresse nicht gesperrt ist?	19	18
Steuerbehörden	Dürfen ausserkantonalen Steuerbehörden Unterlagen zugestellt werden?	17	17
Strassenverkehrsamt	Verkauft das Strassenverkehrsamt Halterdaten an Autohändler?	18	17
Team	Darf das Team Einsicht in die Leistungserfassung der einzelnen Mitarbeitenden haben?	4	11
Verkehrserhebung	Was ist bei einer Verkehrserhebung mittels Bildaufzeichnung zu beachten?	12	15
Videoaufzeichnung	Was ist bei einer Verkehrserhebung mittels Bildaufzeichnung zu beachten?	12	15
Videoüberwachung	Wie sieht es mit der Auswertung von Aufzeichnungen der SBB aus?	10	14
Videoüberwachung	Videoüberwachung - oder «Moskito»?	11	14
Vormundschaftsbehörde	Wie geht die Familienhilfe vor, wenn sie das Kindeswohl als gefährdet erachtet?	20	18
Wahlgeheimnis	Woher weiss das Schweizer Fernsehen, wer an der Wahl teilgenommen hat?	16	17
Whistleblowing	Was ist aus datenschutzrechtlicher Sicht bei der Regelung des Whistleblowings zu beachten?	7	12
Zuständigkeit des DSB	Wann ist die Zuständigkeit des Zuger Datenschutzbeauftragten gegeben?	1	10

**Fall 1 Wo wir zuständig sind – wo nicht**

Mehrmals wöchentlich erhalten wir Anfragen, die Datenbearbeitungen von *Zuger Unternehmen* oder *Zuger Privatpersonen* betreffen.<sup>20</sup> Dafür sind wir nicht zuständig.

Unsere Zuständigkeit ist im Datenschutzgesetz klar festgelegt: Wir sind ausschliesslich zuständig für Datenbearbeitungen der kantonalen und gemeindlichen Verwaltungen und von Privaten, sofern diese für das Gemeinwesen öffentlich-rechtliche Aufgaben<sup>21</sup> erfüllen.

Für die Datenbearbeitungen von Privaten hingegen ist schweizweit der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte [EDÖB] in Bern zuständig.<sup>22</sup> Wir müssen die Anfragenden in diesen Fällen somit an ihn verweisen. Der EDÖB verfügt auch nur über begrenzte personelle Ressourcen und ist deshalb nicht in der Lage, jede einzelne Anfrage beantworten zu können. Allenfalls ist auch mit Wartezeiten zu rechnen. Ohne in die Zuständigkeit des EDÖB einzugreifen: Soweit wir fachlich und zeitlich in der Lage sind, geben wir den Zuger Anfragenden gerne erste – wenn auch naheliegenderweise «unverbindliche» – datenschutzrechtliche Hinweise.

20 So etwa bezüglich der Bearbeitung von Daten durch den Hausarzt, den Vermieter, den Arbeitgeber, Vereine oder Telekommunikationsanbieter. Auch nicht zuständig sind wir etwa für die Löschung von Veröffentlichungen durch Private, Unternehmen oder soziale Netzwerke im Internet.

21 S. «www.zug.ch» die Auflistung in der Rubrik «Organisationen mit Leistungsvereinbarung».

22 Eidg. Datenschutz- und Öffentlichkeitsbeauftragter, Feldeggweg 1, 3003 Bern, Tel. 031 322 43 95, «www.edoeb.admin.ch».

23 Anders ist die Rechtslage bei unpersönlichen E-Mail-Adressen wie etwa info@zg.ch oder servicedesk@zg.ch, wo nicht eine ganz bestimmte Person angesprochen wird.

## 2. Personalrecht

**Fall 2 Das Personaldossier – und im Geheimen die «Fichen»?**

Aufgrund entsprechender Anfragen ist klarzustellen: Das Personaldossier muss sämtliche Unterlagen und Dokumente enthalten, welche die Mitarbeiterin, den Mitarbeiter betreffen. Es ist nicht zulässig, «Schattendossiers» zu führen, somit Akten, die vor dem Mitarbeitenden verheimlicht werden. Die Mitarbeitenden haben das Recht, grundsätzlich jederzeit ihr vollständiges Personaldossier einzusehen.

Von «Schattendossiers» ist die Frage zu unterscheiden, ob Dossiers an zwei verschiedenen Stellen geführt werden dürfen. Das ist zulässig, kommt in der Praxis häufig vor und ist kein Problem, weil dies den Mitarbeitenden bekannt ist oder sie bei Anfrage auf Einsicht über Unterlagen bei anderen Stellen zu informieren sind. So verfügt einerseits die Personalabteilung über gewisse Daten und Unterlagen von Mitarbeitenden, andererseits aber auch der direkte Vorgesetzte. Dies ist nicht zu beanstanden.

Fazit: Neben dem Personaldossier darf es keine «Schattendossiers» oder «Fichen», somit versteckt geführte Unterlagen über Mitarbeitende geben.

**Fall 3 Ein Dauerbrenner: Wie ist mit eingehenden E-Mails bei Ferienabwesenheit umzugehen?**

Der korrekte Umgang mit eingehenden E-Mails an persönliche Adressen<sup>23</sup> ist sehr wichtig, nicht nur für den Adressaten, sondern auch für den Absender. Dieser geht nämlich in aller Regel davon aus, dass seine Nachricht nur vom Adressaten selber gelesen wird.

Bei vorhersehbarer Abwesenheit ist das korrekte Vorgehen, dass eine Abwesenheitsmeldung erfasst wird, die angibt, bis wann der Adressat abwesend ist und an wen sich der Absender in der Zwischenzeit wenden kann. Zudem ist ausdrücklich darauf hinzuweisen, dass die eingehende Mitteilung nicht weitergeleitet wurde. Dass eine korrekte Identifikation nicht fehlen darf,

ist in der kantonalen Verwaltung ausdrücklich vorgeschrieben,<sup>24</sup> sollte aber eigentlich ohnehin selbstverständlich sein.

Eingehende E-Mails dürfen somit nicht automatisch weitergeleitet werden, weder an ein eigenes verwaltungsexternes Konto noch an die Stellvertretung oder an Sekretariate.

Ergänzend: Bei unerwarteter länger dauernder Abwesenheit aufgrund unvorhersehbarer Ereignisse wie Unfall oder Krankheit hat der Mitarbeitende, sofern er in der Lage ist, eine entsprechende Abwesenheitsmeldung einzurichten. Ist er dazu nicht in der Lage, kann der Vorgesetzte bei der kantonalen Informatik/AIO veranlassen, dass auf dem E-Mail-Konto eine entsprechende Abwesenheitsmeldung eingerichtet wird. Dabei wird kein Einblick in das E-Mail-Konto genommen.

Unzulässig ist es, dass Mitarbeitende im Voraus oder im Ereignisfall ihr Passwort bekannt geben – weder auf Druck des Vorgesetzten noch freiwillig.<sup>25</sup>

#### Fall 4 Gegenseitige Einsicht von Mitarbeitenden in Arbeitsleistungserfassungen?

Eine Amtsstelle hat für ihre Mitarbeitenden eine Leistungserfassung entwickelt, die für alle Mitarbeitenden gegenseitig einsehbar ist. Neben verschiedenen Auswertungen zu Leistungserfüllung und Angaben zu Leistungsbeurteilungen sind von jedem Mitarbeitenden auch Hinweise über die Teilnahme an Sitzungen und über Abwesenheiten wegen Weiterbildung, Ferien und Krankheit aufgeführt.

Wir wurden von der Leitung angefragt, ob die gegenseitige Einsichtnahme zulässig sei.

Bei den Angaben über die einzelnen Mitarbeitenden handelt es sich um detaillierte Leistungsbeurteilungen. Aus den erfassten Angaben lassen sich direkt Rückschlüsse auf Qualität, Quantität, Effizienz und Motivation jedes einzelnen Mitarbeitenden ziehen. Solche Beurteilungen bilden die Grundlage für die Mitarbeiterbeurteilung.<sup>26</sup> Mitarbeitergespräche bilden ihrerseits die Grundlage für die berufliche Standortbestimmung, für

die Beurteilung der Fort- und Weiterbildungsbedürfnisse, für die Laufbahnplanung sowie für die fähigkeitsbezogene Funktionszuweisung und leistungsgerechte Entlohnung und Beförderung.

Bei sämtlichen hier geführten Angaben handelt es sich um besonders schützenswerte Personendaten beziehungsweise um Persönlichkeitsprofile, die vom Vorgesetzten im Personaldossier jedes einzelnen Mitarbeiters zu führen sind. Das Personaldossier ist vertraulich. Daten daraus dürfen für Dritte nicht zugänglich sein. Dies ist auch dem Merkblatt «Personaldossier und Aktenablage» des Personalamtes zu entnehmen.

Fazit: Es ist unseres Erachtens nicht zulässig, dass alle Mitarbeitenden gegenseitig Einsicht in ihre Leistungserfassungen haben. Die entsprechende Stelle hat unsere Hinweise umgesetzt.

Ergänzung: Der Vorgesetzte darf solche Leistungsangaben als persönliches Führungsinstrument nutzen, sofern er diese Daten Dritten nicht bekannt gibt. Falls verschiedene Teams die gleichen Arbeiten ausführen, ist die Zusammenfassung der einzelnen Mitarbeiterdaten zu anonymisierten Teamdaten zulässig, sofern dabei keine Rückschlüsse auf einzelne Personen gemacht werden können.

#### Fall 5 Freigeschalteter Outlook-Kalender – alle sehen meinen Arzttermin!

Der Outlook-Kalender kann für die Planung von Besprechungen ein sehr nützliches Instrument sein. Viele Verwaltungsstellen nutzen denn auch diese Funktion. Dabei sind aus datenschutzrechtlicher Sicht folgende Punkte zu beachten:

- Das Amtsgeheimnis gilt. Alle Einträge sind so zu formulieren, dass andere Stellen keine Informationen erhalten, die dem Amtsgeheimnis unterliegen. Gleiches gilt für Dokumente, die dem Termin beigelegt sind. Dies ist insbesondere dann ein Thema, wenn der Kalender der Mitarbeitenden für die ganze Verwaltung zugänglich ist.
- Wer eine Abwesenheit aus privaten Gründen erfasst (Arzttermin, Todesfall etc.), muss dies so vornehmen, dass nicht die ganze Verwaltung weiss, was der Grund der Abwesenheit ist.

24 § 6 [Identifikation von E-Mails] der Verordnung über die Benutzung von elektronischen Geräten und elektronischen Kommunikationsmitteln im Arbeitsverhältnis [BGS 154.28] lautet: «Gegenüber der Empfängerin oder dem Empfänger von E-Mails sind Name, betriebliche Funktion sowie die betriebliche Adresse inklusive Telefonnummer und E-Mail-Adresse der Absenderin oder des Absenders anzugeben.»

25 § 2 Abs. 1 der vorstehenden Verordnung lautet: «Das Passwort ist persönlich und darf nicht weitergegeben werden.»

26 § 65 Personalgesetz [BGS 154.21].

- Kreis der Zugriffsberechtigten: Die Freischaltung des Kalenders muss sorgfältig eingerichtet werden, damit nur die Berechtigten den Zugriff erhalten. Andernfalls kann es passieren, dass nicht nur das eigene Team, sondern versehentlich verwaltungsweit sämtliche Mitarbeitende Einsicht nehmen können.
- Der Kreis der Einsichtsberechtigten sollte verhältnismässig sein. Nur Stellen, mit denen häufig zusammengearbeitet wird, sollen Einsicht nehmen dürfen.

#### **Fall 6 Broschüre «Sexuelle Belästigung am Arbeitsplatz» – was ist aus Sicht des Datenschutzes zu beachten?**

Ein sehr heikles Thema, bei dem sich viele datenschutzrechtliche Fragen stellen. Eignet sich ein entsprechender Vorfall und entschliesst sich die betroffene Person, den Arbeitgeber zu informieren, so kommt es in der Folge zur Bekanntgabe von sehr sensiblen Personendaten, sowohl hinsichtlich der betroffenen wie auch der beschuldigten Person. Diese Daten werden allenfalls bei verschiedenen Stellen bearbeitet, etwa beim Vorgesetzten, beim übergeordneten Vorgesetzten oder beim Personalamt.

Näher zu regeln ist hier somit insbesondere, wer in welchem Abklärungsstadium in welchem Umfang zur Erhebung von welchen Personendaten zuständig ist, wo, wie und wie lange diese aufbewahrt werden und unter welchen Umständen sie wem bekannt gegeben werden.

Zudem ist zu beachten, dass sowohl die betroffene wie auch die beschuldigte Person ein grundsätzlich umfassendes Recht auf Einsicht in ihre eigenen Daten hat.<sup>27</sup> Einschränkungen sind zwar ausnahmsweise möglich, dabei stellen sich jedoch schwierige Fragen der Interessenabwägung: Schutz der Privatsphäre der angeschuldigten Person gegenüber dem Recht des Angeschuldigten auf Information über die ihm vorgeworfene Handlung. Jeder Beschuldigte muss das Recht haben, sich in umfassender Kenntnis der Vorwürfe verteidigen zu können. Zu bedenken gilt es, dass eine Anschuldigung allenfalls auch zu Unrecht erfolgt sein könnte.

