



Datenschutzbeauftragter
des Kantons Zug

Tätigkeitsbericht 2005 [Nr. 7]

Datenschutzbeauftragter des Kantons Zug

Tätigkeitsbericht 2005 [Nr. 7]

Der Datenschutzbeauftragte hat dem Regierungsrat jährlich einen Bericht über seine Tätigkeit zu erstatten.¹

Der vorliegende Tätigkeitsbericht Nr. 7 deckt den Zeitraum zwischen 1. Januar 2005 und 31. Dezember 2005 ab.

Er ist auch auf der Website des Datenschutzbeauftragten veröffentlicht:
«www.datenschutz-zug.ch»

Zug, 18. Januar 2006

Datenschutzbeauftragter des Kantons Zug
Dr. iur. René Huber

Ein paar häufig verwendete Abkürzungen:

| | |
|-------|--|
| Abs. | Absatz |
| BBl | Bundesblatt |
| BGS | Bereinigte Gesetzes- sammlung [Kt. Zug] |
| Bst. | Buchstabe |
| DS | Datenschutz |
| DSB | Datenschutzbeauftragter |
| DSG | Datenschutzgesetz |
| EDSB | Eidg. Datenschutz- beauftragter |
| E-DSG | Eidg. Datenschutzgesetz |
| GVP | Gerichts- und Verwaltungs- praxis des Kantons Zug |
| IT | Informatik-, Informations- technologie |
| SR | Systematische Sammlung des Bundesrechts |
| TB | Tätigkeitsbericht |

¹ § 19 Abs. 1 Bst. h Datenschutz-
gesetz des Kantons Zug.

² Eidg. Datenschutzbeauftragter,
Feldeggweg 1, 3003 Bern,
Tel. 031 322 43 95,
«www.edsb.ch».

Ein wichtiger Hinweis

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

Für die Datenbearbeitung von privaten Unternehmen [Versicherern, Banken, Arbeitgebern etc.] sowie der Bundesverwaltung ist der Eidg. Datenschutzbeauftragte² zuständig.

ISSN 1424-4756

Inhaltsverzeichnis

| | |
|----|---|
| 2 | Soll uns die Technik regieren? |
| 3 | Sind Sie in Eile? – Hier das Wichtigste des Jahres 2005 |
| | I. Grundlegende Themen und Projekte |
| 4 | 1. Die Pendenzen aus dem Jahre 2004 |
| 4 | 2. «Schengen/Dublin» |
| 5 | 3. Leistungsvereinbarungen mit privaten Dritten |
| 6 | 4. Datensicherheit in der kantonalen Informatik |
| | II. Berichterstattung 2005 |
| 8 | 1. Fälle aus der Beratungspraxis |
| 8 | 1.1 Übersicht: Die Fälle auf einen Blick |
| 9 | 1.2 Recht auf Einsicht in die eigenen Daten |
| 9 | 1.3 Arbeitsrechtliches |
| 10 | 1.4 Schule |
| 13 | 1.5 Sicherheit und Polizei |
| 14 | 1.6 Forschung |
| 15 | 1.7 Informatik und Datensicherheit |
| 15 | 1.8 Einwohnergemeinde |
| 17 | 1.9 Bürgergemeinde |
| 17 | 1.10 Kirchgemeinde |
| 19 | 2. Unsere Öffentlichkeitsarbeit |
| 19 | 2.1 Zuger Datenschutz im Internet |
| 19 | 2.2 Elektronischer Newsletter des Datenschutzbeauftragten |
| 20 | 2.3 Tätigkeitsbericht 2004 |
| 20 | 2.4 «Gerichts- und Verwaltungspraxis des Kantons Zug» |
| 20 | 2.5 Medienarbeit |
| 21 | 3. Mitarbeit bei der Gesetzgebung |
| 21 | 3.1 Datenschutzgesetz |
| 21 | 3.2 Datensicherheits- und Online-Verordnung |
| 21 | 3.3 Polizeigesetz |
| 21 | 3.4 Vernehmlassungen |
| 23 | 4. Register der Datensammlungen |
| 24 | 5. Weiterbildung |
| 24 | 5.1 Unser Weiterbildungsangebot |
| 24 | 5.2 Auch der Datenschutzbeauftragte muss sich weiterbilden |
| 26 | 6. Zusammenarbeit mit dem Eidgenössischen und mit den kantonalen Datenschutzbeauftragten |
| 27 | 7. Wir über uns |
| 28 | Dank! |
| 29 | Sachregister |

Soll uns die Technik regieren?

Sehr geehrte Leserin
Sehr geehrter Leser

Möchten Sie eine viel günstigere Haftpflichtversicherung für Ihr Auto? Nicht einfach gleich viel bezahlen wie alle anderen, sondern eine Prämie bezahlen, die aufgrund Ihrer «effektiven Nutzung» berechnet wird? Die «effektive Nutzung» der Versicherung liesse sich technisch durchaus ermitteln: Man könnte in Ihr Auto ein kleines Gerät einbauen, das der Versicherungsgesellschaft automatisch übermittelt, wann Sie mit welcher Geschwindigkeit auf welchen Strassen unterwegs sind. Wie bei der Telefonabrechnung erhielten Sie dann monatlich eine Abrechnung Ihrer Prämie. Diese berechnete sich aufgrund Ihrer Fahrten. Sie könnten ohne weiteres nachvollziehen, dass Sie für eine Fahrt von Zug nach Luzern an einem schönen Augusttag auf der Autobahn bei einer Geschwindigkeit von 110 km/h eine um Faktoren günstigere Prämie bezahlen würden als für eine rasante Fahrt um zwei Uhr nachts an einem Samstag im Januar auf der schneebedeckten Strasse von Zug nach Oberägeri.

Alles Utopie? Technisch gar nicht machbar? Nicht in Grossbritannien. Seit Herbst 2005 bietet die Versicherungsgesellschaft «Norwich Union» die «massgeschneiderte» Haftpflichtversicherung an.³ Der Kunde lässt sich durch die Versicherungsgesellschaft einen GPS-Sender etwa in der Grösse einer Zigarettenschachtel in seinen Wagen einbauen. Dadurch werden dem Versicherer minutiös und dauernd sämtliche Informationen über das Fahrverhalten des Autos übermittelt.⁴ Als Gegenleistung erhalten die Kunden eine günstigere Grundprämie und monatlich eine Aufstellung sämtlicher getätigter Fahrten und deren Versicherungskosten pro Fahrt. Bis Ende 2005 liessen sich bereits mehr als 20'000 Kunden solche Geräte einbauen. Ob sie die Sache zu Ende gedacht haben, steht aber auf einem anderen Blatt.

Denn dieses Konzept, das so verführerisch daherkommt, hat natürlich seinen Preis. Wollen Sie denn, dass der Versicherer zu jedem

Zeitpunkt Bescheid weiss, wie und wo Sie unterwegs sind, somit «Big Brother» in Ihrem Auto mitfährt?

Wissen Sie denn, was mit diesen Daten genau geschieht: Wo sie gespeichert werden? Wie lange? Wer alles Einsicht nimmt? Wozu? An welche Firmen und Stellen sie weiter gegeben werden? Man muss kein Hellseher sein – absehbar ist die Nutzung Ihrer Daten in zwei Richtungen. Erstens wird sie der *Versicherer* selber im Schadenfall gegen Sie verwenden. Sie können ein noch so anständiges Fahrverhalten haben, bei einer entsprechend ausgeklügelten Analyse all Ihrer Fahrdaten haben Sie schlechte Karten.

Zweitens wird sich bald auch der *Staat* für Ihre Daten interessieren. Denken Sie etwa an Polizei, Nachrichtendienste, Strassenverkehrsämter, an Sozial- und Steuerbehörden. Aber auch Ihr Arbeitgeber könnte an solchen Daten durchaus ein Interesse haben.

Sie sehen: Die Sache ist etwas komplizierter, als sich ein kleines Gerät einbauen zu lassen, um dann weniger Prämien zu zahlen.

Hier – wie auch in anderen Bereichen⁵ – stellt die Technik Instrumente zur Verfügung, die unabsehbare Auswirkungen auf unsere Privatsphäre und damit auf unsere Lebensgestaltung haben.

Lassen wir uns von der Technik vorgeben, welche Privatsphäre uns zusteht? Wohl besser nicht. Die Privatsphäre ist die Grundlage eines freiheitlichen demokratischen Rechtsstaates und somit auch die Grundlage einer freiheitlichen Lebensführung. Hier darf nicht die Technik entscheiden. Hier sind wir alle aufgefordert, sorgfältig zu prüfen und zu entscheiden, über welche Freiheiten wir verfügen und in welcher Gesellschaft wir leben wollen.

Haben Sie Fragen oder Anregungen? Der Datenschutzbeauftragte steht Ihnen in Sachen Datenschutz und Datensicherheit jederzeit gerne zur Verfügung.



Dr. iur. René Huber
Datenschutzbeauftragter des Kantons Zug

3 Versicherungsmodell «Pay-as-you-drive» des Haftpflichtversicherers Norwich Union. Näheres unter: «www.norwichunion.com». Medienberichterstattungen dazu sind zu finden unter: «www.bbc.co.uk».

4 Registriert werden Zeit/Datum, Geschwindigkeit sowie jederzeit die räumliche Lokalisierung auf wenige Meter genau. Der Betreiber der Infrastruktur verfügt über geografische und meteorologische Datenbanksysteme. Dadurch kann insbesondere jederzeit auch ermittelt werden, welche Strasse/Strassenart befahren wird (Autobahn, Landstrasse oder Quartierstrasse). Offenbar sind zurzeit noch nicht sämtliche Strassen Grossbritanniens im System erfasst. Sobald dies der Fall ist, kann der Versicherer ohne weiteres auch die Einhaltung der gesetzlich vorgeschriebenen Geschwindigkeit überprüfen.

5 Etwa im Gesundheitsbereich betreffend Gesundheitskarte oder im Konsumbereich bezüglich der RFID-Technologie [s. dazu Näheres DSB TB 2004 S. 31 Fussnote 142].

Sind Sie in Eile? – Hier das Wichtigste des Jahres 2005

Beratung: 27 Fälle aus der Praxis

Anhand von 27 konkreten Beispielen erhalten Sie einen Einblick in unsere Beratungspraxis des Jahres 2005. Eine Übersichtstabelle erleichtert Ihnen dabei den Einstieg.

Näheres → S. 8

Register der Datensammlungen: 1'328 Datensammlungen erfasst

Das Register umfasst die Datensammlungen der kantonalen Verwaltung, aller Gemeinden und von Privaten, die öffentliche Aufgaben erfüllen. Zurzeit sind 1'328 Datensammlungen registriert. Das Register steht Ihnen im Internet zur Verfügung. Diese Dienstleistung im Internet wird rege genutzt.

Näheres → S. 23

«Schengen/Dublin» und der Datenschutzbeauftragte

Voraussichtlich wird die Umsetzung dieser Abkommen grosse Auswirkungen auf Organisation, Befugnisse und Ressourcen der Datenschutzstelle haben.

Näheres → S. 4

Datensicherheit: Noch immer fehlen die Ausführungsbestimmungen

Der Regierungsrat hätte bis Ende 2001 die Datensicherheitsverordnung und die Online-Verordnung erlassen müssen. Beides ist noch immer nicht erfolgt.

Näheres → S. 7

Internet-Angebot und elektronischer Newsletter des Datenschutzbeauftragten

Der DSB informiert in seinem elektronischen Newsletter über Aktuelles aus Datenschutz und Datensicherheit in Kurzform kostenlos per E-Mail. Damit entfällt zeitaufwändiges Ab-suchen der DSB-Website auf Neuigkeiten. Die Nutzung unseres Internet-Angebots ist im Berichtsjahr leicht gestiegen, das Herunterladen von Dokumenten hat um etwa 40% zugenommen. Die Nutzung des Archivs des Newsletters hat sich gar verdoppelt.

Näheres → S. 19

Internationale Konferenzen

Der DSB nahm an zwei wichtigen internationalen Veranstaltungen teil. In diesem Abschnitt erfahren Sie, was in Sachen Datenschutz und Datensicherheit weltweit aktuell ist.

[Hinweis: An den Konferenzen, die im Ausland stattfinden, nimmt der DSB jeweils in seiner Freizeit teil und kommt für Kosten und Spesen vollumfänglich selber auf.]

Näheres → S. 25

Die sechs Pendenzen aus dem Jahre 2004: Wie ging die Geschichte aus?

Nicht alle Geschäfte können im Berichtsjahr abgeschlossen werden. Hier erfahren Sie, ob die sieben Geschäfte, die im letzten Tätigkeitsbericht noch offen waren, nun erledigt sind.

Näheres → S. 4

I. Grundlegende Themen und Projekte

1. Die Pendenzen aus dem Jahre 2004: Wie ging die Geschichte aus?

Im letztjährigen Tätigkeitsbericht haben wir Ihnen bei verschiedenen Themen versprochen, Sie über den Abschluss oder die weitere Entwicklung zu informieren. Bei einem Teil dieser Geschäfte war der DSB in Pflicht genommen, bei einem Teil andere Verwaltungsstellen.