#### **Fall 7 «Whistleblowing» – und der Datenschutz?**

Wir wurden angefragt, was aus datenschutzrechtlicher Sicht bei einer allfälligen Regelung von «Whistleblowing» in der Verwaltung zu beachten ist. Beim Melden von beobachteten «Missständen» durch Mitarbeitende geht es – ähnlich wie im vorstehenden Fall – insbesondere um die folgenden Themen:

- Wann liegt ein melderrelevanter «Missstand» vor?
- Welche Anforderungen sind an die Qualität der Meldungen zu stellen, d.h. welche konkreten Angaben muss eine Meldung beinhalten?
- Wo ist eine allfällige Meldestelle angesiedelt?
- Ist zuerst der interne Dienstweg zu beschreiten oder kann man sich direkt an die Meldestelle wenden?
- Wird einem Whistleblower Anonymität gewährt oder wird Offenlegung der Identität des Whistleblowers verlangt? Zu welchem Zeitpunkt wird offen gelegt?
- Wie wird ein Whistleblower vor Vergeltungsmassnahmen geschützt?
- Welcher Schutz besteht für eine beschuldigte Person, welche Rechte hat sie? Wann und wie wird sie informiert? Wie sind die Auskunfts- und Einsichtsrechte geregelt? Wann und wie kann die beschuldigte Person Stellung nehmen zu den Vorwürfen?
- Was sind die Konsequenzen für den Whistleblower, wenn die Meldung missbräuchlich erfolgt oder die belastete Person unschuldig ist?

Fazit: Es ist sicherzustellen, dass die Informationen über die Whistleblower und die beschuldigten Personen in einem Meldeverfahren nach den Grundsätzen des Datenschutzgesetzes bearbeitet werden.

Insbesondere sind daher ausdrücklich zu regeln: Verhältnismässigkeit, Zweckgebundenheit, Bearbeitung nach Treu und Glauben, Aufbewahrungsfristen, Vernichtung von Daten, Auskunfts-, Einsichts-, Berichtigungs- und Löschrechte sowie die Datensicherheit.

### 3. Schule

#### Fall 8 Darf ein Lehrer den zukünftigen Lehrbetrieb einer Schülerin informieren?

Die Eltern einer Schülerin der 3. Oberstufe erkundigten sich bei uns, ob der Klassenlehrer dem zukünftigen Lehrmeister unaufgefordert Negatives über ihre Tochter erzählen dürfe. Weder Eltern noch Tochter waren naheliegenderweise mit diesem Vorgehen einverstanden. Es lohnt sich, hier eine kleine Auslegeordnung bezüglich des Informationsflusses im Zusammenhang mit der Leistungsbeurteilung vorzunehmen.

Ausgangspunkt: Aufgrund des Schulgesetzes haben Lehrpersonen Schülerinnen und Schüler zu beurteilen.<sup>28</sup> Diese Daten werden ausschliesslich für schulische Zwecke erhoben.

Als Betroffene haben die Schüler selber grundsätzlich einen umfassenden Anspruch, in alle sie betreffenden Daten Einsicht nehmen zu können. Gleiches gilt für die Eltern von minderjährigen Schülern.<sup>29</sup> Dritte hingegen, beispielsweise zukünftige Lehrmeister, erhalten ohne ausdrückliche Einwilligung von Eltern oder Schülerin keinerlei Auskünfte. Diejenigen Informationen, die für die weiteren Karriereschritte wichtig sind, und die für Dritte zugänglich sein sollen, stehen im Zeugnis.

Hält eine Lehrperson eine Datenbekanntgabe an eine zukünftige Lehrperson in einer besonderen Situation für wichtig, so ist das Gespräch mit den Betroffenen [SchülerIn/Eltern], nötigenfalls unter Einbezug der Schulleitung zu suchen.

Es ist abschliessend darauf hinzuweisen, dass eine Datenbekanntgabe gegen den Willen der Betroffenen für die Lehrperson grundsätzlich<sup>30</sup> disziplinarische, zivilrechtliche oder auch strafrechtliche Sanktionen nach sich ziehen kann.

Fazit: Ohne ausdrückliche Zustimmung der Eltern beziehungsweise der betroffenen Schülerin<sup>31</sup> darf der Lehrer nicht Informationen über diese an den zukünftigen Lehrbetrieb weitergeben.

#### Fall 9 Schweigepflicht beim Schulpsychologischen Dienst abgeschafft?

«Die Mitarbeiter des Schulpsychologischen Dienstes sind zur Geheimhaltung verpflichtet. Eltern, Kindergärtnerin und Lehrer ist die Einsichtnahme in schriftliche Berichte zu ermöglichen, soweit dem nicht übergeordnete öffentliche oder private Interessen entgegenstehen.» So wurde die Schweigepflicht des Schulpsychologischen Dienstes bis am 11. Juli 2011 geregelt.<sup>32</sup> Entgegen unserer Stellungnahme hat der Regierungsrat diese Bestimmung auf den 12. Juli 2011 ersatzlos gestrichen. Der Grund zu diesem Schritt liegt nun aber nicht darin, dass die Mitarbeitenden des SPD nicht mehr zur Geheimhaltung verpflichtet wären. Vielmehr gelten nun die übergeordneten Vorschriften: betreffend Geheimhaltung das Personalrecht, betreffend Datenhandling und Einsicht das Datenschutzgesetz. Konkret bedeutet dies:

#### Amtsgeheimnis<sup>33</sup>

Grundsätzlich unterstehen alle Datenbearbeitungen des SPD dem Amtsgeheimnis. Was immer wieder übersehen wird: Das Amtsgeheimnis gilt auch gegenüber anderen Amtsstellen.

#### Datenbekanntgabe

Bei den Daten des SPD handelt es sich in aller Regel um besonders schützenswerte Personendaten<sup>34</sup>. Diese dürfen nur bekannt gegeben werden, wenn dies in einem Gesetz ausdrücklich vorgesehen ist, für eine in einem formellen Gesetz umschriebene Aufgabe offensichtlich unentbehrlich ist oder die betroffene Person ausdrücklich zustimmt. In aller Regel benötigt die Weitergabe von Daten des SPD somit die Zustimmung der Eltern.

#### Einsicht

Gestützt auf das Datenschutzgesetz haben die Betroffenen<sup>35</sup> das Recht, grundsätzlich sämtliche sie betreffenden Daten einzusehen und/oder kostenlose Kopien<sup>36</sup> zu verlangen. Dies bezieht sich auf Berichte, Protokolle oder Gesprächsnotizen, unabhängig von der Form der Aufzeichnungen.

Fazit: Ohne Zustimmung der gesetzlichen Vertreter erhalten Lehrpersonen grundsätzlich keine Einsicht in Unterlagen des SPD.

28 § 17 Abs. 1 des Schulgesetzes [BGS 412.11].

29 § 20 Abs. 2 Bst. d des Schulgesetzes.

30 Es kann finanzieller Schaden bzw. eine Persönlichkeitsverletzung entstehen.

31 Es ist davon auszugehen, dass eine Oberstufenschülerin diesbezüglich handlungsfähig ist und ihre Rechte daher grundsätzlich selber wahrnehmen kann.

32 § 18 Abs. 3 der Verordnung zum Schulgesetz [BGS 412.111].

33 Geregelt in § 29 des Personalgesetzes [BGS 154.21] und § 11 der Personalverordnung [BGS 154.211].

34 § 2 Bst. b Datenschutzgesetz.

35 Somit die Erziehungsberechtigten, je nach Alter allenfalls der betroffene Schüler selber [§ 13/§ 14 Datenschutzgesetz].

36 § 17 Abs. 2 Datenschutzgesetz.

## 4. Sicherheit

### Fall 10 SBB überwachen den Bahnhof Zug mit Video – Auswertung durch die Zuger Polizei?

Die SBB sind aufgrund von Bundesvorschriften grundsätzlich berechtigt, ihre Fahrzeuge, Bauten, Anlagen und Einrichtungen mit Videokameras zu überwachen.<sup>37</sup> Offenbar erfolgte die Sichtung und Auswertung von Bildaufzeichnungen teilweise verzögert. Die Sicherheitsdirektion erkundigte sich beim DSB, ob nicht die Zuger Polizei beauftragt werden könnte, die im Bahnhof Zug erfassten Bildaufzeichnungen auszuwerten.

Vorweg: Diese Frage haben die SBB zu beurteilen, da es um deren Daten geht. Unseres Erachtens präsentiert sich die Rechtslage wie folgt:

Gemäss ausdrücklicher Bundesvorschrift müssen Aufzeichnungen mit Personendaten spätestens am nächsten Werktag ausgewertet werden. Ist dies aus betrieblichen oder technischen Gründen nicht möglich, so müssen sie innert zwei weiteren Werktagen ausgewertet werden.<sup>38</sup>

Aufgrund der Verordnung ist klar, dass nur die SBB, die den Einsatz von Videogeräten beschlossen haben und diese betreiben, Auswertungen vornehmen dürfen. Gestützt auf die Auswertung entscheiden die SBB, ob und allenfalls welche Aufnahmen sie den Behörden bekannt geben dürfen. Ausdrücklich unzulässig wäre somit die Übergabe aller unausgewerteten Aufzeichnungen an die Zuger Polizei.

Die Verordnung enthält keinerlei Ermächtigungen an die SBB, die Auswertung von Videoaufzeichnungen auszulagern und durch Dritte vornehmen zu lassen. Im Gegenteil, die SBB sind vielmehr verpflichtet, dafür zu sorgen, dass im Zusammenhang mit Aufzeichnungen erfasste Personendaten vor unbefugtem Zugriff geschützt sind.<sup>39</sup>

Fazit: Eine Auswertung durch die Zuger Polizei käme einer Bekanntgabe sämtlicher Aufzeichnungen gleich. Dies würde klar gegen die Regelung der Bekanntgabe und gegen die Pflicht des Unternehmers, die Aufzeichnungen vor unbefugten

Zugriffen zu schützen, verstossen. Die Auswertung der im Bahnhof Zug gemachten Videoaufzeichnungen durch die Zuger Polizei ist aufgrund der Bundesvorschriften somit unzulässig.

Ergänzend: Die SBB haben die gesetzlich vorgegebenen Fristen einzuhalten. Diese sind klar, abschliessend und nicht verhandelbar. Darauf können sich die Zuger Behörden berufen. Sollten die SBB wiederholt dagegen verstossen, kann der Kanton aufsichtsrechtlich gegen die SBB vorgehen.

### Fall 11 «Moskito» – oder lieber Videoüberwachung?

Beim Gewerblich-Industriellen Bildungszentrum Zug/GIBZ wurde im Jahr 2007 eine Anlage «Sound-Systeme» angebracht, um zwischen 23 und 05 Uhr Jugendliche aus einem bestimmten Bereich des Schulhausplatzes zu vertreiben. Auslöser waren offenbar Schäden durch Jugendvandalismus. Die Anlage sendet einen Sinuston mit einer relativ hohen Frequenz, den Jugendliche in aller Regel als störend empfinden und sie deshalb vertreibt. Erwachsene hingegen können diesen Ton kaum oder gar nicht hören. Solche Anlagen werden auch als «Moskitos» bezeichnet. Die Anlage führte zu einer Interpellation im Kantonsrat.<sup>40</sup> Die Antwort des Regierungsrates<sup>41</sup> wurde im Berichtsjahr im Kantonsrat ausführlich diskutiert.<sup>42</sup>

«Moskitos» haben direkt nichts mit Datenschutz zu tun. Trotzdem wurde der DSB bei der Ausarbeitung der regierungsrätlichen Antwort einbezogen. Hintergrund: Es stellte sich die Frage nach Alternativen – etwa die Installation von Videoüberwachungsgeräten. Ohne hier darauf einzugehen, ob der Einsatz einer solchen Anlage beim GIBZ notwendig oder sinnvoll sei, ist den Ausführungen des Regierungsrates in seiner Antwort zuzustimmen: Wenn nur zwischen dem Einsatz eines «Moskitos» und einer Videoüberwachung zu wählen ist – ist es eine Wahl zwischen Skylla und Charybdis? Wohl fast. Trotzdem würden wir dem «Moskito» den Vorzug zu geben, da er – im Gegensatz zur Videoüberwachung – einen viel geringeren Eingriff in Grundrechte und Persönlichkeitsrechte bewirkt<sup>43</sup> und der verhältnismässige Einsatz aus technischen Gründen viel eher möglich ist.<sup>44</sup>

37 Art. 1 der Verordnung über die Videoüberwachung im öffentlichen Verkehr [Videoüberwachungsverordnung ÖV, VüV-ÖV, SR 742.147.2].

38 Art. 4 Abs. 1 VüV-ÖV.

39 Art. 6 VüV-ÖV.

40 Interpellation von Markus Jans betreffend die Installation von Sound-Systemen zur Vertreibung von Jugendlichen beim Gewerblich-Industriellen Bildungszentrum Zug vom 11. November 2008 [Vorlage Nr. 1751.1 - 12918].

41 Vom 25. Januar 2011 [Vorlage Nr. 1751.2 - 13654].

42 Protokoll des Kantonsrates, 8. Sitzung vom 5. Mai 2011 [Nachmittagssitzung] S. 221-226.

43 Beim Einsatz von «Moskitos» erfolgen im Gegensatz zur Videoüberwachung keinerlei Datenaufzeichnungen.

44 Durch entsprechende Regelung der Frequenz, der Lautstärke und des Beschallungsbereiches [neben der zeitlichen Dauer als wichtigstem Kriterium].

## 5. Kanton

### Fall 12 Was machen all diese Videokameras in der Stadt Zug – Polizei-Überwachung total?

Im Dezember erkundigten sich verschiedene Personen bei uns, wozu an und über vielen Strassen in der Stadt Zug Videokameras installiert waren. Sie wollten auch wissen, wer was aufzeichnet und was damit genau gemacht wird.

An insgesamt 17 Standorten in der Stadt Zug waren im Auftrag der Baudirektion durch eine deutsche Firma Videokameras installiert worden, weil für die Planung des Zuger Stadttunnels an zwei Tagen eine Verkehrserhebung durchgeführt wurde. Die Baudirektion hat die Zuger Medien entsprechend informiert, diese berichteten darüber. Zudem waren bei allen Kamerastandorten Schilder vorhanden, die auf die Verkehrszählung hinwiesen.

Welche Daten wurden hier nun aber genau erfasst und wo sind meine Daten, wenn ich als Automobilist erfasst wurde?

Untersucht wurden die *Verkehrsflüsse* an zwei Tagen. Somit mussten an den verschiedenen Kamerastandorten die Autokennzeichen erfasst und miteinander verglichen werden, damit ersichtlich ist, welche Routen die einzelnen Automobilisten nehmen, wenn sie etwa von Walchwil herkommend in die Stadt Zug einfahren.

An jedem Kamerastandort befand sich ein Computer mit entsprechender Software, der in einem parkierten Auto geschützt war und der mit einem Kabel mit der Kamera verbunden war. Dieser erfasste und analysierte automatisch die Signale der Videokamera und legte von jedem durchfahrenden Fahrzeug ein Foto des Nummernschildes ab. Videoaufzeichnungen, somit bewegte Bilder, wurden keine gemacht. Nach diesen zwei Tagen der Erfassung nahmen die deutschen Spezialisten die Computer mit den Aufnahmen an den Hauptsitz nach Deutschland mit. Dort wurden die Rohdaten, somit die Aufnahmen mit den erkennbaren Nummernschildern, ausgewertet. Nach der Auswertung werden die Rohdaten anonymisiert,

sodass das Nummernschild nun nicht mehr vorhanden ist, sondern durch eine beliebige Nummer ersetzt wird. Dadurch ist gewährleistet, dass zu einem späteren Zeitpunkt noch ergänzende Auswertungen vorgenommen werden können. Beispielsweise erhält das Schild «LU 546 918» bei der Anonymisierung die beliebige Bearbeitungsnummer «72 397». Anhand dieser Nummer kann nach wie vor die gefahrene Route ermittelt werden, es ist aber nicht mehr bekannt, um welchen Fahrzeughalter es sich dabei gehandelt hat. Nach diesem Anonymisierungsvorgang werden die Rohdaten vernichtet. Die anonymisierten Daten erhält zu Analyse Zwecken ein Planungsunternehmen in Zürich. Der Baudirektion werden keine Rohdaten übergeben, sondern nur fahrzeugunabhängige Statistiken, Mengenangaben oder Fahrzeiten.

Die Baudirektion regelte die Datenbearbeitungen des deutschen Unternehmens und des Zürcher Planungsbüros im Rahmen von detaillierten vertraglichen Vereinbarungen. Diese wurden dem DSB zur Stellungnahme vorgelegt. Die Baudirektion hat alle unsere Hinweise in dieser Sache übernommen.

Fazit: Bei einer Verkehrserhebung werden teilweise sehr sensible Daten über Private erhoben. Der Auftraggeber muss die Datenbearbeitung durch Externe bezüglich Datenschutz und Datensicherheit detailliert regeln. Zu einem möglichst frühen Zeitpunkt ist nur noch mit anonymisierten Daten zu arbeiten und die Rohdaten sind definitiv zu löschen.

### Fall 13 Outsourcen: Welche Daten gehen an einen privaten Beauftragten?

Eine Gemeinde erkundigte sich bei uns, ob sie berechtigt sei, einer privaten Firma Einsicht in Bauakten von historisch bedeutenden Gebäuden zu gewähren. Die Firma hatte vom Amt für Denkmalpflege den Auftrag erhalten, beim gemeindlichen Bauamt Grundlagen für die Inventarisierung zu beschaffen.

Die Firma wollte nun beim Bauamt zu über hundert Gebäuden Pläne, Fotos, Gesuchsunterlagen, Beschlüsse und Korrespondenz fotokopieren.

Wir wurden angefragt, ob diese private Firma berechtigt sei, alle diese Unterlagen zu kopieren und an ihren ausserkantonalen Geschäftssitz mitzunehmen.

Aufgaben, die der Staat aufgrund einer gesetzlichen Grundlage zu erfüllen hat, kann er in aller Regel auch an Private auslagern. Je nach Bedeutung und Umfang der fraglichen Aufgabe ist für die Auslagerung wegen des Legalitätsprinzips eine ausdrückliche gesetzliche Regelung erforderlich. Handelt es sich um blosser Hilfstätigkeit, kann auch ohne gesetzliche Grundlage ausgelagert werden.

Das Gesagte gilt auch im Zusammenhang mit der Bearbeitung von Daten. Voraussetzung ist, dass die Auftraggeberin dafür sorgt, dass die Daten nur so bearbeitet werden, wie sie es selbst tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.<sup>45</sup> Die Einhaltung von Datenschutz und Datensicherheit wird durch Auflagen oder Vereinbarungen sichergestellt. Die auslagernde Stelle bleibt dabei umfassend in der Verantwortung.

Es besteht eine Rechtsgrundlage, dass das Amt für Denkmalpflege selber berechtigt ist, die für die Aufgabe erforderlichen Daten zu beschaffen.<sup>46</sup> Da es sich im vorliegenden Fall um eine Hilfstätigkeit handelt, kann die Aufgabe auch an eine private Firma übertragen werden. Die Datenbearbeitung muss dabei verhältnismässig sein. Es dürfen somit nur diejenigen Unterlagen erfasst werden, die für die Aufgabenerfüllung notwendig sind. Datenschutz und Datensicherheit sind vertraglich zu regeln. So muss etwa gewährleistet werden, dass keine Daten an Dritte weitergegeben werden, dass die Daten für keine anderen Zwecke bearbeitet werden und dass sämtliche Datenbearbeitungen den aktuellen Stand der Datensicherheitsvorgaben erfüllen. Ist der Auftrag abgeschlossen, sind dem Auftraggeber alle erhobenen Unterlagen zu übergeben.

#### Fall 14 Das Protokoll des Kantonsrats im Internet verletzt Persönlichkeitsrechte

Eine betroffene Privatperson verlangte aus Gründen des Persönlichkeitsschutzes, dass Daten

über sie in der Internet-Version des Kantonsratsprotokolls zu löschen seien. Weil sich diese Frage bereits früher verschiedentlich stellte, galt es, eine grundsätzliche Regelung zu finden.

Bekanntlich vergisst das Internet nichts. Grundsätzlich werden alle publizierten Dokumente durch Suchmaschinen kopiert und archiviert. Im Moment der Publikation hat man in aller Regel die Herrschaft über seine Daten bereits verloren. Löschen nützt wenig, meist nichts, weil die Daten durch Google und Co. bereits kopiert und weltweit verteilt archiviert sind. Heikle Daten dürfen deshalb nicht im Internet publiziert werden.

Das Kantonsratsprotokoll wird von der Staatskanzlei betreut und veröffentlicht. Es gibt keine gesetzliche Grundlage, die der Staatskanzlei auf dem vorliegenden Gebiet erlauben würde, besonders schützenswerte Personendaten im Internet zu veröffentlichen.

Die Staatskanzlei wird in Zukunft Geschäfte des Kantonsrates, die Personendaten aus den folgenden Bereichen enthalten, nicht im Internet veröffentlichen:

- Unterlagen zu Wahlen, die der Kantonsrat vornimmt
- personalrechtliche Geschäfte
- Aufsichtsbeschwerden
- persönlichkeitschutzrelevante Petitionen
- Begnadigungen
- weitere Geschäfte, die besonders schützenswerte beziehungsweise heikle Personendaten zum Gegenstand haben.<sup>47</sup>

Die Nichtveröffentlichung im Internet ist umfassend zu verstehen. Sie bezieht sich somit nicht nur auf das Protokoll des Rates, sondern auch auf sämtliche Unterlagen und Berichte, die einen Zusammenhang mit diesen Geschäften haben. Somit insbesondere: Kantonsratsvorlagen, parlamentarische Vorstösse, Traktandenliste, Berichte und Anträge von Regierung und Kommissionen etc.

Ergänzend: Die Papierversion des Kantonsratsprotokolls muss umfassend und vollständig sein.

45 § 6 des Datenschutzgesetzes.

46 § 14 des Denkmalpflegegesetzes [BGS 423.11].

47 Beispielsweise Vorstösse im Zusammenhang mit Straffällen oder konkreten Ereignissen [etc.], die bestimmte oder bestimmbare Personen betreffen.

### Fall 15 Welche Daten dürfen der Ombudsstelle zugestellt werden?

Eine Privatperson hat sich bei der Ombudsfrau über die Behandlung durch eine Verwaltungsstelle beschwert. Sie verlangt nun von der betroffenen Verwaltungsstelle, dass diese ihr vollständiges Dossier der Ombudsfrau zustellt.

Die Leitung erkundigt sich beim Datenschutzbeauftragten, ob sie berechtigt sei, der Ombudsfrau das Dossier zuzustellen.

«Zur Abklärung des Sachverhalts kann die Ombudsstelle von der betroffenen Behörde und der Verwaltung jederzeit und auf jeder Hierarchiestufe schriftliche oder mündliche Auskünfte einholen, fallbezogen uneingeschränkt Einsicht in die Akten nehmen und deren Herausgabe verlangen» – so lautet die hier wichtige Bestimmung des Ombudsgesetzes.<sup>48</sup>

Fazit: Nachdem die betroffene Person die Ombudsfrau um Beratung ersucht hat und mit der Aktenzustellung an die Ombudsfrau ausdrücklich einverstanden war, ist dieser das vollständige Dossier zuzustellen.

### Fall 16 Ist das Wahlgeheimnis abgeschafft?

Das Schweizer Fernsehen präsentierte detaillierte Angaben über das Abstimmungsverhalten von Frauen und Männern bei der Abstimmung zum Waffengesetz. Eine Privatperson wollte wissen, wie es denn um das Wahlgeheimnis stehe, wenn dem Fernsehen solche Informationen zur Verfügung stünden.

Es gibt Kantone und Städte, welche die Stimmrechtsausweise mit einem «nicht sprechenden» Code bedrucken. Nach durchgeführter Wahl werden die Stimmrechtsausweise maschinell ausgewertet. Es können anschliessend gewisse Aussagen über die Beteiligten der Wahl gemacht werden. Es ist aber nicht möglich, Aussagen zu machen, wie abgestimmt wurde, werden doch die Stimmrechtsausweise von den Umschlägen mit den Wahlzetteln sowohl bei der brieflichen Stimmabgabe als auch im Wahllokal *getrennt*.

Damit ist die Anonymität bei den Abstimmungen/Wahlen vollumfänglich gewährleistet.

Im Kanton Zug enthalten die Stimmrechtsausweise übrigens keine solchen Codes. Es werden somit bei Abstimmungen oder Wahlen durch den Kanton oder die Gemeinden keinerlei solche statistischen Auswertungen vorgenommen.

Das Schweizer Fernsehen beauftragt übrigens Meinungsforschungsinstitute, die nach Abstimmungen und Wahlen jeweils durch telefonische Befragungen von Stimmbürgerinnen und Stimmbürgern deren Abstimmungsverhalten erfragen.

Fazit: Das Wahl- und Abstimmungsgeheimnis ist in Zug in jedem Fall vollumfänglich gewährleistet. Niemand erfährt, wer wie abgestimmt oder gewählt hat.

### Fall 17 Wenn ausserkantonale Steuerbehörden Auskunft verlangen?

Das Testament und sämtliche Unterlagen zu einem Nachlassinventar einer verstorbenen Person – das verlangt die Steuerverwaltung eines andern Kantons von der gemeindlichen Erbschaftsbehörde. Diese erkundigt sich beim Datenschutzbeauftragten, ob sie berechtigt ist, alle diese heiklen Dokumente herauszugeben.

Sowohl Bundesrecht<sup>49</sup> wie auch das Zuger Steuerrecht<sup>50</sup> sehen vor, dass Verwaltungsstellen den Steuerbehörden im Rahmen der Amtshilfe Auskünfte erteilen müssen. Die anfragende Steuerbehörde hat dazu in einem schriftlichen Gesuch kurz darzulegen, welche Unterlagen sie wozu benötigt. Ist die Anfrage plausibel und verhältnismässig, hat die angefragte Verwaltungsstelle Amtshilfe zu leisten, somit die verlangten Dokumente in Kopie herauszugeben. Dabei ist das Verhältnismässigkeitsprinzip zu beachten.

### Fall 18 Verkauft das Strassenverkehrsamt Daten an Autohändler?

Mehrere Privatpersonen beschwerten sich beim DSB darüber, dass sie von einem Autohändler persönlich angeschriebene Werbung erhalten haben, bei der im Schreiben ausdrücklich darauf Bezug genommen wurde, dass ihr Fahrzeug bereits seit acht Jahren im Verkehr sei – was zu-

48 § 8 Bst. a des Ombudsgesetzes [BGS 156.1].