Über Folgendes gilt es zu berichten:

- **Hat der Regierungsrat nun die Datensicherheitsverordnung verabschiedet?**⁶
Nein – Informationen dazu finden Sie auf S. 7.
- **Hat der Regierungsrat unterdessen die Online-Verordnung verabschiedet?**⁷
Nein – Informationen dazu finden Sie auf S. 7.
- **Wie ging es mit der Änderung des Datenschutzgesetzes bezüglich der Sammelauskünfte weiter?**⁸
Der Kantonsrat hat die Vorlage in erster Lesung beraten. Näheres dazu finden Sie hinten auf S. 21.
- **Wie weit ist das neue Polizeigesetz?**⁹
Die Sicherheitsdirektion hat die Vernehmlassung durchgeführt. Der Regierungsrat plant, die Vorlage im Jahr 2006 dem Kantonsrat zuzustellen. Informationen dazu finden Sie auf S. 21.

- **Hat der DSB nun sämtliche Zuger Datensammlungen im Register erfasst?**¹⁰
Noch nicht ganz. Mehr dazu auf S. 23.
- **Leistungsvereinbarungen mit Dritten – sind die offenen Fragen nun geklärt?**¹¹
Die im Jahr 2004 festgestellten Differenzen wurden entschieden, jedoch nicht im Sinne des Datenschutzes. Siehe dazu auf S. 6.

- **Internationale Konferenz der Datenschutzbeauftragten in Montreux**¹²
Die Konferenz fand im September statt. Der DSB hat ein Panel organisiert und geleitet. Näheres dazu hinten auf S. 26.

2. «Schengen/Dublin»

Ausgangslage

In der Volksabstimmung vom 5. Juni 2005 wurde «Schengen/Dublin» angenommen.¹³ Dieses Abkommen hat einen sehr direkten und bedeutenden Zusammenhang zum Thema Datenschutz, geht es dabei doch im Wesentlichen um den Datenaustausch zwischen der Schweiz und den Schengen-Staaten im Bereich Polizei und Justiz. Da es hier somit um die Bekanntgabe von sehr heiklen Daten ins Ausland geht, sind – im Sinne eines Ausgleichs – verschiedene Mechanismen zum Schutze von Betroffenen vorgesehen. Es erstaunt deshalb nicht, dass in der Botschaft des Bundesrates zu diesem Abkommen das Wort «Datenschutz» nicht weniger als 233-mal vorkommt.

Die Polizeihochheit in der Schweiz liegt grundsätzlich bei den Kantonen. Die Bearbeitung von Daten durch die kantonale Polizei untersteht der Aufsicht und Kontrolle der kantonalen Datenschutzbeauftragten. Weil die mit der Durchführung befassten Sicherheitsbehörden sehr weit reichende Kompetenzen bezüglich Datenweitergaben zwischen den Schengen-Staaten erhalten, sehen die Abkommen – zum Schutze der Betroffenen – vor, dass diese polizeilichen Datenbearbeitungen zumindest durch *vollständig unabhängige Kontrollinstanzen* [= Datenschutzbeauftragte] mit entsprechend *wirksamen Befugnissen* und den *erforderlichen Ressourcen* ausgestattet, beaufsichtigt und überprüft werden können.

Welche Folgen hat Schengen somit auf die Zuger Datenschutzstelle?

Hier kann schon zum heutigen Zeitpunkt festgestellt werden, dass die Zuger Datenschutzstelle den Anforderungen der Abkommen *nicht* entspricht. Einerseits verfügt der DSB nicht über die erforderlichen *wirksamen Befugnisse*, andererseits sind die Vorgaben bezüglich der *Unabhängigkeit des DSB* nicht gegeben.

Zu den «wirksamen Einwirkungsbefugnissen»: Der DSB muss neu die Möglichkeit haben, die Sperrung oder Vernichtung von Daten sowie das Verbot einer Verarbeitung verbindlich anordnen zu können. Zudem muss er Verwarnungen/Ermahnungen gegenüber den datenbearbeitenden Stellen aussprechen können und

6 DSB TB 2004 S. 6.

7 DSB TB 2003 S. 7.

8 DSB TB 2006 S. 26 f.

9 DSB TB 2004 S. 27.

10 DSB TB 2004 S. 29.

11 DSB TB 2004 S. 6.

12 DSB TB 2004 S. 32.

13 Etwas genauer: Annahme des «Bundesbeschlusses vom 17. Dezember 2004 über die Genehmigung und die Umsetzung der bilateralen Abkommen zwischen der Schweiz und der EU über die Assoziierung an Schengen und an Dublin» [BBl 2004 7149; Botschaft in BBl 2004 5965].

ein Klagerecht bzw. eine Anzeigebefugnis haben. Somit muss er bei Uneinigkeit mit den Verwaltungsstellen den Rechtsweg beschreiten können.

Zur Unabhängigkeit: Gemäss geltendem Zuger Datenschutzgesetz stellt der Regierungsrat – als oberstes Verwaltungsorgan – den DSB mit einem kündbaren Arbeitsvertrag an. Aufgrund der neuen Vorgaben darf der Kontrollierte, somit die Verwaltung, grundsätzlich aber nicht ihr eigenes Kontrollorgan bestimmen. Da der DSB bis anhin bloss Empfehlungen abgeben konnte, ihm jedoch keine wirksamen Rechtsbehelfe zustanden, war die alleinige Wahl durch die Exekutive nicht weiter problematisch. Voraussichtlich muss der DSB zukünftig auf eine *feste Amtsdauer* gewählt werden, seine *administrative Zuordnung* wird *unabhängiger* auszugestaltet sein und die für die neuen Arbeitsgebiete *erforderlichen Ressourcen* müssen zur Verfügung gestellt werden.

Wie geht es weiter – was ist zu tun?

Damit nun nicht jeder Kanton bei der datenschutzrechtlichen Umsetzung der Vorgaben von Schengen das Rad selbst erfinden muss, hat die «Konferenz der Kantonsregierungen»/KdK Ende 2005 einen externen Experten beauftragt, ihr bis im März 2006 in einem Bericht aufzuzeigen, wie eine Schengen-konforme Datenschutzaufsicht zu organisieren ist. Die KdK wird darauf gestützt voraussichtlich eine Empfehlung zuhanden der Kantone abgeben. Anschliessend ist es Sache jedes einzelnen Kantons, seine Gesetzgebung entsprechend anzupassen. Die Schweiz kann übrigens bei Schengen erst mitmachen, wenn die Schengen-Konformität von Bund und Kantonen durch die jetzigen Schengen-Staaten vor Ort überprüft und bestätigt wurde. Der Bund wird deshalb vermutlich ein nicht geringes Interesse haben, dass die Kantone hier die erforderlichen Gesetzesanpassungen innerhalb nützlicher Frist vornehmen.

DSB Zug als Vertreter der kantonalen Datenschutzstellen

Zur Umsetzung, Begleitung und Weiterentwicklung des Schengen-Rechts wurde in der Schweiz eine ganze Reihe von Arbeitsgruppen geschaffen. Sie setzen sich, je nach Fachgebiet, zusammen aus Vertretern des Bundes, kantonaler

Regierungen und auch kantonaler Fachspezialisten. René Huber wurde im Berichtsjahr von der KdK als Vertreter der kantonalen DSB in die Arbeitsgruppe «Polizeibereich»¹⁴ sowie als Stellvertreter der Arbeitsgruppe «Markt/Ausschuss Datenschutz Art. 31» gewählt. Da auf dem vorliegenden Gebiet noch sehr vieles im Fluss ist, ist zurzeit noch nicht absehbar, welchen zeitlichen Aufwand diese Aufgaben erforderlich machen werden.

3. Leistungsvereinbarungen mit privaten Dritten

Ausgangspunkt

Der Kanton Zug lagert aus den verschiedensten Gründen immer mehr öffentliche Aufgaben an private Institutionen oder Unternehmen aus. Er macht dies mit sogenannten Leistungsvereinbarungen.¹⁵ Ende 2005 waren insgesamt 44 Aufgaben ausgelagert. Durch die Auslagerung darf für die Bevölkerung aber keine Verschlechterung ihrer Rechte resultieren. Damit solche Auslagerungen in der gesamten Verwaltung rechtmässig und einheitlich vorgenommen werden, hat der Regierungsrat entsprechende Musterverträge verabschiedet. Lagert eine Verwaltungsstelle eine Aufgabe an Private aus, sind diese Verträge zwingend zu verwenden. Dabei haben die Privaten selbstverständlich auch die Vorschriften bezüglich Datenschutz und Datensicherheit zu beachten. Dies ist denn auch Vorgabe der Musterverträge. Der DSB hat dazu ein Merkblatt verfasst, das den Privaten mit dem Vertrag abgegeben wird.¹⁶ Bereits im Jahr 2004 haben sich zwei Probleme gezeigt, auf die hier kurz zurückzukommen ist.¹⁷

DSB wird erst nach Vertragsabschluss informiert

Sämtliche Leistungsvereinbarungen werden durch den Regierungsrat genehmigt. *Anschliessend*¹⁸ wird der DSB darüber durch Zustellung einer Vertragskopie in Kenntnis gesetzt. Es hat sich verschiedentlich gezeigt, dass in solchen Verträgen Bestimmungen aufgenommen wurden, die zwingenden datenschutzrechtlichen Vorgaben widersprechen. Solche Bestimmungen sind rechtswidrig¹⁹ und daher unverbindlich. In zwei Fällen stellte die zuständige Direktion die

14 «JAI [Justice et affaires intérieures (Justiz und Innere Sicherheit)]/Datenschutz im Bereiche des dritten Pfeilers». Näheres zum «dritten Pfeiler» findet sich hinten auf S. 25 in Fussnote 105.

15 Dies sind Verträge, die alle Rechte und Pflichten der Privaten und der Verwaltung regeln. Näheres dazu s. DSB TB 2004 S. 5 f.

16 Vgl. dazu DSB TB 2004 S. 5 f. und DSB TB 2003 S. 12 Fälle Nr. 10 und 11.

17 DSB TB 2004 S. 5 f.

18 Es kommt auch vor, dass sich die mit der Ausarbeitung einer Leistungsvereinbarung befasste Verwaltungsstelle bezüglich datenschutzrechtlicher Aspekte frühzeitig an den DSB wendet.

19 Zwingend anwendbares öffentliches Recht kann nicht durch vertragliche Vereinbarungen mit privaten Dritten – zulasten von Bürgerinnen und Bürgern – abgeändert bzw. ausser Kraft gesetzt werden.

Entwürfe entsprechender Leistungsverträge dem DSB zur Stellungnahme zu. Dadurch konnte die Aufnahme von rechtswidrigen Bestimmungen verhindert werden.

Im Berichtsjahr hat der Regierungsrat die Musterverträge überarbeitet. Aufgrund der gemachten Erfahrungen hat der DSB in seiner Vernehmlassung beantragt, ihm Leistungsvereinbarungen bereits zum Zeitpunkt der Vertragsverhandlungen – jedenfalls *vor* Beschlussfassung durch den Regierungsrat – zuzustellen. Überprüft der DSB eine Leistungsvereinbarung auf Rechtmässigkeit mit den Vorgaben des Datenschutzes, so erbringt er zuhanden der Vertragsparteien eine kostenlose *Dienstleistung*. Diese macht aber nur dann überhaupt einen Sinn, wenn sie *rechtzeitig* erfolgt, also *vor* der Genehmigung durch den Regierungsrat.

Der Regierungsrat hat dies jedoch *abgelehnt*; der DSB²⁰ wird deshalb erst «post festum», somit *nach* Vertragsabschluss informiert.

Problematik der Archivierungspflicht bei privaten Institutionen

Externe Private, die mit der öffentlichen Verwaltung Leistungsvereinbarungen abschliessen, haben nicht nur die zwingenden Vorschriften des Datenschutzrechts, sondern auch diejenigen des *Archivrechts*²¹ einzuhalten. Bei gewissen Institutionen, deren Dienstleistungen auf absolut freiwilliger Basis in Anspruch genommen werden können, ergeben sich nun Frontalkollisionen zwischen den Vorgaben des Archivrechts und denjenigen des Privatsphärenschutzes.

Die besondere Problematik liegt hier darin, dass die Personen, die das Angebot einer *privaten Institution* nutzen, nicht damit rechnen müssen, dass ihre Akten eines Tages ins Staatsarchiv wandern und später – nach Ablauf der Schutzfristen – dort grundsätzlich für jedermann einsehbar werden.²² Diese Situation ist grundverschieden bei der Nutzung von *staatlichen* Dienstleistungen, da allgemein bekannt ist, dass Amtsstellen ihre Unterlagen archivieren müssen. Der DSB ist der Ansicht, dass hier akuter Handlungsbedarf besteht. Grundsätzlich gibt es nur die Lösung, dass in heiklen Bereichen die Unterlagen anonymisiert²³ archiviert werden.