49 Art. 39 Abs. 3 des Bundesgesetzes über die Harmonisierung der direkten Steuern der Kantone und Gemeinden [StHG, SR 642.14].

50 § 110 des Steuergesetzes [StG, BGS 632.1].

treffend war. Die betroffenen Fahrzeughalter gingen davon aus, dass der Autohändler ihre Angaben nur vom Zuger Strassenverkehrsamt erhalten haben konnte.

Gestützt auf das Strassenverkehrsrecht des Bundes, gibt das Strassenverkehrsamt im Einzelfall auf Anfrage zu einem bestimmten Kontrollschild nur Namen und Adresse des Halters bekannt.<sup>51</sup>

Das Jahr der erstmaligen Inverkehrsetzung eines Fahrzeugs ist dem Strassenverkehrsamt zwar bekannt, wird anfragenden Privaten jedoch in keinem Fall mitgeteilt. Das Strassenverkehrsamt kam somit als Datenquelle nicht in Frage. Es war vielmehr davon auszugehen, dass der Garagist der betroffenen Kunden die fraglichen Daten dem Autohändler bekannt gegeben hatte.

Fazit: Das Strassenverkehrsamt betreibt mit Halterdaten keinen Handel.

Datenbekanntgabe zu verweigern ist, wenn dadurch schutzwürdige Interessen einer betroffenen Person beeinträchtigt werden.<sup>53</sup>

Fazit: Der Anspruch auf Bekanntgabe einer Adresse ist nicht absolut, es können überwiegende schutzwürdige Interessen der betroffenen Person berücksichtigt werden. In der Praxis ist dabei Voraussetzung, dass der Einwohnerkontrolle solche überhaupt bekannt sind.

#### Fall 20 Desolater Zustand einer Wohnung – Meldung an die Vormundschaftsbehörde?

Eine Mitarbeiterin der Familienhilfe hat festgestellt, dass die Wohnung einer unterstützten Familie mit einem Kind in einem sehr schmutzigen und desolaten Zustand ist. Die Familienhelferin hat die Familie verschiedentlich erfolglos aufgefordert und gemahnt, die Wohnung in Ordnung zu bringen. Es fragt sich, ob die Vormundschaftsbehörde beziehungsweise der Beistand des Kindes informiert werden darf.

«Jede Person, die eine Gefährdung des Kindeswohls wahrnimmt, insbesondere Amtspersonen und diejenigen Personen, die beruflich mit der Betreuung oder der medizinischen oder psychologischen Behandlung von Kindern zu tun haben und im Rahmen ihrer Tätigkeit eine Gefährdung des Kindeswohls wahrnehmen, ist verpflichtet, der zuständigen Vormundschaftsbehörde Anzeige zu erstatten» – so lautet die hier wichtige Gesetzesbestimmung.<sup>54</sup> Kommt die Familienhilfe somit zum Schluss, dass die Zustände derartig sind, dass das Kindeswohl gefährdet ist, ist sie verpflichtet, die zuständige Vormundschaftsbehörde zu informieren. Zwischen der Familienhilfe und den durch sie betreuten Familien muss jedoch ein gewisses Vertrauensverhältnis bestehen, nur so kann die Familienhilfe ihre Aufgabe erfüllen. Dies verlangt, dass verhältnismässig vorgegangen wird. Vorweg ist daher zu versuchen, auf gutlichem Weg die Zustände zu verbessern, allenfalls mit dem Hinweis auf die bevorstehende Information des Beistandes. Ist dieses Vorgehen erfolglos, ist in einem nächsten Schritt der Beistand beziehungsweise die Vormundschaftsbehörde zu informieren.

## 6. Gemeinden

#### Fall 19 Adressauskunft: Es besteht keine Sperre – kann die Auskunft trotzdem verweigert werden?

Auf Anfrage im Einzelfall gibt die Einwohnerkontrolle voraussetzungslos die Adresse einer bestimmten Person bekannt. Die Anfrage bedarf somit keiner Begründung. Hat die betroffene Person ihre Daten gesperrt, wird die Auskunft verweigert. Wir wurden angefragt, ob eine nicht gesperrte Adresse in jedem Fall bekannt zu geben ist oder ob sie allenfalls auch verweigert werden kann.

Der Grundsatz besagt, dass eine nicht gesperrte Adresse bekannt zu geben ist. Liegen jedoch Anhaltspunkte vor, dass eine Adresse missbraucht werden könnte oder dass davon auszugehen ist, dass die betroffene Person ein überwiegendes schutzwürdiges Interesse geltend machen könnte,<sup>52</sup> so ist die Bekanntgabe zu verweigern, wie wenn eine Sperre eingerichtet wäre.

Diese Rechtslage ergibt sich aufgrund des Datenschutzgesetzes, sieht dieses doch vor, dass die

51 Art. 126 Abs. 1 der Verkehrszulassungsverordnung [VZV, SR 741.51] lautet:

<sup>1</sup> Namen und Adresse von Inhabern eines Kontrollschildes können jedermann bekannt gegeben werden.

<sup>2</sup> Über die Namen von Fahrzeughaltern und ihre Versicherer ist bei Unfällen gegenüber den Beteiligten und bei Halterwechsel gegenüber dem neuen Halter Auskunft zu erteilen.

<sup>3</sup> Angaben aus dem Fahrzeugausweis dürfen auf begründetes schriftliches Gesuch Personen bekannt gegeben werden, die im Hinblick auf ein Verfahren ein zureichendes Interesse geltend machen.

52 Wenn etwa bekannt ist, dass eine Frau von ihrem ehemaligen, gewalttätigen Partner verfolgt wird, sie aus Nichtwissen jedoch keine Adresssperre verlangt hat.

53 § 8 Abs. 2 Bst. d Datenschutzgesetz.

54 § 34 des Gesetzes betreffend die Einführung des Schweizerischen Zivilgesetzbuches für den Kanton Zug [EG ZGB, BGS 211.1].

## III. Unsere Öffentlichkeitsarbeit

### 1. Website

Auf unserer Website «www.datenschutz-zug.ch» finden Sie viele wichtige Informationen und weiterführende Links zu Datenschutz und Datensicherheit in Zug, der Schweiz und auf internationaler Ebene. Auch steht Ihnen dort das Register aller Zuger Datensammlungen des Kantons und aller Gemeinden zur Verfügung.<sup>55</sup> Den Inhalt der Website überprüfen und aktualisieren wir etwa alle zwei Wochen.

#### Wie wird unser Web-Angebot genutzt?

Täglich besuchen 60 bis 150 einzelne Personen aus der Schweiz die DSB-Website während 5 bis 10 Minuten. Im Vergleich zum letzten Jahr hat die Nutzung erfreulicherweise weiter stark zugenommen – insgesamt um rund 40%.<sup>56</sup>

Viele wichtige Dokumente stehen auf der DSB-Website zur Verfügung. Die zehn meistverlangten Dokumente wurden im Berichtsjahr zwischen 310 und 4400 Mal heruntergeladen. Im Vergleich zum Vorjahr bedeutet dies teilweise eine Verdoppelung, teilweise sogar eine Vervierfachung der Downloads. Hier die zehn meistverlangten Dokumente:

– DSB TB 2010	4470
– Massnahmenkatalog: Muster	2840
– Massnahmenkatalog: Vorlage	2780
– Merkblätter zur Datensicherheit	1520
– DSB TB 2004	860
– Botschaft des Bundesrates zum DSG	710
– Hinweise des EDÖB zur Internet-Nutzung	630
– unser Beitrag in GVP 2002	570
– Zuger Datenschutzgesetz	460
– unser Beitrag in schulinfo 2005/3	310

**Fazit:** Unser Internetangebot wird wahrgenommen und sehr rege genutzt.

### 2. Newsletter

Das Konzept unseres Web-Auftritts hat sich sehr bewährt: Alle grundlegenden Informationen werden auf der Website veröffentlicht.<sup>57</sup> Aktuelles aus den Bereichen Datenschutz und Datensicherheit wird hingegen per E-Mail in Form von Kurzhinweisen – versehen mit Links auf Fundstellen, wo sich ausführliche Informationen finden – verschickt.<sup>58</sup> Unser Newsletter kann auf einfachste Weise abonniert werden: Es genügt, wenn man auf der entsprechenden Seite der DSB-Website<sup>59</sup> seine E-Mail-Adresse bekannt gibt, mehr braucht es nicht. Wer übrigens keine Nachrichten mehr erhalten möchte, kann sich ebenso einfach selber wieder aus der Versandliste des Newsletters austragen.

#### Hier das Wichtigste in Kürze:

##### Häufigkeit des Nachrichtenversands

Monatlich werden per E-Mail 2 bis 3 Kurznachrichten verschickt.

##### Archiv der verschickten Nachrichten

Sämtliche verschickten Nachrichten sind in einer Archiv-Datenbank gespeichert [z. T. mit zusätzlichen Dokumenten versehen]. Diese Datenbank ist via Website auch für nicht eingeschriebene Personen zugänglich. Das Archiv verfügt über eine effiziente Suchmaschine. Ende 2011 befanden sich insgesamt 896 Nachrichten im Archiv.

##### Besucherstatistik 2011

Pro Monat besuchen zwischen 60 und 120 Personen das Archiv. Das entspricht einer starken Abnahme im Vergleich zum Vorjahr. Dabei werden pro Monat zwischen 20 und 30 PDF-Dokumente heruntergeladen – auch dies ein massiver Rückgang der Downloads im Vergleich zum Vorjahr. Der Rückgang der Archivnutzung ist schwer erklärbar, da die Zahl der Abonnierten erneut stark zugenommen hat, ebenso die Nutzung unserer Website. Wir werden im kommenden Jahr unsere Bemühungen verstärken.

##### Zuwachs der Abonnenten 2011

+ 67 Neuabonnierte!

##### Verschickte Nachrichten 2011

21 per E-Mail verschickte Nachrichten

##### Abo-Kosten

keine

##### Fazit

Schreiben auch Sie sich ein – es lohnt sich.

55 Näheres zum Register der Datensammlungen s. hinten S. 27.

56 Gemäss der bereinigten Statistik – wobei zu beachten ist, dass statistische Auswertungen der Internetnutzung grundsätzlich mit einiger Vorsicht zu geniessen sind [siehe dazu unsere ausführlichen Hinweise in DSB TB 2004 S. 23 Ziff. 2.1.].

57 Insbesondere Gesetze, Literatur, Adressen und Links.

58 Verschickt werden Hinweise zu Aktuellem aus Gesetzgebung, Rechtsprechung, Medienberichterstattung sowie Hinweise auf Veranstaltungen und Literatur.

59 «www.datenschutz-zug.ch», Rubrik «Newsletter/Anmeldung».

### 3. Tätigkeitsbericht 2010

Unser Tätigkeitsbericht erscheint in einer Auflage von 1500 Exemplaren und soll die Themen Datenschutz und Datensicherheit einem breiten Publikum vorstellen. Worum es beim Datenschutz geht, wird insbesondere anhand von konkreten Fällen aus unserer Beratungspraxis des Berichtsjahrs gezeigt. Dabei versuchen wir, die Fälle möglichst kurz, verständlich und praxisnah zu präsentieren.

Neben der Öffentlichkeit sollen aber insbesondere auch die Mitarbeitenden der Verwaltung bezüglich Datenschutz und Datensicherheit sensibilisiert und auch ein Stückweit ausgebildet werden.

Sehr erfreulich ist, dass die meisten Zuger Gemeinden unser kostenloses Angebot nutzen und unseren Tätigkeitsbericht jeweils für einen Teil – einige auch für alle – ihrer Mitarbeitenden bestellen. Eine kostengünstigere und effizientere Sensibilisierungsmassnahme im Bereich Datenschutz/Datensicherheit gibt es vermutlich nicht.

Auch wenn der kantonale Datenschutzbeauftragte für die Datenbearbeitung von Privatpersonen und Unternehmen nicht zuständig ist, gehen trotzdem viele Bestellungen auch von Privaten und von Unternehmen ein. Dies ist sinnvoll, da sehr viele Informationen und Hinweise im Tätigkeitsbericht nicht nur für die Verwaltung, sondern in analoger Weise auch in den Unternehmen relevant sind.

Ein Hinweis zur Print-Ausgabe: Allen elektronischen Medien und Geräten zum Trotz – nach wie vor ziehen sehr viele Personen für ihre Arbeit den gedruckten Tätigkeitsbericht der elektronischen Version vor. Wer die Papierversion bei uns bestellt, das PDF somit nicht auf seinem Drucker ausdruckt, handelt übrigens ökologischer, weil die Print-Ausgabe in hoher Auflage auf umweltfreundlichem Papier und mit optimierter Technik hergestellt wird.

Print-Ausgabe und PDF ergänzen sich somit und stellen – je nach Zielgruppe – beide eine nützliche Arbeitshilfe dar.

[Wer die letztjährigen Tätigkeitsberichte zurate ziehen möchte, kann sie beim DSB kostenlos bestellen oder sie auf der DSB-Website<sup>60</sup> als PDF herunterladen.](#)

### 4. «Gerichts- und Verwaltungspraxis des Kantons Zug»

Die offizielle Zuger Publikation, die einmal pro Jahr einen umfassenden und vertieften Einblick in die Rechtsprechung der Zuger Gerichte und der Verwaltung gibt, ist die «Gerichts- und Verwaltungspraxis des Kantons Zug» [GVP]. Sie richtet sich in erster Linie an ein juristisch interessiertes Fachpublikum. Die GVP wird von der Staatskanzlei herausgegeben und erscheint in einer Auflage von 700 Exemplaren.

Der Datenschutzbeauftragte publiziert in der GVP Stellungnahmen aus seiner Beratungspraxis. In GVP 2010<sup>61</sup> veröffentlichte er die folgenden fünf Fälle:

- Datenbeschaffung durch die Steuerverwaltung
- Videoaufnahmen für Audits an Schulen?
- Vertrauensärztliche Kontrolluntersuchung – welche Daten gehen ans Strassenverkehrsamt?
- Zum Datenaustausch zwischen Asylbehörde und Polizei
- Einsicht in Akten abgeschlossener Strafverfahren

[Die Beiträge des DSB in der GVP der Jahre 2000 bis 2010 können von der DSB-Website<sup>62</sup> heruntergeladen werden.](#)

60 «www.datenschutz-zug.ch» [Rubrik «Tätigkeit»].

61 GVP 2010 S. 328–336.

62 «www.datenschutz-zug.ch» [Rubrik «Tätigkeit»].

## 5. «Schulinfo Zug»

Das Magazin «Schulinfo Zug» informiert Lehrpersonen aller Stufen, Schulbehörden und weitere interessierte Stellen über Aktuelles aus der Zuger Schule. Diese wichtige und attraktive Schulpublikation wird von der Direktion für Bildung und Kultur herausgegeben. Sie erscheint dreimal pro Jahr in einer Auflage von 3400 Exemplaren.

Weil wir regelmässig Anfragen aus dem Schulbereich erhalten, stellen die Herausgeber dem DSB freundlicherweise jeweils pro Ausgabe eine Seite zur Verfügung, um die Leserschaft kurz über Aktuelles aus dem Bereich Datenschutz und Schule zu informieren. Im Berichtsjahr hat der DSB die folgenden drei Beiträge verfasst: «Sensibilisierungskampagne NetLa»<sup>63</sup>, «Weiterbildung zum Datenschutz»<sup>64</sup> und «Wenn Schüler straffällig werden – was erfährt die Schule?»<sup>65</sup>.

Die Beiträge des DSB in der «Schulinfo Zug» der Jahre 2004 bis 2011 können von der DSB-Website heruntergeladen werden.

## 6. «Personalzeitig»

Die Personalzeitung der Zuger Verwaltung erscheint viermal pro Jahr in einer Auflage von jeweils 2750 Exemplaren. Sie wird allen aktiven und pensionierten Mitarbeitenden der Zuger Verwaltung sowie weiteren Kreisen kostenlos zugestellt.

Die «Personalzeitig» veröffentlichte im Berichtsjahr ein zweiseitiges Interview mit dem Datenschutzbeauftragten über die Nutzung von PC, Internet und E-Mail am Arbeitsplatz zu privaten Zwecken.<sup>66</sup> In einem weiteren Beitrag<sup>67</sup> konnte der DSB den Verwaltungsmitarbeitenden vier aktuelle Fälle aus der Praxis vorstellen, die einen direkten Bezug zu ihrer Arbeit haben: Ist die Videoüberwachung eines Büros der Verwaltung zulässig? Das Zuger E-Learning-Tool – damit Sie über Datensicherheit Bescheid wissen. Zum

Umgang mit «cc» und «bc» beim Verschicken von E-Mails. Wie sicher ist der Versand von passwortgeschützten Dokumenten?

## 7. In der Zeitung – die Kolumne «Ratgeber Datenschutz»

Der Datenschutzbeauftragte betreute im Berichtsjahr für die Zuger Presse die Kolumne «Ratgeber Datenschutz». Er verfasste die folgenden sechs Beiträge:

- Wie gefährlich ist Surfen?
- Fahren auch Sie im gläsernen Auto?
- Facebook und Ihre Bewerbung
- Ein Testament für unsere Daten?
- Sind auch wir alle bald Promis?
- Datenklau am Bancomat

Die Kolumne soll die Leserinnen und Leser in Sachen Datenschutz und Datensicherheit sensibilisieren und ihnen praktische Tipps für den Umgang mit ihren eigenen Daten geben.

## 8. Zuger Datenschutz in den Medien

Über Datenschutz oder die Zuger Datenschutzstelle berichteten die Zuger Printmedien und Lokalradios verschiedentlich. Im Zentrum stand die Veröffentlichung unseres Tätigkeitsberichts des Vorjahres. Aber auch im Zusammenhang mit Gesetzgebung, Politik oder weiteren datenschutzrechtlichen Aktualitäten erhielten wir Anfragen von Medien, so etwa zum Umgang mit den persönlichen Daten bei facebook oder zur Zulässigkeit der polizeilichen Fahndung im Internet.

Über die Veröffentlichung unseres Tätigkeitsberichts 2010 berichteten auch verschiedene deutsche Medien.<sup>68</sup>

63 Schulinfo Zug 2010-11/Nr. 3 S. 48.

64 Schulinfo Zug 2011-12/Nr. 1 S. 49.

65 Schulinfo Zug 2011-12/Nr. 2 S. 38/39.

66 Personalzeitig Nr. 56/2011 S. 24/25.

67 Personalzeitig Nr. 57/2011 S. 24/25.

68 Datenschutz und Datensicherheit/DuD 2011/6 S. 433, Datenschutz-Berater/DSB 05/2011 S. 4 und Medienmitteilung des «Virtuellen Datenschutzbüros» vom 29. März 2011.

## IV. Mitarbeit bei der Gesetzgebung

«Die kantonale Datenschutzstelle nimmt zu rechtsetzenden Erlassen aus datenschutzrechtlicher Sicht Stellung» – so lautet eine der vielen Aufgaben, die in § 19 des Datenschutzgesetzes dem Datenschutzbeauftragten übertragen ist. Dies wurde durch den Gesetzgeber zu Recht so vorgesehen. Denn: Werden neue Rechtserlasse geschaffen, werden grundlegende und weitreichende Weichenstellungen für die Zukunft getroffen. Dabei muss der verfassungsmässige Schutz der Privatsphäre der Bürgerinnen und Bürger beachtet werden. Die Mitarbeit bei der Gesetzgebung ist für den Datenschutzbeauftragten daher wichtig.

Damit der DSB seinen Auftrag auch erfüllen kann, ist die Verwaltung verpflichtet, ihn über geplante Rechtsetzungserlasse unaufgefordert, frühzeitig und vollständig zu informieren. Dabei bedeutet «frühzeitig»: sobald ein Projekt in Angriff genommen wird. Das ist wichtig, weil dann noch Varianten, Alternativen und Verbesserungen gesucht und gefunden werden können.

Wie sah es diesbezüglich im Berichtsjahr aus? Der Einbezug des DSB bei der Gesetzgebung hat sich in den letzten Jahren gut eingespielt und ist weitgehend eine Selbstverständlichkeit. Die Direktionen haben auf ihren Anträgen an den Regierungsrat jeweils darauf hinzuweisen, dass das Geschäft auch dem Datenschutzbeauftragten zur Kenntnis gebracht worden ist.

Gelegentlich kommt es allerdings vor, dass eine vorbereitende Stelle die Datenschutzrelevanz eines Gesetzesprojektes übersieht. In diesem Fall weist der Regierungsrat die Vorlage an die zuständige Direktion zurück, diese hat die Stellungnahme des DSB einzuholen.

Im Berichtsjahr hat die Information seitens des Regierungsrates an den Kantonsrat bezüglich wichtiger Stellungnahmen des DSB teilweise nicht geklappt. Das Büro des Kantonsrates hat deshalb den DSB aufgefordert, die jeweiligen Kommissionen des Kantonsrates bei wichtigen Geschäften selber zu informieren. Näheres dazu s. vorne S. 4.

### 1. Vernehmlassungen

Sollten Sie sich für eine der untenstehenden Stellungnahmen des Datenschutzbeauftragten interessieren – in aller Regel können wir sie Ihnen gerne kostenlos zusenden. E-Mail genügt.

#### Bundesrecht

Schafft der Bund neues Recht, können sich die Kantone dazu in aller Regel frühzeitig äussern. Tangiert eine solche Vorlage Datenschutz/Datensicherheit – was sehr oft der Fall ist –, so lädt der Regierungsrat den DSB zu einer Stellungnahme ein. Nicht immer, aber sehr oft übernimmt der Regierungsrat in seiner Vernehmlassungsantwort gegenüber dem Bund die Hinweise des DSB. Im Berichtsjahr hat der Datenschutzbeauftragte insbesondere zu den folgenden Vorlagen Stellung genommen:

- Änderung der Bundesverfassung, des Strafgesetzbuches, des Militärstrafgesetzes und des Jugendstrafgesetzes [betr. Tätigkeitsverbot und Kontakt- und Rayonverbot]
- Änderung des Bundesstatistikgesetzes und der Statistikerhebungsverordnung: Vorentwurf der Staatspolitischen Kommission des Nationalrates betr. «Keine Ausweitung der obligatorischen Auskunftspflicht bei statistischen Erhebungen des Bundes»
- Änderung der Strafprozessordnung: Vorentwurf der Kommission für Rechtsfragen des Nationalrates betreffend Präzisierung des Anwendungsbereichs der Bestimmungen über die verdeckte Ermittlung
- Bundesgesetz über das elektronische Patientendossier
- Verordnung über die Überwachung des Post- und Fernmeldeverkehrs [VÜPF]
- Verordnung über das Zentrale Migrationsinformationssystem [ZEMIS-Verordnung]

#### Kantonales Recht

Der DSB hat im Berichtsjahr insbesondere zu den folgenden Vorlagen Stellung genommen:

- Konkordat über private Sicherheitsdienstleistungen vom 12. November 2010
- Teilrevision Kantonsverfassung sowie Wahl- und Abstimmungsgesetz

- Revision Datenschutzgesetz [Schengen]
- Revision Polizeigesetz [Schengen]
- Revision Polizeigesetz [verdeckte polizeiliche Vorermittlung]
- Gesetz über die Videoüberwachung des öffentlichen und öffentlich zugänglichen Raums
- Gesetz über Geoinformation im Kanton Zug
- Revision des Gemeindegesetzes
- Änderung des Schulgesetzes
- Übertretungsstrafgesetz
- Totalrevision des Einführungsgesetzes zum Bundesgesetz über die Ausländerinnen und Ausländer und zum Asylgesetz
- Gesetz betreffend die Einführung des Schweizerischen Zivilgesetzbuches für den Kanton Zug [EG ZGB] betr. des Kindes- und Erwachsenenschutzrechts
- Teilrevision Personalgesetz [betr. Whistleblowing/Meldestelle]
- Zuger Spitalliste 2012
- Totalrevision der Verordnung zur Einführung des Bundesgesetzes über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekanntem oder vermissten Personen [kantonale DNA-Verordnung]
- Änderung der Verordnung zum Schulgesetz [betr. den Schulpsychologischen Dienst]
- Verordnung über die Aktenführung [«GEVER-Verordnung»]
- Änderung der Delegationsverordnung [betr. den Datenschutzbeauftragten]
- Totalrevision der Vollziehungsverordnung zum Bundesgesetz über explosionsgefährliche Stoffe
- Verordnung zum Einführungsgesetz betreffend Zivilschutz
- personalrechtliche Weisung des Regierungsrates betr. Austrittsgespräche

- Interpellation von Markus Jans betreffend die Installation von Sound-Systemen zur Vertreibung von Jugendlichen beim Gewerblich-Industriellen Bildungszentrum Zug<sup>71</sup>
- Postulat von Kantonsrat Daniel Stadlin betreffend Solarkataster<sup>72</sup>

## 2. Unsere Mitarbeit bei ausgewählten Rechtserlassen

### Revision Datenschutzgesetz

Das Schengen-Recht verlangt eine stärkere Unabhängigkeit des Datenschutzbeauftragten von der Verwaltung. Das Datenschutzgesetz muss deshalb angepasst werden. Dies hat die Regierung im Jahr 2009 beschlossen. Über dieses Gesetzgebungsprojekt haben wir bereits im letzten Tätigkeitsbericht ausführlich berichtet.<sup>73</sup> Folgendes war 2011 Sache:

Die federführende Sicherheitsdirektion überarbeitete die Vorlage im ersten Quartal und führte im Sommer ein zweites internes Mitberichtsverfahren durch. Nach der Auswertung der eingegangenen Stellungnahmen kam die Vorlage – zusammen mit den Änderungen des Polizeigesetzes – am 20. September 2011 zur ersten Lesung in den Regierungsrat. Der Chef der Zuger Kriminalpolizei stand dem Regierungsrat dabei als Experte für den polizeilichen Teil, der DSB für den datenschutzrechtlichen Teil der Vorlagen für ergänzende mündliche Hinweise zur Verfügung. Der Regierungsrat verabschiedete die Vorlage. Vom 4. Oktober 2011 bis zum 10. Januar 2012 dauerte das externe Vernehmlassungsverfahren. Es ist davon auszugehen, dass der Regierungsrat die Vorlage im Sommer 2012 dem Kantonsrat vorlegen wird.