Es fragt sich hier zudem, ob die privaten Institutionen nicht überhaupt verpflichtet sind, ihre Klienten unaufgefordert über die Rechts-

lage bezüglich der Archivierung aufzuklären. Dann können die Klienten entscheiden, ob sie – nun in Kenntnis der Sachlage – die Dienstleistungen solcher Institutionen nutzen wollen oder gegebenenfalls nicht.

4. Datensicherheit in der kantonalen Informatik²⁴

Datensicherheit ist wichtig!

Die Bearbeitung von Daten der Zuger Bevölkerung ist das Kerngeschäft der Verwaltung. Darunter befinden sich sehr viele, sehr sensible Daten. Man denke etwa an die Daten bei Polizei und Justiz, Gesundheits- und Sozialbehörden – und nicht zuletzt auch an die Steuerverwaltung. Aufgrund des Datenschutzgesetzes ist die Verwaltung verpflichtet, bezüglich Datensicherheit ihre *besondere Verantwortung* wahrzunehmen.²⁵ Dabei ist mindestens der aktuelle Stand der Technik einzuhalten. Nur dadurch können die zunehmenden Gefahren²⁶, denen IT-Strukturen ausgesetzt sind, gebannt werden. Weil die Datensicherheit die *Grundlage jeglichen* Datenschutzes ist, ist der Datenschutzbeauftragte denn auch von Gesetzes wegen in die Pflicht genommen.²⁷

Technische Sicherheitsüberprüfung bei der kantonalen Informatik

Der DSB hat im Berichtsjahr eine externe Firma damit beauftragt, beim kantonalen Informatikdienstleister AIO²⁸ wichtige Server bezüglich Sicherheits- und Zugriffskonfiguration zu überprüfen. Diese Sicherheitsüberprüfung fand in enger Zusammenarbeit zwischen dem AIO, der externen Firma und dem DSB als Auftraggeber statt.

Aus verständlichen Gründen kann hier nicht auf die Untersuchungsergebnisse eingegangen werden. Festgehalten werden kann, dass die untersuchten Systeme grundsätzlich sicher betrieben wurden. Wo sich gewisse Mängel oder Verbesserungsmöglichkeiten ergaben, wurden die erforderlichen Massnahmen umgesetzt.

Umsetzung der Informatikverordnung (ITV)

Mitte 2004 ist die Informatikverordnung in Kraft getreten.²⁹ Sie regelt Planung, Beschaffung, Betrieb und Kontrolle der Informatik in der kantonalen Verwaltung. Da sie die Grundlage

20 Sowie auch das Staatsarchiv.

21 Archivgesetz [BGS 152.4].

22 Zur Illustration: Wer wird wohl eine freiwillige Beratung, etwa im Bereiche AIDS-Hilfe, Drogen- oder Alkoholberatung bei einer *privaten* Institution in Anspruch nehmen, wenn er zu Beginn der Beratung darüber in Kenntnis gesetzt wird, dass seine vollständige Akte später dem Staatsarchiv übergeben wird, und – nach Ablauf der entsprechenden Schutzfristen – grundsätzlich für jedermann frei zugänglich sein wird?

23 Gemäss § 11 Datenschutzgesetz.

24 Fälle aus der Beratungspraxis zum Thema Datensicherheit finden Sie hinten auf S. 15.

25 § 7 Abs. 1 Datenschutzgesetz: «Daten sind insbesondere vor Verlust, Fälschung, Entwendung, Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte zu sichern.»

26 Die vom Bund eingesetzte «Melde- und Analysestelle Informationssicherung/MELANI» hat in ihrem ersten Halbjahresbericht im Dezember 2005 eine starke Zunahme der Gefahren im Bereich IT-Sicherheit festgestellt. Beunruhigend sei die Tatsache, dass immer mehr Angriffe von beauftragten, professionell vorgehenden Hackern ausgehen, insbesondere im Bereiche Industriespionage.

27 § 19 Abs. 1 Bst. a Datenschutzgesetz.

28 Amt für Informatik und Organisation (bei der Finanzdirektion).

29 Informatikverordnung vom 29. Juni 2004 [ITV, BGS 153.53].

der Datenverarbeitung in der Zuger Verwaltung bildet, hat sie einen sehr engen Bezug zu Datenschutz und Datensicherheit. Die ITV sieht deshalb vor, dass der DSB frühzeitig über sämtliche IT-Vorhaben, die einen direkten Bezug zu Datenschutz/Datensicherheit haben, zu informieren ist.³⁰ Nur so ist gewährleistet, dass der DSB rechtzeitig auf Aspekte des Datenschutzes und der Datensicherheit von IT-Projekten hinweisen kann. Die Informationspflicht liegt in erster Linie bei den Direktionen oder Ämtern, die entsprechende IT-Projekte planen. Im Berichtsjahr hat sich nun gezeigt, dass nicht alle von ihnen den DSB rechtzeitig mitbezogen haben.

Da mit dem AIO bereits Ende 2004 vereinbart worden ist, dass jeweils die verantwortlichen IT-Projektleiter des AIO – sicherheitshalber – überprüfen, ob die Direktion ihrer Informationspflicht gegenüber dem DSB nachgekommen ist, wurde der DSB im Berichtsjahr bei verschiedenen Projekten durch das AIO entsprechend informiert.

Die gute Zusammenarbeit zum AIO hat sich somit sehr bewährt. Der frühzeitige Einbezug des DSB muss aber aufgrund der Informatikverordnung³¹ durch die *Direktionen und Ämter* gewährleistet werden. Der DSB hat die diesbezügliche Rechtslage anlässlich einer Sitzung der Direktionssekretäre im Sommer kurz vorgestellt und Ende Jahr alle Direktionen aus aktuellem Anlass nochmals kurz an die vorliegende Informationspflicht bezüglich IT-Projekten erinnert.

Datensicherheitsverordnung

Entgegen dem ausdrücklichen gesetzlichen Auftrag,³² bis spätestens im *Dezember 2001* eine Datensicherheitsverordnung zu erlassen, ist der Regierungsrat dem auch in diesem Jahr nicht nachgekommen.³³

Zum Inhalt einer Datensicherheitsverordnung: Sie muss Verfahren und Zuständigkeiten zur Sicherung von Daten regeln. Ziel wird es sein, bei der Datenbearbeitung Vertraulichkeit, Richtigkeit und Verfügbarkeit von Daten zu gewährleisten. Es wird somit zu regeln sein, was die *Datenbearbeitenden* – die Verwaltungsstellen und die Verwaltungsmitarbeitenden – tun müssen, um den sicheren Umgang mit Daten in der Verwaltung zu gewährleisten.³⁴

Im Berichtsjahr hat die für dieses Geschäft zuständige Finanzdirektion in Zusammenarbeit mit dem DSB den Verordnungsentwurf weiterbearbeitet. Im April hat der Regierungsrat beschlossen, über den Sommer eine verwaltungsinterne Vernehmlassung durchzuführen. Die Finanzdirektion hat die Vernehmlassung entsprechend durchgeführt und anschliessend eine Zusammenstellung der Vernehmlassungantworten erarbeitet. Seit Herbst 2005 ist das Geschäft bei der Finanzdirektion nach wie vor pendent.

Es ist davon auszugehen, dass der Regierungsrat diese Verordnung im Jahr 2006 verabschieden wird, handelt es sich doch hier um ein Jahresziel der Finanzdirektion für 2006. Im nächsten Tätigkeitsbericht – sowie umgehend im elektronischen Newsletter³⁵ – werden Sie über den weiteren Verlauf dieses Projekts informiert.

Online-Verordnung

Was soeben bezüglich der Datensicherheitsverordnung festgehalten wurde, kann hier wiederholt werden: Der Regierungsrat hat auch in diesem Jahr die Online-Verordnung nicht erlassen³⁶ – trotz des ausdrücklichen gesetzlichen Auftrags, dies bis spätestens im *Dezember 2001* zu tun.³⁷ Im Berichtsjahr ergab sich diesbezüglich Folgendes:

Vorerst war strittig, ob diese Verordnung durch die Staatskanzlei oder die Finanzdirektion auszuarbeiten sei. Im Mai beschloss die Regierung, dieser Rechtserlass sei durch die Staatskanzlei auszuarbeiten und der Finanzdirektion zur zweckdienlichen Weiterverwendung zuzuleiten. Vom DSB erwartete die Regierung dabei eine aktive Mithilfe. Dem kam der DSB gerne nach. Er erarbeitete wenig später zuhanden der Finanzdirektion einen ersten Verordnungsentwurf. Dieser wurde in der Folge durch eine Arbeitsgruppe der Finanzdirektion – unter Einbezug des DSB – weiterbearbeitet. Weil die Finanzdirektion ihre Ressourcen für andere Geschäfte einsetzte, blieb das vorliegende Geschäft seit Herbst 2005 bei ihr liegen.

Als Jahresziel für 2006 hat sie sich jedoch vorgenommen, diesbezüglich die verwaltungsinterne Vernehmlassung durchzuführen.

30 § 4 Abs. 1 Informatikverordnung.

31 § 4 Abs. 1 Informatikverordnung.

32 § 7 Abs. 2 Datenschutzgesetz.

33 Zur Vorgeschichte:
DSB TB 2004 S. 8;
DSB TB 2003 S. 6;
DSB TB 2002 S. 5/6;
DSB TB 2001 S. 5/6.

34 Die Datensicherheitsverordnung hat somit einen ganz anderen Fokus als die vorstehend erwähnte Informatiksicherheitsverordnung.

35 Informationen zum elektronischen Newsletter finden Sie hinten in Kapitel II Ziff. 2.2 S. 19.

36 Zur Vorgeschichte:
DSB TB 2003 S. 7.

37 § 7 Abs. 2 Datenschutzgesetz.

II. Berichterstattung 2005

1. Fälle aus der Beratungspraxis

Falls Sie im Folgenden wichtige Themen vermissen, konsultieren Sie die früheren Tätigkeitsberichte – Sie finden dort über 240 weitere Fallbeispiele. Die Tätigkeitsberichte 1999–2004 können Sie beim Datenschutzbeauftragten kostenlos bestellen [041 728 31 47]. Sie finden sie zudem auch layoutgetreu im Internet unter: «www.datenschutz-zug.ch», Rubrik «Kanton Zug/Tätigkeiten».

1.1 Übersicht: Die Fälle auf einen Blick

| Stichwort | Fragestellung | Fall Nr. | Seite |
|--------------------------------------|--|----------|-------|
| Adressbekanntgabe | Siehe Einwohnerkontrolle | | |
| Ahnenforschung | Ist die Einsicht in Zivilstandsunterlagen zulässig? | 17 | 14 |
| Amtsgeheimnis | Rechtslage nach Austritt aus der Verwaltung? | 4 | 10 |
| Baugesuchseinsicht | Müssen die Personalien bei Einsicht in ein Baugesuch bekannt gegeben werden? | 21 | 16 |
| Bürgergemeindeversammlung | Welche Daten sind bezüglich Einbürgerung bekannt zu geben? | 25 | 17 |
| Datenbekanntgabe | Wann sind bei einer Datenbekanntgabe die Personalien des Anfragenden zu registrieren? | 21, 22 | 16 |
| Datensicherheit | Wie ist die elektronische Steuererklärung sicher zu installieren? | 18 | 15 |
| DNA-Probenahme | Bei Jugendlichen erlaubt? | 13 | 13 |
| Einbürgerung | Welche Daten sind der Bürgergemeindeversammlung bekannt zu geben? | 25 | 17 |
| Einsichtsrecht | Zum Recht auf Einsicht in die eigenen Daten | 1 | 9 |
| Einwohnerkontrolle | Dürfen Angaben zu Beruf und Arbeitgeber von Neuzuziehenden erhoben werden? | 24 | 17 |
| Einwohnerkontrolle | Unter welchen Voraussetzungen sind die «erweiterten Personalien» bekannt zu geben? | 20 | 15 |
| Elektronische Steuererklärung | Zur Datensicherheit | 18 | 15 |
| E-Mail | Hinweise zum Umgang mit E-Mails | 3 | 9 |
| E-Mail | Wie können vertrauliche Daten sicher übermittelt werden? | 8 | 11 |
| Fahrzeughalterdaten | Einführung der Gebühr für Nachtparkieren: alle Fahrzeughalterdaten an die Gemeinde? | 23 | 16 |
| Familienforschung | Ist die Einsicht in Zivilstandsunterlagen zulässig? | 17 | 14 |
| Forschung | Auswertung des Polizeinotfunks für eine Sprachuntersuchung? | 15 | 14 |
| Forschung | Bekanntgabe von Adressen durch die Einwohnerkontrolle? | 16 | 14 |
| Foto | Foto des Mitarbeitenden im Internet? | 2 | 9 |
| Homepage | Siehe Internet | | |
| Informanten | Welchen Rechtsschutz geniessen Informanten? | 14 | 13 |
| Internet | Foto des Mitarbeitenden im Internet? | 2 | 9 |
| Internet | Was gehört nicht auf die Homepage der Schule? | 9 | 11 |
| Kindeswohl | Kindeswohl möglicherweise gefährdet – wer hat wen zu informieren? | 5 | 10 |
| Kirchgemeinde | Darf das Kollektenergebnis von Beerdigungen im Pfarrblatt veröffentlicht werden? | 27 | 17 |
| Lehre | Wie kommt der Lehrbetrieb zum Zeugnis seiner Lehrperson? | 11 | 12 |
| Polizei | Zur DNA-Probenahme bei Jugendlichen | 13 | 13 |
| Schule | Was hat der Schulfotograf zu beachten? | 12 | 12 |
| Schule | Wie gewährleisten Lehrpersonen die Privatsphäre der Schülerinnen und Schüler? | 7 | 11 |
| Schule | Wie ist die Zugriffsberechtigung auf Schulservern zu organisieren? | 10 | 12 |
| Schule | Zur Privatsphäre von Schülerinnen und Schülern | 6 | 11 |
| Statistik | Datenbekanntgabe für statistische Zwecke? | 19 | 15 |
| Verschlüsselung | Wie können Dokumente sicher per E-Mail verschickt werden? | 8 | 11 |
| Zivilstandsfälle | Dürfen Taufen, Hochzeiten oder Todesfälle im Pfarrblatt und im Internet veröffentlicht werden? | 26 | 17 |

1.2 Recht auf Einsicht in die eigenen Daten

Fall 1 Betroffene Personen verlangen Einsicht in die eigenen Daten – was ist zu beachten?

Der DSB erhielt auch dieses Jahr wieder sehr viele Anfragen von Privaten, aber auch von Verwaltungsstellen, die den Anspruch auf Einsicht in die eigenen Daten betrafen. Auf die wichtigsten Fragen rund um das Einsichtsrecht wurde schon in früheren Tätigkeitsberichten eingegangen. Da alle DSB-Tätigkeitsberichte kostenlos bestellt werden können³⁸ und auch im Internet zugänglich sind, beschränken wir uns hier auf die Übersicht bereits veröffentlichter Informationen:

Fragen rund um das Einsichtsrecht in die eigenen Daten

Grundsätzliches zum Einsichtsrecht

TB 2004 S. 13, TB 2003 S. 8, TB 2002 S. 9 Fall Nr. 1, TB 2001 S. 9 Fall Nr. 1, TB 2000 S. 18 Fall Nr. 14

Einsicht in Daten: Wo sind überhaupt welche Datensammlungen vorhanden?

s. hinten zum Register S. 23

Darf ich meine eigenen Daten einsehen?

TB 2004 S. 13 f. Fall Nr. 11

Einsicht in das eigene Personaldossier

TB 2000 S. 19 Fall Nr. 15

Findet die Einsicht beim DSB statt?

[Antwort vorweg: Nein – beim datenbearbeitenden Organ]
TB 2004 S. 14 Fall Nr. 14

Archivierte Daten

TB 2004 S. 14 f. Fall Nr. 15

Polizeidaten

TB 2004 S. 19 f. Fall Nr. 30, TB 2003 S. 25 f. Fall Nr. 54

Schuldaten/Prüfungsdaten: Einsicht und Kopien?

TB 2003 S. 19 f. Fall Nr. 35, TB 2002 S. 16 f. Fall Nr. 25

Zum Anspruch auf kostenlose Kopie

TB 2004 S. 14 Fall Nr. 12

Schliesslich: Einsicht erhalten – aber sind denn das alle Unterlagen ...?

TB 2004 S. 14 Fall Nr. 13

38 Beim DSB-Sekretariat telefonisch unter 041 728 31 47 oder per E-Mail bei «hildegard.steiner@allg.zg.ch».

39 Es liegt in der Entscheidungsbefugnis des Arbeitgebers, ob er direkte Telefonnummer und persönliche geschäftliche E-Mail-Adresse seiner Mitarbeitenden gegenüber der Öffentlichkeit kommunizieren will.

40 Privatadresse, Jahrgang, Hobbys etc.

41 Wie vertraulicher Inhalt von E-Mails verschlüsselt werden kann, s. hinten S. 11 Fall 8.

1.3 Arbeitsrechtliches

Fall 2 Foto des Mitarbeitenden im Internet?

Regelmässig fragen Mitarbeitende gemeindlicher Verwaltungen, ob ihr Arbeitgeber dazu berechtigt sei, gegen ihren Willen ihr Foto auf der gemeindlichen Homepage zu veröffentlichen. Der Arbeitgeber hat das Recht, der Öffentlichkeit gegenüber bekannt zu geben, wer die Ansprechpersonen sind und wo und wie sie geschäftlich zu erreichen sind. Diese Angaben dürfen auch im Internet veröffentlicht werden. Es handelt sich somit um die geschäftliche Adresse, gegebenenfalls³⁹ Telefonnummer und E-Mail-Adresse.

Nicht zulässig ist dagegen die Publikation von Fotos im Internet gegen den Willen der Mitarbeitenden. Die Gründe einer ablehnenden Haltung sind unerheblich, es besteht denn auch keinerlei Begründungspflicht. Gleich verhält es sich übrigens mit allen persönlichen/privaten Angaben über Mitarbeitende.⁴⁰

Mit Zustimmung der Betroffenen ist die Publikation erlaubt. Zu betonen ist hier aber, dass die Zustimmung *vollständig freiwillig* zu erfolgen hat und somit keinerlei Druck – oder Androhung von Nachteilen – auf die Mitarbeitenden ausgeübt werden darf. Auch wenn 90% der Mitarbeitenden ihre Zustimmung gegeben haben, muss eine ablehnende Haltung der restlichen 10% respektiert werden.

Fall 3 Vertrauliches im E-Mail? Und schon bald hat die halbe Welt Kenntnis!

E-Mails sind schnell geschrieben und noch viel schneller vielen Adressaten zugestellt. Und diese wiederum haben sie ebenso rasch vielen weiteren Adressaten zur Kenntnis gebracht.

Diese Tatsache sollte man bedenken, wenn man ein E-Mail mit vertraulichem Inhalt verfasst.⁴¹ Etwa wie im Falle der Mitarbeiterin, die dem Vorgesetzten per E-Mail eine heikle Situation am Arbeitsplatz mitteilte, um dann später feststellen zu müssen, dass die Antwort des Vorgesetzten an die Mitarbeiterin in Kopie auch gleich an sämtliche Abteilungsleiter ging.

Die Rechtslage ist klar: Unabhängig vom Informationsträger – Brief, Telefongespräch oder eben E-Mail – hat der Arbeitgeber Informationen

eines Mitarbeitenden nur dann anderen Personen bekannt zu geben, wenn dies für deren Aufgabenerfüllung erforderlich ist.

Werden Daten über Personen unrechtmässig bekannt gegeben und entsteht dadurch ein Schaden, sei er materieller Art oder auch in Form einer Persönlichkeitsverletzung, so kann der Verursacher zivilrechtlich, disziplinarisch und gegebenenfalls strafrechtlich zur Verantwortung gezogen werden.

Im Gegensatz zum Schriftverkehr ist die elektronische Post ein eher informelles Medium. E-Mails werden oft nicht mit der gleichen Sorgfalt bearbeitet wie die briefliche Korrespondenz. Die Unaufmerksamkeit eines Sekundärbruchteils, und schon ist das E-Mail an die falsche Adressatengruppe entwischt. Es muss zudem auch immer davon ausgegangen werden, dass E-Mails bei Abwesenheit des Adressaten an Stellvertreter oder Sekretariate weitergeleitet werden. Der Verfasser eines E-Mails muss daher grundsätzlich damit rechnen, dass weitere Personen Kenntnis erhalten können.

Fazit: Falls man wirklich Vertrauliches mitteilen möchte, ist E-Mail wohl nicht das richtige Medium. Ein Brief mit dem Vermerk «Persönlich/Vertraulich» ist nach wie vor die bessere Wahl.

Fall 4 Gilt das Amtsgeheimnis auch nach Verlassen der Arbeitsstelle?

Ein ehemaliger Verwaltungsmitarbeiter wurde von der Polizei aufgefordert, Aussagen zu einem Vorfall zu machen, der sich während seines früheren Anstellungsverhältnisses mit der Verwaltung zugetragen hat. Er fragte beim DSB nach, ob er berechtigt sei, der Polizei Auskunft zu geben.

Verwaltungsmitarbeitende unterstehen dem Amtsgeheimnis. Sie dürfen somit geschäftliche Informationen weder anderen Verwaltungsstellen, noch gar Dritten bekannt geben. Dies gilt grundsätzlich auch gegenüber der Polizei. Das Amtsgeheimnis ist zudem *auch nach Verlassen* der Stelle zu beachten.⁴² Ob gegenüber der Polizei Aussagen zu machen sind, das Amtsgeheimnis somit aufzuheben ist, prüft und entscheidet die zuständige vorgesetzte Stelle des Mitarbeitenden, in der kantonalen Verwaltung der Direktionsvorsteher, in der Gemeinde

der zuständige Gemeinderat [gegebenenfalls der Gemeindeschreiber]. Diese Stellen sind denn auch zuständig, ehemalige Mitarbeitende vom Amtsgeheimnis zu entbinden.

1.4 Schule

Fall 5 Kindeswohl gefährdet? – Wer ist zu informieren?

Anlässlich von Präsentationen und Besprechungen des DSB zeigt es sich immer wieder, dass weder Lehrpersonen noch Personen, die im Sozialbereich tätig sind, wissen, welche Stelle wie zu informieren ist, wenn aus ihrer Sicht das Kindeswohl gefährdet erscheint. Es lohnt sich deshalb, auf zwei Punkte hinzuweisen.

Erstens: Wird der Name des Kindes nicht genannt, so kann bei Berufskollegen, Lehrpersonen oder entsprechenden Fachstellen ohne weiteres Rat eingeholt werden. Voraussetzung ist dabei, dass die Anonymität gewährleistet ist, das Kind und sein Umfeld somit auch aufgrund der Schilderung nicht bestimmbar wird.

Zweitens: «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 anwendbare Bestimmung des Zuger Einführungsgesetzes zum ZGB.⁴³ Wichtig ist dabei:

- wer eine Gefährdung des Kindeswohls wahrnimmt, ist *gesetzlich verpflichtet*, zu handeln;
- ob das Kindeswohl gefährdet ist, ist interpretationsbedürftig, somit situationsabhängig und aufgrund einer Gesamtbeurteilung nach bestem Wissen und Gewissen vorzunehmen;
- die Datenbekanntgabe erfolgt nicht an Kollegen, Schule oder an die Sozialbehörde, sondern an die *zuständige Vormundschaftsbehörde*;
- vorbehalten bleibt die polizeiliche Anzeige in entsprechenden Fällen.

Diese Bestimmung stammt nicht etwa aus der Frühzeit der Zuger Gesetzgebung, sondern wurde durch den Gesetzgeber erst vor wenigen Jahren ins Gesetz eingefügt.⁴⁴

42 Betr. kantonalem Arbeitsverhältnis: § 29 Personalgesetz [BGS 154.21].

43 § 34 des Gesetzes betreffend die Einführung des Schweizerischen Zivilgesetzbuches für den Kanton Zug [EG-ZGB, BGS 211.11].

44 In Kraft seit dem 17. November 2001.

Wer als Mitarbeiter einer öffentlichen Verwaltungsstelle hingegen eigenmächtig *andere* Stellen oder Personen informiert, macht sich gegebenenfalls der Verletzung des Amtsgeheimnisses strafbar.⁴⁵

Fall 6 Auch Schülerinnen und Schüler haben eine Privatsphäre

Wenn Schülerinnen und Schüler ihre persönlichen Sachen im Schulzimmer unter ihrer Bank lassen – darf die Lehrperson diese ungefragt kontrollieren?

Auch wenn Ablagefächer in der Schulbank offen zugänglich sind, so ist trotzdem davon auszugehen, dass die Lehrperson diesen Bereich respektiert, somit nicht ohne nachzufragen Unterlagen kontrolliert.

Anders verhält es sich nur, wenn es um Abklärungen bezüglich disziplinarischer oder gar strafrechtsrelevanter Vorfälle geht und ein konkreter Verdacht gegeben ist.

Fall 7 Privatsphäre in Schul- und Lehrerzimmer

Lehrpersonen verfügen oft über recht viele Informationen, nicht nur über ihre Schülerinnen und Schüler, sondern meist auch über deren familiäres Umfeld. In kleinräumigen Verhältnissen trifft dies besonders zu. Viele dieser Informationen sind sehr persönlicher Natur und dementsprechend vertraulich zu behandeln.

Wie der beim DSB eingegangene Bericht eines Schulinspektors zeigte, ist der Umgang mit Vertraulichem in der Schulpraxis offenbar nicht immer rechtmässig: Häufig sei zu beobachten, dass Lehrpersonen vertrauliche Dokumente wie Beobachtungs- und Beurteilungsbogen, Notentabellen, Elternkorrespondenz oder persönliche Notizen auf dem Lehrerpult liegen lassen und beim Verlassen des Schulzimmers dieses nicht etwa abschliessen. Auch in den Lehrerzimmern sei oft einiges zu erfahren – unter voller Namensnennung aller Beteiligten, betreffe es Schüler oder deren Eltern.