Positiv fällt auf:

- neu wird der Datenschutzbeauftragte durch den Kantonsrat auf eine Amtszeit von vier Jahren gewählt;
- geklärt wurden verschiedene Punkte, die mit der verstärkten Unabhängigkeit im Zusammenhang stehen.

69 Vorlage Nr. 1923.1.

70 Vorlage Nr. 1681.1-12750.

71 Vorlage Nr. 1751.1-12918 vom 11. November 2008.

72 Vorlage Nr. 2075.1-13873 vom 6. September 2011.

73 DSB TB 2010 S. 24.

### Stellungnahmen zu politischen Vorstössen

- Motion der erweiterten Justizprüfungskommission betreffend Erarbeitung gesetzlicher Grundlagen zur Weitergabe von Informationen durch die Generalsekretäre<sup>69</sup>
- Motion der CVP-Fraktion betreffend Einführung eines wirksamen Kontrollmechanismus über den Geschäftsgang in der kantonalen Verwaltung<sup>70</sup>

Aus unserer Sicht besteht bezüglich Folgendem Verbesserungspotenzial: Der DSB hat ein eigenes Budget, das er im Kantonsrat vertreten kann. Wir haben – bis anhin erfolglos – vorgeschlagen, dass der DSB sein Budget bereits auch in den vorbereitenden Gremien vertreten kann bzw. diesen bei deren Beratung mündlich Hinweise geben kann, so bei der Beratung durch den Regierungsrat, durch die Delegation der Staatswirtschaftskommission und durch die Staatswirtschaftskommission.

Im Weiteren haben wir darauf hingewiesen, dass die Strafbestimmung nicht bloss Busse als Höchststrafe vorsehen soll, sondern bei sehr schweren Verstössen auch Freiheitsstrafe [analog zu Amtsgeheimnisverletzungen nach Art. 320 StGB].

#### Revision Polizeigesetz: Schengen

Wie die Revision des Datenschutzgesetzes ist auch die Revision des Polizeigesetzes weitgehend durch Schengen vorgegeben. Die beiden Projekte bilden denn auch ein Gesamtpaket und unterliegen dem gleichen Fahrplan [s. oben].

Im bisherigen Gesetzgebungsverfahren wurden unsere Hinweise weitgehend berücksichtigt – bis auf die beiden folgenden Punkte: Einträge im Polizei-Journal dürfen nicht geheim gehalten werden, sondern müssen unseres Erachtens betroffenen Personen grundsätzlich offengelegt werden, da sie sehr wichtige Informationen über diese enthalten können. Zudem geht es aus Gründen der Rechtsstaatlichkeit nicht an, dass die Polizei Informationen von Dritten entgegennehmen kann, ohne allenfalls diese Quellen den Betroffenen offenzulegen.

#### Revision Polizeigesetz: verdeckte polizeiliche Vorermittlung

Verdeckte polizeiliche Vorermittlung – darum geht es hier: Mitarbeiter der Polizei oder beauftragte Dritte [!] geben sich dem Bürger gegenüber unter einer fiktiven Identität aus und täuschen diesen somit aktiv, um an gewisse Daten oder Informationen zu kommen. In der Praxis: Ein Polizist gibt sich als Drogenverkäufer, als Waffenhändler, als Chat-Partner oder als Kunsthändler

aus, um im jeweiligen Umfeld abzuklären, ob Personen möglicherweise zukünftig beabsichtigen, Straftaten zu begehen. Zur Klarstellung: Es geht hier somit nicht darum, bereits begangene Straftaten abzuklären, sondern herauszufinden, ob in Zukunft allenfalls Straftaten begangen werden könnten.

Unbestritten ist, dass dem Staat dieses Instrument für die Verbrechensbekämpfung grundsätzlich zur Verfügung stehen muss. Weil diese Materie in einem Rechtsstaat aber per se äusserst heikel ist, da sie in schwerer Weise verfassungsmässige Grundrechte tangiert, müssen die gesetzlichen Grundlagen höchsten Anforderungen genügen. Diese ergeben sich insbesondere auch aufgrund langjähriger Praxis des Bundesgerichts. Verletzen solche kantonale Rechtsgrundlagen die Verfassung, sind sie unbeachtlich und allfällig erhobene Beweismittel der Polizei dürfen in Strafverfahren nicht berücksichtigt werden.

Erstaunlich war es daher, dass der DSB durch die zuständige Sicherheitsdirektion über die geplante Änderung des Polizeigesetzes zur Regelung der verdeckten polizeilichen Vorermittlung erst im allerletzten Moment informiert wurde. Unseres Wissens wurde diese Gesetzesrevision zudem durch den Regierungsrat nur in einer – üblich sind zwei – Lesung beraten, ein eigentliches Mitberichtsverfahren wurde nicht durchgeführt, ebenso wenig eine öffentliche Vernehmlassung. Tempo war hier offenbar alles.

Der DSB konnte gegenüber dem Regierungsrat eine Stellungnahme abgeben. Allerdings blieben viele Hinweise des DSB unberücksichtigt. Am 1. März 2011 ging die Vorlage an den Kantonsrat.<sup>74</sup> Im Vorfeld der Beratung durch die zuständige Kommission des Kantonsrates erkundigte sich ein Mitglied beim DSB nach der Datenschutzrelevanz der Vorlage. In der Folge besprach der Kommissionspräsident mit dem Datenschutzbeauftragten dessen Stellungnahme detailliert. Der DSB wies insbesondere auf die folgenden Punkte hin:

- Die verdeckte polizeiliche Vorermittlung sollte nicht im Polizeigesetz in einer einzigen Bestimmung, sondern vielmehr in einem

74 Bericht und Antrag des Regierungsrates vom 1. März 2011 betr. Änderung des Polizeigesetzes [Rechtsgrundlagen für die polizeiliche verdeckte Vorermittlung], Vorlage Nr. 2020.1-13699.

eigenständigen Gesetz sorgfältig geregelt werden.

- Mindestens sind jedenfalls zu regeln: die Rechte und Pflichten der Ermittelnden, das Mass der zulässigen Einwirkung, die Beendigung der Einsätze und die Verwendung von Vorzeigegeld.
- Personen, gegen die zu Unrecht verdeckt ermittelt wurde, sind darüber zu informieren.
- Aus rechtsstaatlichen Gründen ist das Instrument der verdeckten Ermittlung einem Controlling zu unterwerfen. Zu berichten wäre jedenfalls über den polizeilichen Aufwand, über den Erfolg, über die Anzahl erteilter und verweigerter Gesuche durch das Zwangsmassnahmengericht und über die Dauer der verdeckten Ermittlungsverfahren.
- Auch ein politisches Controlling ist bezüglich einer rechtsstaatlich derart sensiblen Materie ausdrücklich vorzusehen. Es kann etwa darin bestehen, dass die Genehmigungspraxis des Zwangsmassnahmengerichts sowie die polizeiliche Tätigkeit auf diesem Gebiet einmal pro Jahr explizit und zwingend durch die Justizprüfungskommission näher zu überprüfen sind.

Die kantonsrätliche Kommission und anschliessend auch der Kantonsrat haben sich mit den Hinweisen des DSB auseinandergesetzt, haben aber schliesslich die Vorlage des Regierungsrates unverändert beschlossen.<sup>75</sup> In der Beratung hat der Kommissionspräsident ausgeführt, die Kommission erwarte aber ausdrücklich, dass die verdeckte polizeiliche Vorermittlung «eng» zu führen sei und zudem, dass die Polizei im Rechenschaftsbericht adäquat informiere.<sup>76</sup>

Ob die getroffene Lösung verfassungskonform ist, wird sich dann zeigen, wenn das Bundesgericht in einem Fall zu prüfen hat, ob Beweise, die im Rahmen einer verdeckten polizeilichen Vorermittlung erhoben wurden, verwertbar sind.

#### Entwurf Videoüberwachungsgesetz

Im Kanton Zug ist der Einsatz von Videoüberwachung gesetzlich nach wie vor nicht geregelt. Aufgrund eines politischen Vorstosses aus dem Jahre 2007<sup>77</sup> ist die Sicherheitsdirektion zurzeit

damit befasst, eine Vorlage auszuarbeiten.<sup>78</sup> Wir berichteten darüber bereits im letzten Tätigkeitsbericht.<sup>79</sup> Im Berichtsjahr hat uns die Sicherheitsdirektion nun dazu eingeladen, zu einem ersten Entwurf Stellung zu nehmen. Anlässlich einer Besprechung mit dem Sicherheitsdirektor im Herbst konnten verschiedene wichtige Punkte geklärt werden. Den in der Folge überarbeiteten Entwurf schickte die Sicherheitsdirektion den Direktionen und den Gerichten im Rahmen des internen Mitberichtsverfahrens zur Stellungnahme bis Ende 2011. Der DSB hat sich zu diesem Entwurf ebenfalls geäussert. Zurzeit befasst sich die Sicherheitsdirektion mit der Auswertung der Stellungnahmen und der Überarbeitung der Vorlage. Es ist davon auszugehen, dass der Regierungsrat die Vorlage im Frühjahr 2012 in erster Lesung beraten wird. Darüber werden wir Sie gerne in unserem Newsletter informieren.

#### Geoinformationsgesetz

Geoinformationsrecht – eine eher neue und sehr komplexe Materie, bei der es um die gesetzliche Regelung von Daten und Informationen geht, die einen Bezug zu Grund und Boden haben und die insbesondere geografischer, räumlicher oder rechtlicher Natur sein können.

Das Geoinformationsgesetz des Bundes sieht vor,<sup>80</sup> dass die Kantone ihre Gesetzgebung über die Geoinformation bis Juli 2011 anzupassen haben. Der Regierungsrat hat das Gesetz über Geoinformation im Kanton Zug [GeolG-ZG] im Dezember 2010 in erster Lesung beraten und es anschliessend bis am 31. März 2011 in die öffentliche Vernehmlassung gegeben. Der DSB hat dazu – wie bereits im internen Mitberichtsverfahren – eine Stellungnahme abgegeben. Die meisten Hinweise hat der Regierungsrat in der zweiten Lesung vom 12. Juli 2011 nicht übernommen. Gleichentags ging die Vorlage an den Kantonsrat.<sup>81</sup>

Weil die datenschutzrechtlichen Anliegen in der Vorlage des Regierungsrates weitgehend unberücksichtigt und im Bericht kleingeredet wurden, wandte sich der Datenschutzbeauftragte mit Stellungnahme vom 25. Oktober 2011 an die zuständige Kommission des Kantonsrats.

75 Einfügen von § 10a (neu) und § 43 Abs. 4 (neu) in das Polizeigesetz, Vorlage Nr. 2020.5-13837; Inkrafttreten: 17. September 2011.

76 Protokoll des Kantonsrates vom 5. Mai 2011 S. 185/186.

77 Motion von Andreas Hausheer vom 8. November 2007 [Vorlage Nr. 1606.1-12 534]. Unsere Ausführungen dazu finden sich im DSB TB 2008 S. 24.

78 Mit dem Arbeitstitel: Gesetz über die Videoüberwachung des öffentlichen und öffentlich zugänglichen Raums [Videoüberwachungsgesetz; VideoG].

79 DSB TB 2010 Fall Nr. 5 S. 12/13.

80 Bundesgesetz über Geoinformation [Geoinformationsgesetz, GeolG; SR 510.62].

81 Bericht und Antrag des Regierungsrates vom 12. Juli 2011 [Vorlage Nr. 2068.1-13848].

Er wies darauf hin, dass:

- es sich bei den meisten raumbezogenen Daten um Personendaten handelt, da ohne Weiteres der Bezug zum Grundeigentümer hergestellt werden kann. Die Beachtung dessen Privatsphäre ist wichtig und muss deshalb im Gesetz ausdrücklich erwähnt werden;
- kantonale und gemeindliche Geobasisdaten nur aufgrund einer entsprechenden gesetzlichen Grundlage bearbeitet werden dürfen;
- bei der Bearbeitung von kantonalen oder gemeindlichen raumbezogenen Daten nicht das eidgenössische Datenschutzgesetz, sondern das kantonale Datenschutzgesetz zur Anwendung kommt;
- dem Regierungsrat keine Blankovollmacht für die Verknüpfung des GIS Zug mit beliebigen «anderen Informationssystemen» zu erteilen ist, insbesondere nicht für Verknüpfungen mit Informationssystemen, die Personendaten von Zuger Bürgerinnen und Bürgern enthalten;
- es nicht zulässig ist, dass der Regierungsrat alle raumbezogenen Daten – somit Daten der GrundeigentümerInnen – im Internet veröffentlicht.

Auf Einladung der Kommissionspräsidentin konnte der DSB seine Hinweise der Kommission anlässlich der Sitzung vom 31. Oktober 2011 mündlich erläutern und Fragen der Kommissionsmitglieder beantworten. Es wurde dabei auch ein allfälliges Recht der GrundeigentümerInnen auf Sperrung ihrer Daten im Internet zur Sprache gebracht und sowohl von der Kommission wie auch von der Staatswirtschaftskommission befürwortet.

Über die Ergebnisse der ersten Lesung im Kantonsrat im ersten Quartal 2012 werden wir Sie in unserem Newsletter<sup>82</sup> gerne informieren.

## V. Register der Datensammlungen

### Was ist das Register der Datensammlungen?

In der Schweiz dürfen die Behörden nicht im Geheimen Daten über Bürgerinnen und Bürger sammeln und bearbeiten. Die staatlichen Datenbearbeitungen müssen gegenüber den Betroffenen und der Öffentlichkeit vielmehr transparent sein.