Auch wenn dieser unsorgfältige Umgang mit Vertraulichem durch Lehrpersonen auf Gedankenlosigkeit beruht, es macht die Sache nicht besser. Ist das Amtsgeheimnis verletzt, stellt sich die Frage nach strafrechtlichen⁴⁶ Konsequenzen. Ist den Betroffenen durch die unzulässige Weitergabe von Daten Schaden

entstanden,⁴⁷ haftet der Schadensverursacher gegebenenfalls zivilrechtlich.

Fazit: Vertrauliche Dokumente sind im Schulzimmer stets unter Verschluss zu halten, Persönliches über Schülerinnen und Schüler sowie deren Eltern ist vertraulich zu behandeln, somit weder im Lehrerzimmer noch anderswo zu verbreiten.

Fall 8 Wie müssen Lehrpersonen sensible Dokumente per E-Mail versenden?

Lehrpersonen haben in der Regel zwei Arbeitsplätze – den einen in der Schule, den anderen zu Hause. Von beiden werden E-Mails im Zusammenhang mit der Schule versandt. Dabei ist zu beachten, dass die Übertragung von E-Mails vom privaten Arbeitsplatz aus, somit via Internet, vollständig unsicher ist. Solche E-Mails können an vielen Stellen eingesehen, kopiert, verändert oder auch gelöscht werden.⁴⁸ Aus Gründen der Datensicherheit ist es deshalb nicht erlaubt, *besonders schützenswerte Daten* wie etwa schulpsychologische Anmeldungen, medizinische Informationen oder Protokolle von Elterngesprächen unverschlüsselt via Internet zu mailen. Wie Office-Dokumente zu verschlüsseln sind, damit sie geschützt per E-Mail zugestellt werden können, ist einem Merkblatt des DSB zu entnehmen. Dieses ist im Zuger «Schulinfo Zug»⁴⁹ veröffentlicht und steht auch auf der DSB-Homepage zur Verfügung. Die Hinweise sind nicht nur für Lehrpersonen nützlich, sondern für jedermann, der vertrauliche Dokumente per E-Mail zustellen will. Ergänzend anzumerken ist, dass das verwaltungseigene Netzwerk von Gemeinde und Kanton als sicher zu betrachten ist. Verwaltungsintern dürfen daher grundsätzlich auch vertrauliche Daten unverschlüsselt per E-Mail übermittelt werden.

Fall 9 Was gehört nicht auf die Homepage der Schule?

Viele Anfragende aus dem Schulbereich wollten wissen, was auf der Homepage der Schule oder einer Klasse veröffentlicht werden darf. Die Publikation im Internet entspricht nicht der Veröffentlichung in einem gedruckten Medium. Informationen, die im Internet veröffentlicht werden, erhalten eine neue Dimension. Sie sind

45 Ausser es liege eine Entbindung vom Amtsgeheimnis vor.

46 Verletzung des Amtsgeheimnisses, Art. 320 des Strafgesetzbuches (StGB, SR 311.01).

47 Wenn etwa ein Schüler aufgrund einer unzutreffenden Information zu Unrecht eine Lehrstelle nicht erhält.

48 Vgl. zur Problematik des Versendens von E-Mails auch den Fall 3 vorne auf S. 9.

49 Schulinfo Zug Nr. 3, 2004–05, S. 36/37.

weltweit für jedermann zugänglich, praktisch nicht mehr löschar⁵⁰ und können auf viele Weisen missbraucht werden. Dadurch kann den Betroffenen Schaden entstehen. Gewisse Informationen können somit in einer Schulbroschüre oder in einer Schülerzeitung abgedruckt werden, dürfen aber nicht im Internet publiziert werden.

Es dürfen deshalb auf öffentlich zugänglichen Schulwebsites keine persönlichen, namentlich bezeichnete Statements oder Berichte und insbesondere keine Fotos, auf denen Schülerinnen und Schüler erkennbar sind, veröffentlicht werden. Unerheblich ist dabei, ob die Schülerinnen und Schüler ihre Zustimmung zur Veröffentlichung erteilen.

Sind für schulinterne Zwecke passwortgeschützte Bereiche vorhanden, so können gegebenenfalls Fotos enthalten sein. Zu bedenken ist, dass Passwörter keine absolute Sicherheit gewährleisten können, werden doch solche immer wieder durch die eigenen Schüler im Internet veröffentlicht.

Fazit: Die öffentlichen Schulen haben auf dem vorliegenden Gebiet zum Schutze von Schülerinnen und Schülern sowie auch Lehrpersonen ihre Verantwortung wahrzunehmen. Übrigens: Eine Schulwebsite kann auch ohne Personenaufnahmen und namentlich bezeichnete Statements attraktiv gestaltet werden.

Fall 10 **Wie ist die Zugriffsberechtigung auf Schulservern zu organisieren?**

Dürfen auf einem Schulserver, der für sämtliche Lehrpersonen einer bestimmten Stufe zugänglich ist, Notenlisten von Schülerinnen und Schülern, Absenzenlisten und weitere Beurteilungen gespeichert werden?

Antwort: Nein. Die Zugriffsberechtigungen sind so zu definieren, dass die Lehrpersonen jeweils nur Dokumente ihrer eigenen Klassen sehen und bearbeiten können. Denn Lehrpersonen, die nichts mit den betreffenden Schülern zu tun haben, sind als Dritte zu behandeln.

Fall 11 **Auch die Lehrbetriebe müssen die Zeugnisse unterzeichnen**

Lehrlinge sind verpflichtet, dem Lehrbetrieb das Semesterzeugnis zur Unterschrift zu über-

bringen.⁵¹ Verschiedene Lehrbetriebe machten die entsprechenden Schulen darauf aufmerksam, dass diese Regelung in vielen Fällen nicht befriedige, da Lehrlinge die Zeugnisse den Betriebsverantwortlichen oft zu spät oder teilweise auch gar nicht brächten. Diese Betriebe möchten deshalb direkt von der Schule mit einer Kopie des Zeugnisses bedient werden.

Aus datenschutzrechtlicher Sicht ist die geltende Regelung korrekt: Die Lehrlinge als betroffene Personen erhalten ihr Zeugnis und sind verpflichtet, dieses dem Lehrbetrieb zur Unterschrift vorzulegen. Zu bedenken ist, dass wohl die Mehrheit der Lehrlinge bereits volljährig ist, somit mündige Bürgerinnen, mündige Bürger sind.

Fazit: Die geltende Regelung ist zu belassen. Nach entsprechender Information müsste es eigentlich gelingen, zwischen Schule, Lehrperson und Betrieb die korrekte und termingemässe Weitergabe des Zeugnisses zu organisieren.

Fall 12 **Der Schulfotograf und die Privatsphäre**

Es ist dem Datenschutzbeauftragten nicht bekannt, wie verbreitet das Erscheinen des «Schulfotografen» im Klassenzimmer heute noch ist. Gleich in mehreren Fällen stellten sich aber in diesem Jahr Fragen des Privatsphärenschutzes. Einerseits wollten Eltern nicht, dass ihr Kind auf der Foto erscheint, andererseits war man mit der Anfertigung von Einzelporträts nicht einverstanden. Es lohnt sich deshalb, die rechtliche Seite kurz zu beleuchten.

Dieses Thema wird weder im kantonalen noch im hier massgeblichen gemeindlichen Schulrecht geregelt. Somit handelt es sich nicht um eine Angelegenheit, die durch das öffentliche Recht geregelt wird; sie untersteht vielmehr dem *Privatrecht*. Ob der Schulfotograf kommen soll, welcher es sein soll, ob Klassenfotos und/oder Einzelporträts angefertigt werden sollen, zu welchem Preis und welchen weiteren Konditionen – all dies ist zwischen dem Fotografen und den Eltern vorgängig zu vereinbaren.

Sind die Schülerinnen und Schüler bezüglich dieser Frage zudem selber urteilsfähig, so ist es ihnen überlassen, ob sie fotografiert werden möchten oder nicht. Die Schule hat deren Entscheidung zu respektieren.

50 Da Suchmaschinen ständig alle greifbaren Inhalte selber kopieren und ihrerseits wieder zugänglich machen, nützt auch das Löschen der Daten auf dem eigenen Server nichts.

51 § 11 Reglement Bildungszentren (IBGS 413.12).

1.5 Sicherheit und Polizei

Fall 13 DNA-Probenahme bei Jugendlichen erlaubt?

In der Strafverfolgung nimmt die Bedeutung der Analyse von DNA-Proben zur Aufklärung von Straftaten ständig zu.⁵² Dieses Instrument ist aber nicht ein Wundermittel gegen das Verbrechen. Wie überall können Fehler, Missverständnisse oder gar Missbräuche vorkommen. Diese können auf dem vorliegenden Gebiet sehr schwerwiegende Folgen für unschuldige Betroffene haben. Wichtig ist deshalb bei der Anwendung dieses Instrumentes die Bedeutung der Unschuldsvermutung und des Datenschutzes.

Es stellte sich im Berichtsjahr verschiedentlich die Frage, unter welchen Rahmenbedingungen die Polizei bei Jugendlichen eine DNA-Probenahme vornehmen dürfe.

Bei Jugendlichen kommt grundsätzlich – wie bei Erwachsenen – das ordentliche Untersuchungsverfahren zur Anwendung.⁵³ Gemäss Bundesrecht kann bei Personen, die eines Verbrechens *oder Vergehens* verdächtigt werden, eine DNA-Probenahme angeordnet werden.⁵⁴ Ordnet die *Polizei* eine Probenahme an, so informiert sie die betroffene Person über ihre Rechte⁵⁵, insbesondere über die Möglichkeit, diesen Entscheid bei der Strafuntersuchungsbehörde [Untersuchungsrichter] anfechten zu können. Bei einer Anfechtung wird die Entnahme nur vorgenommen, wenn die Strafuntersuchungsbehörde den Entscheid bestätigt.⁵⁶ Der Entscheid der Strafuntersuchungsbehörde kann übrigens im Rahmen des Strafverfahrens mit Beschwerde angefochten werden.⁵⁷

Fazit: Die Polizei kann somit einen Wangenschleimhautabstrich für eine DNA-Analyse *auch ohne vorgängige* untersuchungsrichterliche Anordnung im Rahmen der erkennungsdienstlichen Massnahmen durchführen. Voraussetzung dazu ist jedoch, dass die betroffene Person nach einer korrekt erfolgten Rechtsbelehrung der Probenahme *zugestimmt hat*. Stimmt sie hingegen nicht zu, hat der Untersuchungsrichter zu entscheiden.

Unzulässig ist die Probenahme durch die Polizei jedenfalls, wenn nicht ein – konkreter – Verdacht vorliegt, dass die betreffende Person ein Ver-

brechen oder ein Vergehen begangen hat. Die Massnahme muss zudem, wie jegliches polizeiliches Handeln, in grundsätzlicher Hinsicht verhältnismässig sein.

Die ausführliche Stellungnahme des DSB wird in GVP 2005 veröffentlicht.

Fall 14 Welchen Rechtsschutz geniessen Informanten?

Eine Privatperson äusserte sich in einem Schreiben an die Strafanstalt sehr negativ über einen Insassen. Nachdem dieser vom fraglichen Brief Kenntnis erlangt hatte, wollte er ihn lesen. Konnte er Einsicht verlangen?

Das Schreiben enthielt Informationen über den betreffenden Insassen. Es wurde durch die Strafanstalt in seinem Dossier abgelegt und bildete somit einen Teil seiner Akten. Grundsätzlich hat der Insasse das Recht, jederzeit Einsicht in seine eigenen Daten zu nehmen.⁵⁸ Eine Verwaltungsstelle darf die Auskunft und Einsicht über Daten nur aus *überwiegenden* Interessen der Öffentlichkeit oder Dritter begründet einschränken, mit Auflagen versehen, aufschieben oder verweigern.⁵⁹

Die Einschränkung oder gar Verweigerung der Einsicht in die eigenen Daten ist ein *sehr schwerer* Eingriff in die Rechte Betroffener, da es ihnen dadurch verunmöglicht ist, zu erfahren, was über sie an Daten vorhanden ist und insbesondere, ob die Daten über sie überhaupt korrekt sind. Die Ausübung des praktisch sehr bedeutsamen Rechts auf Berichtigung falscher Daten wird so zum vornherein verhindert – die Problematik von «Fichen» ist angesprochen. Die Beschränkung der Einsicht darf deshalb grundsätzlich nur in *klaren Ausnahmefällen* zur Anwendung kommen.

Dies kann etwa dann der Fall sein, wenn der Anzeigerstatter keinerlei eigene, persönliche Interessen verfolgt⁶⁰ und zudem mit einiger Sicherheit anzunehmen ist, dass der Angezeigte sich am Anzeigenden in gefährlicher Weise rächen könnte.

Im konkreten Fall lagen keine diesbezüglichen Anhaltspunkte vor. Der Insasse konnte deshalb Einsicht in den fraglichen Brief nehmen, eine Kopie wurde ihm abgegeben.

52 Die durch den Bund geführte DNA-Datenbank umfasste Ende 2005 offenbar bereits über 80'000 DNA-Profile [vgl. Tages-Anzeiger vom 6. Januar 2006, S. 17].

53 § 62 Abs. 3 der Strafprozessordnung [BGS 321.1].

54 Art. 3 Abs. 1 DNA-Profil-Gesetz [SR 363].

55 Art. 15 Abs. 1 DNA-Profil-Gesetz: «Die anordnende Behörde informiert die betroffene Person vor der Probenahme über die Aufnahme ihres DNA-Profiles in das Informationssystem, über ihre Auskunftsrechte und über die Voraussetzungen der Löschung.»

56 Art. 7 DNA-Profil-Gesetz. Vgl. dazu § 12 Abs. 1 bis der Zuger Strafprozessordnung [BGS 321.1].

57 § 80 der Strafprozessordnung [BGS 321.1].

58 § 13 Abs. 1 Bst. c DSG.

59 § 14 Abs. 1 DSG.

60 Etwa wenn die Gründe altruistischer oder unter Umständen öffentlicher Natur sind.

1.6 Forschung

Fall 15 Auswertung des Polizeinotrufs für eine Sprachuntersuchung?

Im Rahmen des «Nationalen Forschungsprogramms/NFP 56»⁶¹ beabsichtigte ein Forschungsteam den Wechsel vom Deutschschweizer Dialekt in die hochdeutsche Sprache bei Deutschschweizern in beruflichen Alltagssituationen zu untersuchen. Zu diesem Zweck wollte man den Zuger Polizeinotruf [Telefon 117] systematisch auswerten. Man ging davon aus, dass die polizeilichen Mitarbeitenden bei der Betreuung des Notrufs immer wieder von Mundart auf Hochdeutsch zu wechseln hätten. Zudem werden diese Anrufe aus Beweisgründen aufgezeichnet.

In aller Regel ist der Inhalt von Gesprächen, die über den Polizeinotruf geführt werden, *höchst sensibel*. Die Anrufenden melden Unfälle oder machen gegebenenfalls Hinweise zu kriminellen Vorfällen. Dabei ist die Polizei darauf angewiesen, dass sie möglichst umfassend und genau informiert wird. Die Anrufenden ihrerseits können davon ausgehen, dass ihre Angaben ausschliesslich für polizeiliche Zwecke verwendet werden. Die Weitergabe der aufgezeichneten Gespräche des Polizeinotrufs kann in Anbetracht der Sensibilität des Gesprächsinhalts für die Betroffenen und auch aus polizeilichen Gründen nicht in Frage kommen.

Zulässig wäre eine Weitergabe der Aufzeichnungen hingegen ohne weiteres, wenn die Gespräche *durch die Polizei anonymisiert* würden, ein Bezug zu den konkreten Vorfällen und Personen somit nicht mehr gemacht werden kann. Die rechtmässige Anonymisierung solcher Aufzeichnungen erfordert einen erheblichen Arbeitsaufwand. Dass die knappen polizeilichen Ressourcen dafür nicht eingesetzt werden können, führte verständlicherweise zu einer Absage durch die Zuger Polizei.

Fall 16 Bekanntgabe von Adressen durch die Gemeinde für ein Forschungsprojekt?

Das Forschungsprojekt «Ritualisierungen in Familien» deckt einen Teilbereich des «Nationalen Forschungsprogramms/NFP 52» ab. Beabsichtigt ist die Befragung von jungen Familien in der Deutschschweiz mit Kindern der

Jahrgänge 1996 und 1999 über «Ausgestaltung und Bedeutung von Familienritualen in den Augen von jungen Müttern und Vätern».

Das Forscherteam einer Universität möchte von der Einwohnerkontrolle die Adressen von entsprechenden Familien, um diesen den Fragebogen zustellen zu können. Es ist dann Sache der angeschriebenen Familien, ob sie bei der Studie mitmachen möchten oder nicht. Die Forscher geben ihre datenschutzrechtlichen Rahmenbedingungen bekannt⁶² und verpflichten sich der Gemeinde gegenüber schriftlich, diese auch einzuhalten.

Die Datenbank der gemeindlichen Einwohnerkontrolle könnte die Adressen von solchen Familien ohne weiteres aufbereiten. Die Einwohnerkontrolle erkundigte sich über die Zulässigkeit der Bekanntgabe der fraglichen Adressen.

Da es hier nur um die Bekanntgabe der Adresse von Familien geht, klare datenschutzrechtliche Rahmenbedingungen vorliegen und das Forscherteam Gewähr für deren Einhaltung bietet, kann die Gemeinde die gewünschten Adressen bekannt geben. In der Folge wurden der Forschungsleitung 450 Adressen zugestellt. Abschliessend ist aber festzuhalten, dass die Gemeinde keinesfalls verpflichtet ist, einem solchen Gesuch stattzugeben.

Fall 17 Zur Einsicht in Zivilstandsunterlagen für die Familienforschung

Eine Privatperson wollte beim Zivilstandsamt einer Gemeinde Informationen über ihre eigenen Vorfahren erhalten. Mit Hinweis auf «den Datenschutz» wurde ihr dies nicht gestattet. Sie erkundigte sich deshalb beim Datenschutzbeauftragten nach der Rechtslage. Im Rahmen der Familienforschung kann die *kantonale Aufsichtsbehörde* aufgrund von Bundesrecht die Bekanntgabe von Personenstandsdaten auf Gesuch hin bewilligen, sofern die Beschaffung der Daten bei den direkt betroffenen Personen nicht möglich oder offensichtlich nicht zumutbar ist.⁶³ Im vorliegenden Fall waren die betroffenen Personen schon lange verstorben, sodass einer Bewilligung nichts im Wege stand. Ohne weiteres hat das Zivilstandsamt dem Gesuchsteller auch Kopien anzufertigen, wobei Daten von unbeteiligten Drittpersonen abzudecken sind.

61 Das NFP 56 geht gemäss eigenen Angaben davon aus, dass die Vielfalt der Sprachen heute neue Fragen an Schule, Politik, Wirtschaft, Gesellschaft und auch an jedes einzelne Individuum stelle. Es sollen deshalb Grundlagen zur Erhaltung, Förderung und Nutzung der Sprachenvielfalt in der Schweiz erforscht und entwickelt werden.

62 Inhalt der Datenschutzverpflichtung: Die Adressen werden ausschliesslich für das geplante Projekt verwendet. Die Familien werden einmal angeschrieben. Es wird ausdrücklich auf die Freiwilligkeit des Mitmachens hingewiesen. Nach der Auswertung der Fragebogen wird nur noch mit den anonymisierten Daten gearbeitet. Resultate werden ausschliesslich anonym publiziert. Die vier Personen, die Einsicht in die Fragebogen haben, werden namentlich bekannt gegeben. Sie verpflichten sich schriftlich zur Einhaltung der Datenschutzvorgaben. Es werden zudem Hinweise zur Datensicherheit und zur Datenvernichtung gemacht.

63 Art. 60 der Eidg. Zivilstandsverordnung [ZStV, SR 211.112.2].

Falls betroffene Personen noch leben, so hätte der Gesuchsteller in seinem Gesuch deren schriftliche Zustimmung beilegen oder darlegen müssen, warum es für ihn nicht zumutbar ist, deren Zustimmung einzuholen.

Fazit: «Der Datenschutz» verhindert die Familienforschung in der Regel keineswegs. Die geltenden Vorschriften gewährleisten hingegen, dass nicht Unberechtigte Einsicht in Familiendaten erhalten.

1.7 Informatik und Datensicherheit

Fall 18 Missverständnisse rund um die elektronische Steuererklärung «eTax.zug»

Die Zuger Steuerverwaltung gibt den Steuerpflichtigen die Möglichkeit, ihre Steuererklärung selber elektronisch zu erfassen. Dazu stellt die Steuerverwaltung im Internet die Software «eTax.zug» zum Herunterladen zur Verfügung. Mit dem Hinweis «Falls Sie eine persönliche Firewall- oder Antivirus-Software auf Ihrem Computer haben, empfehlen wir Ihnen, diese während der Installation zu deaktivieren.» soll sichergestellt werden, dass die Installation auf dem PC des Steuerpflichtigen korrekt vorgenommen wird. Diesen Hinweis hatten nun verschiedene Nutzer falsch verstanden und sich deshalb an den Datenschutzbeauftragten gewandt: Ob es denn menschenmöglich sei, dass die Zuger Steuerverwaltung ein Tool zur Verfügung stelle, bei dem während des Herunterladens das Firewall- und Virenschutzprogramm des Nutzers deaktiviert werden müsse, man somit einen PC mit Internetverbindung hat, der ohne jeglichen Schutz ist.

Es kann Entwarnung gegeben werden, denn Folgendes gilt:

- Während des *Herunterladens* von eTax sind Firewall und Virenschutz *nicht* zu deaktivieren. Der PC ist und bleibt somit während der Verbindung zum Internet geschützt.
- Nachdem die Software heruntergeladen ist, soll die Verbindung zum Internet unterbrochen werden. Anschliessend – somit im off-line-Modus – sind Firewall und Virenschutz zu deaktivieren und eTax kann installiert werden.
- Nach erfolgreicher Installation von eTax

können die Schutzprogramme wieder aktiviert werden.

- Das Ausfüllen der elektronischen Steuererklärung sollte *mit unterbrochener Verbindung* zum Internet vorgenommen werden.

Die Hinweise der Steuerverwaltung zur eTax-Installation waren somit durchaus korrekt. Aber bei Schnelllesenden konnten in der Tat gewisse Missverständnisse entstehen.

Die Steuerpflichtigen sollten übrigens beachten, dass sämtliche Steuerdaten auf dem eigenen PC oder Laptop *unverschlüsselt* vorliegen, und dass unter Umständen deshalb Drittpersonen Einblick in die Daten der Steuererklärung nehmen können.⁶⁴

Fall 19 Datenbekanntgabe für statistische Auswertungen

Es stellte sich die Frage, wie vorzugehen ist, wenn eine Verwaltungsstelle sehr sensible Daten einer anderen Verwaltungsstelle beziehen möchte, um Auswertungen zu statistischen Zwecken vornehmen zu können.

Optimal ist es, wenn die datenbearbeitende Stelle die gewünschten Auswertungen gleich selber vornimmt und der anderen Verwaltungsstelle nur die anonymisierten statistischen Angaben liefert.

Ist dies – etwa aus technischen Gründen – nicht möglich, so sind nur die unbedingt erforderlichen Daten zu übermitteln. Im Weiteren hat sich die Verwaltungsstelle zu verpflichten, die Daten nach vorgenommenen Auswertungen umgehend zu löschen.

Eine ähnliche Situation findet sich auch sehr häufig beim Auslagern von Dienstleistungen im Informatikbereich. Zur Gewährleistung datenschutz- und datensicherheitsrechtlicher Aspekte muss in analoger Weise vorgegangen werden: minimaler Datenexport, genaue Instruktion, vertragliche Sicherung des Amtsgeheimnisses sowie entsprechende Kontrollfunktionen durch den Auftraggeber müssen vorgenommen werden.

1.8 Einwohnergemeinde

Fall 20 Bekanntgabe der «erweiterten Personalien»

Bei der Einwohnerkontrolle sind die einfachen Personalien⁶⁵ voraussetzungslos durch jedermann

64 Näheres dazu s. DSB TB 2004 S. 22 f. Fall Nr. 38.

65 Name, Vorname, Geschlecht, aktuelle Adresse [bei Wegzug mit Wegzugsdatum und Wegzugsort], Todestag.

erhältlich.⁶⁶ Die sogenannten «erweiterten Personalien» – Geburtsdatum, Zivilstand, Heimatort, Staatsangehörigkeit und Zuzugsort – kann die Einwohnerkontrolle bei Vorliegen eines *schriftlichen Gesuchs* bekannt geben, sofern ein *Interesse glaubhaft* gemacht wird und die Adresse *nicht gesperrt* ist.

Die Einwohnerkontrolle wollte vom DSB wissen, ob eine Firma das erforderliche Interesse glaubhaft gemacht habe, wenn sie ihrem Gesuch eine *Offerte* beilegt, um dadurch die erweiterten Personalien ihres möglichen zukünftigen Vertragspartners erhalten zu können.

Handelt es sich um eine *unverbindliche* Offerte⁶⁷, rechtfertigt dies grundsätzlich noch nicht die Bekanntgabe der erweiterten Personalien. Dies kann vor Vertragsabschluss noch vorgenommen werden. Dies umso eher, als die Einwohnerkontrolle in der Regel gleichentags Bescheid gibt.

Anders kann es sich dann verhalten, wenn die Ausarbeitung einer Offerte bereits sehr zeitaufwändig ist oder eine besondere terminliche Dringlichkeit gegeben ist.