Im Zuger Datenschutzgesetz steht deshalb, dass jedermann das Recht hat, grundsätzlich jederzeit und umfassend Einsicht in alle seine eigenen Daten nehmen zu können.<sup>83</sup> Woher weiss ein Interessierter nun aber, welche Stelle welche Daten über ihn hat?

Dafür gibt es ein Verzeichnis – das Register der Datensammlungen aller Zuger Verwaltungsstellen. Dieses führt der DSB. Damit dieses Verzeichnis vollständig ist, sind sämtliche Verwaltungsstellen von Kanton und Gemeinden verpflichtet, ihre Datensammlungen dem DSB zu melden.<sup>84</sup>

Durch dieses Register wird gegenüber der Öffentlichkeit Transparenz geschaffen, und jedermann kann sich ein Bild machen, welche Daten bei welcher Verwaltungsstelle bearbeitet werden.

Dieses Verzeichnis ist somit die nötige Grundlage, damit jedermann Einsicht in seine eigenen Daten nehmen kann. Das Register selber enthält übrigens keinerlei Personendaten. Ersichtlich ist nur, unter welcher Bezeichnung eine Verwaltungsstelle eine Datensammlung führt und welche Art von Daten dort in welcher Form gesammelt wird.

Nützlich ist das Register aber auch für die Verwaltung selber. Die einzelnen Verwaltungsstellen erhalten einen Überblick über die bei ihnen vorhandenen Daten und über die Datenflüsse zwischen den Verwaltungsstellen.

Es bietet zudem den leitenden Gremien die Möglichkeit, kritisch zu überprüfen, ob die vorhandenen Datensammlungen inhaltlich in Ordnung und sachlich notwendig sind.

Wird im Kanton Zug das Öffentlichkeitsprinzip in den Verwaltungen eingeführt, wird das Register der Datensammlungen wertvolle Dienste leisten.

### Wer führt das Register?

Für die Führung des Registers der kantonalen Verwaltung ist der Datenschutzbeauftragte zuständig. Die Gemeinden haben ihr Register an und für sich selber zu führen.<sup>85</sup> Um die Einheitlichkeit des Registers zu gewährleisten, war der DSB bereits bei Projektbeginn im Jahr 2000 bereit, auch die Datensammlungen der Gemeinden<sup>86</sup> zu betreuen.

### 1492 Zuger Datensammlungen!

Das Register umfasste Ende 2011 insgesamt 1492 Zuger Datensammlungen [Abnahme aufgrund der Zusammenführung verschiedener Datensammlungen im Vergleich zum Vorjahr: -4]:

- kantonale Verwaltung: 304 [-6]
- externe Beauftragte: 24 [+2]
- Einwohnergemeinden: 897 [keine Änderung]
- Bürgergemeinden: 112 [keine Änderung]
- römisch-katholische Kirchgemeinden: 92 [keine Änderung]
- evangelisch-reformierte Kirchgemeinde: 12 [keine Änderung]
- Korporationsgemeinden: 51 [keine Änderung]

Der Datenschutzbeauftragte veröffentlicht dieses Register auf seiner Website. Es stehen sehr effiziente Suchhilfen zur Verfügung. Statistische Auswertungen zeigen, dass das Internet-Register bei Bevölkerung und Verwaltungsstellen auf Interesse stösst.

### Ausblick

Die Register-Software ist nun bereits seit über zehn Jahren unverändert in Betrieb. Softwaremässig handelt es sich beim Register somit um einen Methusalem. Da die Entwicklerfirma keinen Support mehr gewähren kann, die technische Entwicklung der Browser-Technologie in den letzten Jahren rasante Fortschritte gemacht hat und die bisherige Lösung zudem keinen barrierefreien Zugang erlaubte, musste im Berichtsjahr die Registersoftware vollständig erneuert werden. Die Neuentwicklung des Programms und die Übernahme des bestehenden Registers erfolgten per Ende des Berichtsjahres. Die Veröffentlichung ist für das erste Quartal 2012 vorgesehen.

83 § 13 und § 14 Datenschutzgesetz.

84 § 12 und § 26 Abs. 1 Datenschutzgesetz. Davon ausgenommen sind gemäss § 12 Abs. 2 Datenschutzgesetz die Hilfsdatensammlungen und Datensammlungen, die nur bis maximal sechs Monate geführt werden. Ebenfalls nicht in das Register aufgenommen werden Datensammlungen, die keine Personendaten, sondern ausschliesslich Sachdaten beinhalten.

85 § 12 Abs. 5 Datenschutzgesetz.

86 Einwohnergemeinden, Bürgergemeinden, Kirchgemeinden sowie Korporationsgemeinden.

## VI. Weiterbildung

### **Technische Massnahmen sind wichtig – Sensibilisierung der Mitarbeitenden ist ebenfalls wichtig**

Damit in der Verwaltung die Daten rechtmässig bearbeitet werden, sind Gesetze, Verordnungen und Weisungen wichtig. Daneben gewährleisten technische Massnahmen, dass die Datenbearbeitung in einem sicheren Rahmen abgewickelt wird. Zentral ist aber auch das richtige Verhalten der Mitarbeitenden. Sie müssen wissen, wie sie mit den Daten der Zugerinnen und Zuger umgehen müssen und insbesondere auch, an welche Stellen welche Daten wie weitergegeben werden dürfen. Hier bietet der DSB Unterstützung. Wir führen Schulungen und Weiterbildungen durch und versuchen insbesondere auch, die Mitarbeitenden der kantonalen und gemeindlichen Verwaltungen zu sensibilisieren.

### **Sensibilisierung der neuen Mitarbeitenden**

Alle neuen Mitarbeitenden der kantonalen Verwaltung werden automatisch zum Einführungstag «Die Zuger Verwaltung kennenlernen» eingeladen. Das Seminar soll den neuen Mitarbeitenden zeigen, wie die Zuger Verwaltung strukturiert ist und wie sie funktioniert. Der DSB bestreitet ein Modul. Dabei stellt er die Datenschutzstelle und deren Aufgaben kurz vor und erläutert die wichtigsten Aspekte des Datenschutzes und der Datensicherheit. Da nur eine Lektion zur Verfügung steht, kann es sich nicht um eine Schulung handeln. Trotzdem ist die gebotene Möglichkeit einer Präsentation im Rahmen dieses Seminars sehr wertvoll, werden die neuen Mitarbeitenden doch kurz informiert und sensibilisiert. Im Berichtsjahr fand der Einführungstag zweimal statt. Insgesamt lernten dabei über hundert Personen die Datenschutzstelle kennen.

### **Seminar für neue Gemeinderatsmitglieder**

Im Auftrag der Direktion des Innern führte das Institut für Betriebs- und Regionalökonomie der Hochschule für Wirtschaft/HSW Luzern ein zweitägiges Aus- und Weiterbildungsseminar für neue Zuger Gemeinderätinnen und Gemeinderäte durch. An dieser wichtigen und spannenden Schulung konnte der Datenschutzbeauftragte ein Schulungsmodul von zwei Lektionen übernehmen. Dabei informierte er über die Grund-

lagen des Datenschutzes und der Datensicherheit. Es gab auch genügend Raum, um wichtige Fragen mit den PolitikerInnen zu diskutieren.

### **Ein wichtiges Publikum – die angehenden Lehrpersonen**

Angehende Lehrpersonen für Datenschutz und Datensicherheit zu sensibilisieren ist aus zwei Gründen wichtig: Erstens verfügen Lehrpersonen über viele, teilweise sehr heikle Daten über die SchülerInnen, deren Umfeld und deren Elternhaus. Zweitens können sie ihrerseits bei der Lehrtätigkeit ihre Schülerinnen und Schüler im Umgang mit Daten sensibilisieren, ein Thema, das in den Zeiten von facebook & Co. immer wichtiger wird.

An der Pädagogischen Hochschule Zentralschweiz in Zug hat der DSB im Berichtsjahr gegen 90 StudienabgängerInnen im Rahmen von zwei Lektionen auf das Wichtigste im Datenschutz an der Schule hinweisen können – eine sehr wertvolle Informationsveranstaltung!

### **Kurs für Lehrpersonen**

Der korrekte Umgang mit Personendaten ist auch für langjährige Lehrpersonen ein wichtiges Thema. Die Pädagogische Hochschule Zentralschweiz in Zug bot deshalb in ihrem Weiterbildungsangebot 2011 für Lehrpersonen den Halbtageskurs «Datenschutz in der Schule – das müssen Sie wissen» an, den der Datenschutzbeauftragte durchführte. Die Teilnehmenden brachten viele Themen und Fragen mit, deren Beantwortung nicht nur für die Anwesenden, sondern grundsätzlich für alle Lehrpersonen, Schulhausleitungen und Rektorate von grossem Interesse wäre. Im Bereich Schule werden wir in Zukunft unsere Angebote verbreitern müssen.

### **Präsentationen des DSB**

Regelmässig laden Verwaltungsstellen des Kantons den DSB zu Referaten oder Präsentationen ein, um ihre Mitarbeitenden über Datenschutz oder Datensicherheit zu informieren.

Im Herbst ergab sich etwa die Gelegenheit, an einer Veranstaltung des Datenschutz-Forums in Zürich datenschutzrechtliche Überlegungen zum Thema «Internetpranger» zu präsentieren.<sup>87</sup>

<sup>87</sup> Näheres dazu unter «[www.datenschutz-forum.ch](http://www.datenschutz-forum.ch)» und in der Berichterstattung der Neuen Zürcher Zeitung vom 22. September 2011 S. 18.

## VII. Zusammenarbeit der Datenschutzbeauftragten

### «privatim»

Seit 2006 sind die Datenschutzbehörden aller 26 Kantone<sup>88</sup> im Verein «privatim – Die schweizerischen Datenschutzbeauftragten» zusammengeschlossen.<sup>89</sup> Wichtige Themen, die alle Kantone betreffen, werden gemeinsam, somit effizienter und effektiver, bearbeitet. Ein grosser Teil der Arbeit wird von Arbeitsgruppen geleistet.<sup>90</sup>

«privatim» ist auch Ansprechpartner der Medien. Im Berichtsjahr stand hier das Thema Gesundheit – Stichworte: «SwissDRG» und Spitallisten – im Mittelpunkt.

«privatim» nimmt im Namen der kantonalen Datenschutzstellen jeweils auch zu wichtigen bundesrechtlichen Vernehmlassungsvorlagen Stellung.

### Konferenzen von «privatim»

Am 10./11. Mai 2011 fand die Frühjahrestagung in Vaduz statt. In den Kantonen sind die Datenschutzstellen sehr unterschiedlich strukturiert und organisiert. Das Plenum setzte sich deshalb vertieft mit der Rolle und dem Rollenverständnis der Datenschutzbeauftragten auseinander.

Die Herbstkonferenz fand am 15. November 2011 in Bern statt. Schwerpunkt war das aktuelle Thema Personenidentifikatoren und Authentifizierungsverfahren im E-Government.

### Zusammenarbeit mit dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten

Die Zusammenarbeit mit dem EDÖB erfolgt fall- und anlassbezogen. Im Bereich Schengen sieht das Bundesrecht jedoch ausdrücklich vor,<sup>91</sup> dass der EDÖB und die kantonalen DSB bezüglich der Aufsicht über die Datenbearbeitung bei der Polizei «aktiv» zusammenarbeiten. Dafür wurde im Jahr 2009 die «Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Umsetzung des Schengen-Assoziierungsabkommens» [SDSB] gegründet. Diese Kooperation mit dem EDÖB ist wichtig, da dieser über Know-how, Erfahrung und Ressourcen bezüglich Kontrollen im Rahmen von Schengen verfügt.

### Internationale Zusammenarbeit

#### Ausgangslage

Das Schengen-Recht sieht eine verstärkte Zusammenarbeit der Datenschutzbehörden auf europäischer Ebene vor, und zwar auf nationaler wie auch auf «subnationaler»<sup>92</sup>. Im Rahmen der DSGVO-Revision von 2008 wurde daher die Möglichkeit der Zusammenarbeit zwischen dem Zuger DSB und den Datenschutzbehörden des Auslandes explizit in das Zuger Datenschutzgesetz eingefügt.<sup>93</sup>

#### Interkantonale Begleitorganisation Schengen

Der DSB ist Mitglied der «Arbeitsgruppe Datenschutz» der interkantonalen Begleitorganisation Schengen/Dublin, die im Auftrag der Konferenz der Kantonsregierungen/KdK dieses Thema verfolgt.

#### «Virtuelles Datenschutzbüro»

Seit 2008 ist der Zuger DSB Projektpartner des «Virtuellen Datenschutzbüros». Dieses betreibt im deutschsprachigen Raum eine Internet-Plattform zu Datenschutz und Informationssicherheit. Die Projektpartner sind berechtigt, Informationen auf der Plattform zu veröffentlichen. Zudem wird die Zusammenarbeit unter den deutschsprachigen Datenschutzstellen verstärkt.

#### Konferenz der europäischen Datenschutzbeauftragten

Diese fand am 6. April 2011 auf Einladung des Europäischen Datenschutzbeauftragten und des Präsidenten der «Working Party 29/Art. 29 Arbeitsgruppe» in Brüssel statt. Vertreten waren alle europäischen Datenschutzstellen, die Europäische Kommission, der Rat der Europäischen Union, das Europäische Parlament und der Europarat.