Geht es hingegen um eine *verbindliche* Offerte, so ist die Bekanntgabe der erweiterten Personendaten bereits zu diesem Zeitpunkt zulässig.

Fazit: Da es sich beim fraglichen Fall um eine verbindliche Offerte handelte, zudem um ein längerfristiges, nicht alltägliches, betragsmässig nicht unbedeutendes Rechtsgeschäft, war das Interesse durch Vorlegen der Kopie der Offerte glaubhaft gemacht. Die erweiterten Personalien konnten hier durch die Einwohnerkontrolle bekannt gegeben werden.

Fall 21 Einsichtnahme in ein Baugesuch – nur unter Angabe der Personalien?

Grundsätzlich sind Baugesuche in der Gemeinde während 20 Tagen öffentlich aufzulegen.⁶⁸ Einsicht nehmen darf jedermann *voraussetzungslos*. Eine Gemeinde verlangte von denjenigen, die in Baugesuche Einsicht nehmen wollten, die Angabe der Personalien. Diese wurden in eine Liste eingetragen. Eine Privatperson wollte vom DSB wissen, ob dieses Vorgehen rechtmässig sei. Es sei offenbar schon vorgekommen, dass aufgrund dieser Liste Einsichtnehmende von der Gemeinde oder den Bauwilligen kontaktiert worden seien.

Weil das Baurecht die voraussetzungslose Einsichtnahme vorsieht und diese auch nicht näher regelt, muss dieser Anspruch *ohne Angaben der Personalien*, somit anonym, erfolgen können. Daraus folgt zudem, dass auch nicht Personen in einer Liste notiert werden dürfen, die dem Verwaltungspersonal namentlich bekannt sind. Die Abklärungen des DSB ergaben, dass die Gemeinde nicht «Fichen» von Einsichtnehmenden anlegen wollte. Vielmehr ging es darum, zu eruieren, in welchen Baugebieten Bauvorhaben für die Öffentlichkeit von Interesse seien. Der DSB empfahl der Gemeinde, zukünftig keine Personalangaben mehr zu verlangen – und diese Statistik anonym zu führen, somit in der Form einer schlichten «Strichliste». Die zuständige gemeindliche Verwaltung folgte dieser Empfehlung umgehend.

Fall 22 Muss die Bekanntgabe der «erweiterten Personalien» registriert werden?

Erhält jemand von der Einwohnerkontrolle die «erweiterten Personalien» eines Privaten,⁶⁹ so muss die Einwohnerkontrolle diese Datenbekanntgabe schriftlich festhalten, *unter Einschluss der Angabe der Personalien des Anfragenden*.⁷⁰ Hier verhält es sich somit gerade *anders* als im vorstehenden Fall. Denn der Gesetzgeber hat die Interessen der betroffenen Person, über die Daten durch die Gemeinde bekannt gegeben werden, in einer expliziten Gesetzesbestimmung⁷¹ *höher* gewichtet als die Anonymität des Anfragenden.⁷²

Fall 23 Alle Fahrzeughalterdaten an die Gemeinde?

Eine Gemeinde plante, das Nachtparkieren auf den öffentlichen Parkplätzen in der Gemeinde gebührenpflichtig zu machen. Sie erkundigte sich beim DSB, ob sie vom Strassenverkehrsamt die Angaben sämtlicher Fahrzeughalter mit Wohnsitz in der Gemeinde erhalten könne, um diese brieflich über die neue Rechtslage zu informieren.

Aus verschiedenen Gründen erschien dieser Informationskanal nicht ganz optimal: In der Gemeinde verfügen viele über einen eigenen Parkplatz, sind somit von der Neuerung gar nicht betroffen. Andererseits gibt es Personen, die nicht in der Gemeinde angemeldet sind, jedoch ihr Fahrzeug regelmässig über Nacht auf einem

66 § 8 Abs. 3 Bst. a Datenschutzgesetz.

67 Wenn der Offertsteller sein Angebot etwa als «unverbindlich» bezeichnet [rechtlich handelt es sich dann um eine Aufforderung zur Einreichung einer Offerte, jedoch nicht um eine Offerte im Sinne des OR].

68 § 45 Planungs- und Baugesetz (PBG; BGS 721.111).

69 Gestützt auf § 8 Abs. 3 Bst. b Datenschutzgesetz; s. dazu auch den vorstehenden Fall Nr. 20.

70 Demgegenüber darf die Anfrage nach den einfachen Personalien [§ 8 Abs. 3 Bst. a Datenschutzgesetz] durch die Einwohnerkontrolle *nicht* registriert werden.

71 § 13 Abs. 1 Bst. c Datenschutzgesetz.

72 Verlangt hingegen jemand nur die einfachen Personalien, so darf diese Anfrage *nicht* registriert werden, da sie an jedermann *voraussetzungslos* und *ohne nähere gesetzliche Regelung* erteilt wird.

öffentlichen Parkplatz abstellen – diese Personen wären hingegen nicht informiert worden. Die Bekanntgabe sämtlicher Fahrzeughalterdaten seitens des Strassenverkehrsamtes an die Gemeinde müsste daher wohl als unverhältnismässig und somit als unzulässig beurteilt werden. Vermutlich auch sehr viel günstiger war dann der Weg, den die Gemeinde schliesslich einschlug: In Amtsblatt, Lokalblatt, Internet und bei diversen anderen Gelegenheiten wurde die Öffentlichkeit rechtzeitig über die zukünftige Gebührenpflicht des Nachtparkierens informiert. Anlässlich von ersten Kontrollen kann dann in einer Übergangsphase anstatt ein Bussenzettel ein Informationsblatt unter den Scheibenwischer gesteckt werden, damit auch wirklich alle Bescheid wissen.

Fazit: Der Datenbezug durch das Strassenverkehrsamt entfiel.

Fall 24 Einwohnerkontrolle verlangt bei Neuzuziehenden Angaben zu Beruf und Arbeitgeber

Der DSB hat bereits früher⁷³ darauf hingewiesen: Es gibt *keine* Rechtsgrundlagen, dass die Neuzuziehenden der Einwohnerkontrolle gegenüber bei der Anmeldung zwingend Angaben zu ihrem Beruf oder ihrem Arbeitgeber machen müssen. Schon gar nicht haben sie der Gemeinde ihre private Handynummer bekannt zu geben. Diese Fragen sind demnach *unzulässig*.

Will die Gemeinde solche Informationen auf der Basis der *Freiwilligkeit* erheben, so muss auf dem entsprechenden Formular klar und deutlich darauf hingewiesen werden, dass keinerlei Verpflichtung besteht, die entsprechenden Informationen bekannt zu geben.

1.9 Bürgergemeinde

Fall 25 Zur Datenbekanntgabe an die Bürgergemeindeversammlung

Wie bereits in früheren Jahren,⁷⁴ stellten sich erneut verschiedene Fragen im Zusammenhang mit dem Einbürgerungsverfahren.

In mehreren Fällen galt es abzuklären, ob die Bürgergemeindeversammlung die Gründe kennen muss, warum nicht sämtliche Mitglieder einer Familie ein Gesuch um Einbürgerung gestellt haben.

Das Datenschutzgesetz kommt auf die Datenbekanntgabe an die Bürgergemeindeversammlung anlässlich der Beratung *nicht* zur Anwendung.⁷⁵ Jedoch sind die allgemeinen Verfahrensgrundsätze zu beachten.

Will sich in einer Familie etwa der Mann und die Kinder, nicht jedoch die Ehefrau einbürgern, so sind nur Ehemann und Kinder Verfahrensbeteiligte. *Ihre* Gesuche sind somit abzuklären und zu beurteilen. Die Ehefrau hingegen ist nicht verfahrensbeteiligt, ist somit eine unbeteiligte Drittperson.

Fazit: Daten von Personen, die nicht am Verfahren beteiligt sind, sind der Bürgergemeindeversammlung *nicht* bekannt zu geben.

1.10 Kirchgemeinde

Fall 26 Dürfen Taufen, Hochzeiten oder Todesfälle im Pfarrblatt und im Internet veröffentlicht werden?

Im Tätigkeitsbericht 2004 wurde dargelegt,⁷⁶ dass eine Veröffentlichung dieser Zivilstandsfälle im *Amtsblatt* im Kanton Zug ohne die ausdrückliche Zustimmung der Betroffenen rechtlich *nicht* zulässig ist. Diese Rechtslage gilt auch für die Kirchgemeinden. Eine Veröffentlichung der besagten Ereignisse ist somit nur mit ausdrücklicher Zustimmung der betroffenen Personen – bei Todesfällen: der Angehörigen – erlaubt. Um Klarheit zu schaffen, sollte die Zustimmung *schriftlich* eingeholt werden.

Es ist darauf hinzuweisen, dass von einer Veröffentlichung *im Internet* grundsätzlich abzuraten ist. Im Internet veröffentlichte Informationen stehen bekanntlich weltweit und praktisch für die Ewigkeit zur Verfügung. Sie werden zudem von entsprechenden Unternehmen laufend kommerziell ausgewertet. Dies hat zur Folge, dass die betroffenen Personen in aller Regel mit einer zusätzlichen Werbeflut überschwemmt werden.

Fall 27 Darf das Kollektenergebnis von Beerdigungen im Pfarrblatt veröffentlicht werden?

Beerdigung von Ernst Muster-Müller⁷⁷, Fr. 934.– zugunsten der Lungenliga; Beerdigung von Max Muster-Meier, Fr. 213.25 zugunsten der Aids-hilfe Schweiz; Beerdigung von Frieda Muster,

73 Vgl. DSB TB 2001 S. 18 f. Fall Nr. 31.

74 Vgl. DSB TB 2004 S. 16 f. Fälle Nr. 22 und Nr. 23; DSB TB 2003 S. 16 f. Fälle Nr. 26–28; DSB TB 2002 S. 20 Fälle Nr. 35 und Nr. 36; DSB TB 2000 S. 22 Fall Nr. 24 und S. 27 Nr. 42.

75 § 3 Abs. 2 Bst. b DSG, vgl. dazu DSB TB 2003 S. 16.

76 S. DSB TB 2004 S. 12 Fall Nr. 8.

77 Die hier genannten Familiennamen sind frei erfunden.

Fr. 1'245.20 zugunsten der Tierhilfe – darf dies im Pfarrblatt stehen?

Vorweg: Auf die Bearbeitung von Personendaten durch die Kirchgemeinde ist das Zuger Datenschutzgesetz umfassend anwendbar.⁷⁸

An und für sich ist das Resultat einer Kollekte – als Summe von Einzelspenden von nicht näher bekannten Personen – grundsätzlich ein *Sachdatum*⁷⁹. Die Bearbeitung von Sachdaten unterliegt *nicht* dem Schutz des Datenschutzgesetzes. Nun ist aber zu beachten, dass durch die Verknüpfung des Ergebnisses der Kollekte mit einer ganz bestimmten Beerdigung ein direkter Bezug zur Familie und ihrem Umfeld – und in einem gewissen Sinn dadurch auch zum Verstorbenen – hergestellt wird, da Aussagen über die Spendenbereitschaft gemacht werden. Es geht hier zwar nicht um Daten einzelner, bestimmbarer Personen, weder bezüglich der Spender, noch bezüglich der Familie von Ernst Muster-Müller. Trotzdem muss sich doch jedes einzelne Familienmitglied des Verstorbenen diese Information über das Resultat der Kollekte zurechnen lassen.

Somit ist davon auszugehen, dass es sich um *Personendaten* bezüglich der jeweils betroffenen Familienangehörigen der Beerdigung handelt und dass durch die Publikation die Angehörigen in ihrer geschützten Privatsphäre tangiert sind. Das Datenschutzgesetz kommt somit hier zur Anwendung.

Die Kirchgemeinde darf die Resultate veröffentlichen, wenn diesbezüglich eine ausdrückliche gesetzliche Vorschrift dies vorsieht – was nicht gegeben ist –, die Betroffenen ausdrücklich zustimmen – was ebenfalls nicht gegeben ist – oder diese Publikation für die Erfüllung der kirchlichen Aufgaben *offensichtlich unentbehrlich* ist.

In einem derart heiklen Bereich wie dem vorliegenden müssten die Interessen der Kirchgemeinde die schutzwürdigen Interessen der betroffenen Privaten zudem *deutlich übertreffen*. Der Schutz der Privatsphäre der Trauerfamilien geht dem Interesse der Kirchgemeinde, das Kollektenwesen gewissermassen durch «Ankurbelung des Wettbewerbs» zu beleben, klar vor.

Nach dem Verlust eines Angehörigen möchten die Trauernden, insbesondere in kleinräumigen Verhältnissen, in einer solchen Publikation nicht noch als spendenunfreudig oder gar als

knauserig abqualifiziert werden. Zudem ist ja zu bedenken, dass die Trauerfamilien das Resultat nur dadurch positiv beeinflussen können, indem sie selber grosszügig spenden.

Die Trauernden somit indirekt zu einer grosszügigen Spende zu zwingen, kann aber auch nicht wirklich im Interesse der Kirchgemeinde sein, liegt es doch in der Natur einer Spende, dass sie freiwillig geleistet wird.