[Hinweis: An dieser Konferenz hat der DSB in seiner Freizeit teilgenommen; für Kosten und Spesen kam er selber auf.]

88 Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte ist nicht Mitglied von «privatim» [vgl. dazu DSB TB 2006 S. 28].

89 Alles Nähere zu «privatim» findet sich auf deren Homepage: «www.privatim.ch».

90 Folgende Arbeitsgruppen sind zurzeit aktiv: «AG Gesundheit», «AG innere Sicherheit» und «AG Information/Communication Technology [ICT]».

91 Art. 54 der Verordnung über den nationalen Teil des Schengener Informationssystems [N-SIS] und das SIRENE-Büro vom 7. Mai 2008 [N-SIS-Verordnung, SR 362.0].

92 Betrifft in der Schweiz die kantonalen Datenschutzbeauftragten, in Deutschland die Landesbeauftragten für den Datenschutz und in Spanien diejenigen der autonomen Regionen.

93 Art. 19 Abs. 1 Bst. k Datenschutzgesetz.

## VIII. Wir über uns

### Pensen

Im Berichtsjahr betrug das Arbeitspensum von René Huber [Datenschutzbeauftragter] 100%. Seit dem 1. März 2011 ist Fürsprecherin Christine Andres mit einem Pensum von 80% als juristische Mitarbeiterin tätig. Seit August 2011 bietet die Datenschutzstelle ausgebildeten JuristInnen, die das Rechtsanwaltspatent erwerben möchten, die Möglichkeit, ein zeitlich befristetes juristisches Praktikum zu absolvieren. Bis im September war diese Stelle kurz durch eine Juristin in Teilzeit besetzt, seit dem 1. Dezember 2011 macht lic. iur. Armando Hammer mit einem Pensum von 100% ein halbjähriges juristisches Praktikum bei der Datenschutzstelle.

Das Sekretariat der Datenschutzstelle wird von Hildegard Steiner von der Staatskanzlei betreut.

### Unser Aufwand für die verschiedenen Aufgaben

In der untenstehenden Übersicht sehen Sie, wie viel Arbeitszeit wir für die verschiedenen Tätigkeiten in etwa aufgewendet haben. Wir sind der

Ansicht, dass eine solche Statistik aussagekräftiger ist, als Angaben über die Anzahl der geführten Telefongespräche oder der behandelten Anfragen, lässt sich doch eine einfache Anfrage innerhalb von einer Stunde erledigen, ein komplexes Projekt kann dagegen einen Aufwand von vielen Arbeitstagen erfordern.

Ein Hinweis zur Rubrik «Beratung der Zuger Einwohnerinnen und Einwohner»: Ein Teil der Privaten wendet sich direkt an uns [in der Tabelle mit «Private direkt» bezeichnet], andere lösen bei der gemeindlichen oder kantonalen Verwaltung eine Anfrage dieser Stellen beim DSB aus, so dass sich insgesamt etwas weniger als die Hälfte unserer Arbeitszeit direkt mit Interventionen aus der Bevölkerung befasst.

Alle unsere Tätigkeiten sind – direkt oder indirekt – Dienstleistungen für die Zuger Bevölkerung.

Bereich	2011	[2010]	[2009]	Hinweise
<b>Beratung der Zuger Einwohnerinnen und Einwohner</b>	44%	[39%]	[45%]	Erstkontakt mit: kantonaler Verwaltung 31% [25%] [28%] Gemeinde 5% [6%] [8%] Private direkt 8% [8%] [9%]
<b>Ausbildungsangebote</b>	4%	[4%]	[4%]	Schulungen, Referate und Präsentationen für kantonale oder gemeindliche Verwaltungen
<b>Betreuung grösserer Projekte</b>	13%	[10%]	[8%]	Register der Datensammlungen, Gesetzgebung, Tätigkeitsbericht, Rechenschaftsbericht und Beitrag GVP
<b>Datensicherheit</b>	2%	[3%]	[4%]	Beratung kantonaler und gemeindlicher Verwaltungen
<b>Schengen/Dublin</b>	4%	[7%]	[7%]	Berichterstattungen, Kontrolle, Vorarbeiten zur Revision des Datenschutzgesetzes
<b>Öffentlichkeitsarbeit</b>	6%	[8%]	[8%]	Medienarbeit, Fachbeiträge, Homepage, Newsletter
<b>Zusammenarbeit mit EDÖB und kantonalen DSB</b>	3%	[2%]	[2%]	Informationsaustausch, Teilnahme an den Veranstaltungen des CH-DSB-Vereins «privatim»
<b>Weiterbildung</b>	3%	[3%]	[3%]	Tagungsbesuche [insbesondere im IT-Bereich]
<b>Diverses</b>	21%	[24%]	[19%]	Korrespondenz, Rechnungswesen, Personelles, Betreuung der eigenen IT-Infrastruktur, Bibliothek, Besprechungen – alles soweit nicht direkt einzelnen Projekten zuweisbar
<b>Total</b>	100%	[100%]	[100%]	

# Dank

Die Privatsphäre der Zugerinnen und Zuger wird grundsätzlich nicht durch den Datenschutzbeauftragten geschützt. Verantwortlich dafür sind vielmehr Politik und Verwaltung – und nicht zuletzt jede einzelne Mitarbeiterin, jeder einzelne Mitarbeiter in der kantonalen oder der gemeindlichen Verwaltung. Denn letztlich liegt es an den Mitarbeitenden, dass sie mit den Daten der Zuger Bevölkerung bei ihrer Arbeit in jeder Beziehung rechtmässig und korrekt umgehen. Der Datenschutzbeauftragte unterstützt sie dabei gerne mit seinen Dienstleistungen.

Ich bedanke mich deshalb gerne bei

*allen Mitarbeitenden kantonalen und gemeindlicher Verwaltungen* aller Stufen, mit denen ich im Jahr 2011 zusammenarbeiten durfte, um konstruktive, gute und rechtmässige Lösungen zu erarbeiten;

*allen kritischen Geistern*, die uns durch konstruktive Kritik und wertvolle Hinweise angespornt haben, unsere Dienstleistungen in Sachen Privatsphäre zugunsten der Zuger Bevölkerung weiter zu verbessern;

*den lieben Kolleginnen und Kollegen der Staatskanzlei*, für ihre tatkräftige und wichtige Unterstützung in den administrativen Belangen;

*Hildegard Steiner* für die administrative und den Mitarbeiterinnen der Telefonzentrale für die «telefonische» Unterstützung;

*meiner juristischen Mitarbeiterin Christine Andres* für ihren tatkräftigen, kompetenten und engagierten Einsatz;

*Landschreiber Tino Jorio*, der bis Ende September 2011 seines Amtes waltete. Bei ihm möchte ich mich ganz speziell und herzlich bedanken, hat er doch in den letzten zwölf Jahren durch seine Unterstützung, sein Mitdenken, seine scharfsinnigen, aber auch kritischen Gedanken viel zur Institution Datenschutzstelle beigetragen. Ich wünsche ihm an dieser Stelle ganz herzlich und freundschaftlich alles Gute;

*Landschreiber Tobias Moser*, der seit Oktober 2011 im Amt ist und der sich freundlicherweise bereit erklärt hat, diese Tradition des Gedankenaustausches weiterzuführen.

René Huber

# Sachregister

A	Seite	P	Seite
Adressauskunft	18	Personaldossier	10
Auslagern	15	Personalziitig [Beitrag des DSB]	21
<b>B</b>		Polizeigesetz [Revision]	24
Beauftragen von Privaten	15	«privatim»	29
<b>D</b>		<b>R</b>	
Datenschutzgesetz [Revision]	23	Register der Datensammlungen	27
Datenschutzstelle [«Wir über uns»]	30	<b>S</b>	
Datensicherheit [Rolle des DSB]	7	Schule und Datenschutz	13
<b>E</b>		Schulinfo Zug [Beitrag des DSB]	21
EDÖB [Zusammenarbeit]	29	Schulpsychologischer Dienst	13
E-Learning «Datensicherheit»	8	sexuelle Belästigung am Arbeitsplatz	12
E-Mail und Ferienabwesenheit	10	social media	4
<b>F</b>		soziale Netzwerke	4
facebook & Co.	4	Spital	5
Finanzkontrolle [überprüft DSB]	6	Steuerbehörden [Datenbekanntgabe an ~]	17
Fotokopierer	7	Strassenverkehrsamt	17
<b>G</b>		<b>T</b>	
Geoinformationsgesetz	25	Tätigkeitsbericht des DSB	20
Gesetzgebung [Input des DSB]	22	<b>V</b>	
GVP [Beitrag des DSB]	20	verdeckte polizeiliche Vorermittlung	24
<b>I</b>		Vergessen [Recht auf ~]	2
IT-Security	7	Verkehrserhebung	15
<b>K</b>		Vernehmlassungen	22
Kantonsrat [Informationen des DSB an ~]	4	Videoüberwachung am Bahnhof	14
Kantonsratsgeschäfte im Internet	16	Videoüberwachungsgesetz	25
Kindeswohlgefährdung und Datenbekanntgabe	18	<b>W</b>	
<b>M</b>		Wahl- und Abstimmungsgeheimnis	17
«Moskito» und Datenschutz	14	Website des DSB	19
<b>N</b>		Weiterbildungsangebote des DSB	28
Newsletter des DSB	19	Weiterbildungskonzept [WBK]	6
<b>O</b>		Whistleblowing	12
Outlook-Kalender	11	<b>Z</b>	
Outsourcen	15	Zuständigkeit des DSB	10

# Nützliche Adressen

## Datenschutzstelle des Kantons Zug

Regierungsgebäude  
Seestrasse 2  
Postfach 156  
6301 Zug  
Tel. 041 728 31 87  
Fax 041 728 37 01  
[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)

Dr. iur. René Huber  
[Datenschutzbeauftragter]  
Tel. 041 728 31 87  
[direkt Huber]

Fürsprecherin Christine Andres  
[juristische Mitarbeiterin]  
Tel. 041 728 31 25  
[direkt Andres]

Sekretariat  
Tel. 041 728 31 47  
Fax 041 728 37 01  
[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)

## Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Feldegweg 1  
Postfach  
3003 Bern  
Tel. 031 322 43 95  
[www.edoeb.admin.ch](http://www.edoeb.admin.ch)

## Kantonale Verwaltung

Tel. 041 728 33 11  
[Zentrale]

## Gemeindeverwaltungen

Baar  
Rathausstrasse 2  
Postfach  
6341 Baar  
Tel. 041 769 01 20  
Fax 041 769 01 91  
[www.baar.ch](http://www.baar.ch)

Cham  
Mandelhof  
Postfach 265  
6330 Cham  
Tel. 041 723 87 03  
Fax 041 723 87 02  
[www.cham.ch](http://www.cham.ch)

Hünenberg  
Chamerstrasse 11  
Postfach 261  
6331 Hünenberg  
Tel. 041 784 44 44  
Fax 041 784 44 99  
[www.huenenberg.ch](http://www.huenenberg.ch)

Menzingen  
Alte Landstrasse 2A  
Postfach 99  
6313 Menzingen  
Tel. 041 757 22 22  
Fax 041 757 22 20  
[www.menzingen.ch](http://www.menzingen.ch)

Neuheim  
Dorfplatz 5  
Postfach 161  
6345 Neuheim  
Tel. 041 757 21 30  
Fax 041 757 21 40  
[www.neuheim.ch](http://www.neuheim.ch)

Oberägeri  
Alosenstrasse 2  
Postfach 159  
6315 Oberägeri  
Tel. 041 723 80 25  
Fax 041 723 80 01  
[www.oberaegeri.ch](http://www.oberaegeri.ch)

Risch  
Zentrum Dorfmatte  
6343 Rotkreuz  
Tel. 041 798 18 18  
Fax 041 798 18 88  
[www.rischrotkreuz.ch](http://www.rischrotkreuz.ch)

Steinhausen  
Bahnhofstrasse 3  
Postfach 164  
6312 Steinhausen  
Tel. 041 748 11 11  
Fax 041 748 11 00  
[www.steinhausen.ch](http://www.steinhausen.ch)

Unterägeri  
Seestrasse 2  
Postfach 79  
6314 Unterägeri  
Tel. 041 754 55 00  
Fax 041 754 55 55  
[www.unteraegeri.ch](http://www.unteraegeri.ch)

Walchwil  
Dorfstrasse 4  
Postfach 93  
6318 Walchwil  
Tel. 041 759 80 10  
Fax 041 759 80 07  
[www.walchwil.ch](http://www.walchwil.ch)

Zug  
Stadthaus am Kolinplatz  
Postfach 1258  
6301 Zug  
Tel. 041 728 21 04  
Fax 041 728 23 71  
[www.stadtzug.ch](http://www.stadtzug.ch)

[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)

**Datenschutzstelle des Kantons Zug**  
Regierungsgebäude, Seestrasse 2  
Postfach 156, 6301 Zug  
Tel. 041 728 31 47, Fax 041 728 37 01  
[www.datenschutz-zug.ch](http://www.datenschutz-zug.ch)

**Gestaltung:** Christen Visuelle Gestaltung, Zug  
**Auflage:** 1500 Exemplare  
**Druck:** Multicolor Print AG, Baar  
**Papier:** Refutura Recycling, 100% Altpapier, CO<sub>2</sub>-neutral, FSC