Ohne weiteres zulässig ist dagegen die Publikation der monatlichen Spendeneingänge insgesamt, da kein Bezug mehr zum jeweiligen Anlass gemacht werden kann.

Die Kirchgemeinde stellte in der Folge die Publikation der Resultate von Kollektenspenden von namentlich aufgeführten Beerdigungen ein.

78 § 2 Bst. h DSG.

79 Sachdaten sind Daten, die sich nicht auf eine bestimmte oder bestimmbare Person beziehen. Etwa: die Temperatur des Zugersees, der Gehalt von Feinstaub in der Luft, statistische Angaben etc.

2. Unsere Öffentlichkeitsarbeit

2.1 Zuger Datenschutz im Internet

Informationen werden heute in erster Linie via Internet verbreitet. Das ist auch beim Zuger Datenschutz nicht anders. Auf unserer Homepage «www.datenschutz-zug.ch» finden Sie alle wichtigen Informationen zu Datenschutz und Datensicherheit. Der Inhalt wird in der Regel alle zwei Wochen aktualisiert.

Wie wird unser Internet-Angebot genutzt? Hier die Besucherstatistik

Die bereinigte⁸⁰ Statistik zeigt, dass täglich durchschnittlich 48 einzelne Personen aus der Schweiz die DSB-Website während etwa 5 Minuten besuchen. Die Nutzung der Seiten hält sich insgesamt etwa im letztjährigen Rahmen.

Auf der DSB-Website stehen viele wichtige Dokumente zur Verfügung. Wir haben ermittelt, welche Dokumente wie oft heruntergeladen wurden. Hier die ersten zehn Plätze unserer «Hitparade»:

| Anzahl Downloads | |
|------------------|--|
| 4'616 | Tätigkeitsbericht 2000 [gedruckte Exemplare: 3'000] |
| 3'120 | Tätigkeitsbericht 2004 [gedruckte Exemplare: 3'000] |
| 2'719 | DSB in der «Zuger Gerichts- und Verwaltungspraxis/GVP 2002» [gedruckte Exemplare: 700] |
| 2'443 | Tätigkeitsbericht 2003 [gedruckte Exemplare: 3'000] |
| 1'748 | Tätigkeitsbericht 2002 [gedruckte Exemplare: 3'000] |
| 943 | Leitfaden «Datenschutz in der Schule» |
| 926 | Tätigkeitsbericht 1999 [gedruckte Exemplare: 2'000] |
| 717 | Information des Eidg. DSB «Internetüberwachung am Arbeitsplatz» |
| 598 | Botschaft zum Bundesgesetz über den Datenschutz [DSG] vom 23. März 1988 |
| 595 | DSB in der «Zuger Gerichts- und Verwaltungspraxis/GVP 2001» [gedruckte Exemplare: 700] |

Die Summe der PDF-Downloads der ersten zehn Plätze hat im Vergleich zum Vorjahr *um etwa 40%* zugenommen.

Fazit: Das DSB-Informationsangebot wird in der Datenflut des Internets wahrgenommen und von interessierten Kreisen häufig konsultiert. Nicht unbedeutend ist insbesondere das Herunterladen von Publikationen des DSB. Informiert sich die Öffentlichkeit selbständig, reduziert sich für den DSB der Beratungsaufwand. Das Angebot des DSB im Internet stellt somit insgesamt für die Bevölkerung eine nützliche, kostenlose und effiziente Dienstleistung dar.

2.2 Elektronischer Newsletter des Datenschutzbeauftragten

Das Konzept des Internet-Auftritts sieht seit Juni 2000 wie folgt aus: Alle grundlegenden Informationen werden auf der Homepage veröffentlicht.⁸¹ Alle *aktuellen* Informationen aus den Bereichen Datenschutz und Datensicherheit werden hingegen *per E-Mail* in der Form von Kurzhinweisen – versehen mit Links auf Fundstellen, wo sich ausführliche Informationen finden – verschickt.⁸² Diese Dienstleistung kann auf einfachste Weise in Anspruch genommen werden. Es genügt, wenn Sie sich auf der entsprechenden Seite der DSB-Website⁸³ mit ihrer E-Mail-Adresse einschreiben. Wenn Sie übrigens keine Nachrichten mehr erhalten möchten, können Sie sich ebenso einfach selber wieder aus der Liste austragen.

Hier das Wichtigste in Kürze:

Häufigkeit des Nachrichtenversandes

Pro Woche werden per E-Mail 1 bis 3 Kurznachrichten verschickt.

Archiv der verschickten Nachrichten

Sämtliche verschickten Nachrichten sind in einer Archiv-Datenbank gespeichert [z. T. mit zusätzlichen PDF-Dokumenten versehen]. Diese Datenbank ist via Website auch für nicht eingeschriebene Personen zugänglich. Das Archiv verfügt über eine sehr effiziente Suchmaschine.

Ende 2005 befanden sich rund 690 Nachrichten im Archiv.

Besucherstatistik 2005

Täglich besuchen mehr als 120 Personen das Archiv. Im Vergleich zum Vorjahr ist das eine *Verdoppelung*. Dabei werden pro Besucher etwa 2 bis 3 Seiten konsultiert und täglich rund 10 Archiv-Dokumente heruntergeladen.

Zuwachs der Abonnenten 2005

+ 95 Neuabonnenten.

80 Statistische Auswertungen der Internetnutzung sind grundsätzlich mit grosser Vorsicht zu geniessen – s. dazu die ausführlichen Hinweise im Tätigkeitsbericht des letzten Jahres: DSB TB 2004 S. 23 Ziff. 2.1.

81 Insbesondere Gesetze, Merkblätter, Broschüren, Literatur, Adressen und Links.

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

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

Versickte Nachrichten 2005

57 per E-Mail versickte Nachrichten.

Abo-Kosten

Keine.

Fazit

Schreiben auch Sie sich ein – es lohnt sich!

2.3 Tätigkeitsbericht 2004

Der Tätigkeitsbericht will die Themen Datenschutz und Datensicherheit praxisnah und verständlich einem *breiten Publikum* vorstellen. Er soll insbesondere die Mitarbeitenden der Verwaltung bezüglich Datenschutz sensibilisieren und auch ein Stück weit ausbilden. Deshalb wurde der Tätigkeitsbericht mit der Personalzeitschrift an alle kantonalen Mitarbeitenden, an die Gemeinden, an die Medien sowie an zusätzliche interessierte Stellen verschickt. Es gingen auch sehr viele Bestellungen von Privatpersonen und Unternehmen ein. Von der Auflage (3'000 Expl.) war nach kurzer Zeit nur noch ein kleiner Restbestand vorhanden. Es hat sich erneut klar gezeigt, dass sehr viele Personen den gedruckten Tätigkeitsbericht für ihre Arbeit benützen und diesen dafür als *viel geeigneter und ansprechender* beurteilen als das Herunterladen des Berichts aus dem Internet. Der gedruckte Tätigkeitsbericht und das PDF-Dokument ergänzen sich und stellen – je nach Zielgruppe – beide eine nützliche Arbeitshilfe dar.

Wer die früheren Tätigkeitsberichte zu Rate ziehen möchte, kann sie beim DSB kostenlos bestellen oder sich auf der DSB-Website⁸⁴ eine layoutgetreue Kopie ausdrucken.

2.4 «Gerichts- und Verwaltungspraxis des Kantons Zug» [GVP]

Die «Gerichts- und Verwaltungspraxis des Kantons Zug» [GVP] ist die amtliche Zuger Publikation, die einen umfassenden Einblick in die Rechtsprechung der Zuger Gerichte und der kantonalen Verwaltung gibt. Zielpublikum ist ein juristisch interessiertes Fachpublikum. GVP erscheint jährlich in einer Auflage von 700 Exemplaren.⁸⁵

Der DSB veröffentlichte in GVP 2004⁸⁶ fünf exemplarische Stellungnahmen aus seiner Beratungstätigkeit.

Die Beiträge des DSB in GVP der Jahre 2000–2004 können layoutgetreu (und kostenlos) von der DSB-Website heruntergeladen werden.

2.5 Medienarbeit

Das Thema Datenschutz war verschiedentlich in den Medien. So berichteten die Zuger Printmedien und Lokalradios etwa über die Veröffentlichung des DSB-Tätigkeitsberichts 2004, über Datenschutzrechtliches bezüglich Ahnenforschung sowie im Zusammenhang mit Aktuellem aus Gesetzgebung und Politik.

Über den Tätigkeitsbericht wurde auch in drei deutschen Fachpublikation berichtet.⁸⁷

Verschiedene Medien wünschten eine Stellungnahme des DSB im Zusammenhang mit aktuellen Berichterstattungen [etwa: «Blick-online», «Kommunalmagazin», «KMU-Magazin», «plädoyer»].

Der DSB verfasste im weiteren Beiträge für Fachzeitschriften.⁸⁸

Übrigens: Erfreulicherweise bestand für die Medien im Berichtsjahr kein Anlass, über gravierende datenschutzrechtliche Vorfälle oder gar Skandale zu berichten.

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

85 Die gedruckte Version kann bei der Staatskanzlei zum Preis von Fr. 30.– bezogen werden.

86 GVP 2004 S. 277–290.

87 Datenschutz und Datensicherheit/DuD, 2005/Heft 5, S. 308; IT-Spektrum, Heft 5/Oktober 2005, S. 449; Mitteilung des «Virtuellen Datenschutzbüros».

88 «digma» 2005/Heft 4, S. 192–195; IT-Spektrum, Heft 5/Oktober 2005, S. 449.

3. Mitarbeit bei der Gesetzgebung

Die Mitarbeit bei der Gesetzgebung ist für den Datenschutzbeauftragten *zentral*. Werden die Grundsätze von Datenschutz und Datensicherheit in neuen Rechtserlassen korrekt integriert, entstehen später bei der Anwendung in der Praxis im Idealfall keine, jedenfalls bestimmt weniger Konflikte.

Wichtig ist daher, dass die Verwaltungsstellen den Datenschutzbeauftragten in einem *möglichst frühen Verfahrensstadium* einbeziehen – bevor Regelungen und Verfahrensabläufe in Stein gemeisselt sind. Wird der DSB dagegen zu einem späten Zeitpunkt einbezogen, ist es meist aufwändiger, nachträglich Datenschutz und Datensicherheit systematisch und konsequent in eine Vorlage zu integrieren. Zudem ergeben sich in diesem Fall immer *zeitliche Verzögerungen*.

Es darf hier erfreulicherweise vermerkt werden, dass der Einbezug des Datenschutzbeauftragten bei der Gesetzgebung unterdessen weitgehend eine Selbstverständlichkeit ist. Dies trifft insbesondere auf den Regierungsrat, aber auch auf die übrigen mit der Vorbereitung von Rechtserlassen zuständigen Verwaltungsstellen zu.

3.1 Datenschutzgesetz

Der Regierungsrat hat dem Kantonsrat im Berichtsjahr folgende Änderung des Datenschutzgesetzes vorgeschlagen: Die Einwohnerkontrolle soll bei Sammelauskünften neu auch das Geburtsjahr der Bürgerinnen und Bürger bekannt geben müssen. Der DSB war *gegen* diese Änderung, hat es sich doch gezeigt, dass die Privaten es nicht schätzen, wenn ihre Altersangaben an Dritte weitergegeben werden.⁸⁹ Dem DSB wurde umfassend Gelegenheit geboten, seine Vorbehalte gegenüber dieser DSG-Änderung anlässlich der kantonsrätlichen Kommissions-sitzung darzulegen. Die Kommission folgte jedoch der Vorlage des Regierungsrates. Der Kantonsrat hat anlässlich der ersten Lesung⁹⁰ Folgendes beschlossen: Bei Sammelauskünften ist nicht nur das Geburtsjahr, sondern auch das *Geburtsdatum* bekannt zu geben; zudem müssen neu auf Verlangen auch Listen der in der Gemeinde *Neuzugezogenen* abgegeben werden. Die Sammelauskünfte muss die Gemeinde im Weiteren auf Wunsch auch in *elektronischer Form* zur Verfügung stellen.

Der Kantonsrat hat insgesamt somit die Interessen der Institutionen an Sammelauskünften höher gewichtet als die Interessen der Einwohnerinnen und Einwohner auf Nichtweitergabe ihrer Daten an Dritte. Im Sinne eines Interessenausgleichs hat der Rat aber – wie auch schon die kantonsrätliche Kommission – den DSB darauf hingewiesen,⁹¹ die Bevölkerung aktiver über das ihr zustehende Sperrrecht⁹² zu informieren, werden doch gesperrte Adressen im Rahmen von Sammelauskünften *nicht* an Dritte weitergegeben.

Die zweite Lesung findet im Jahr 2006 statt. Über den Abschluss dieser DSG-Revision wird hier zu berichten sein – im elektronischen Newsletter⁹³ wird umgehend über Aktuelles informiert.

3.2 Datensicherheits- und Online-Verordnung

Hinweise zum aktuellen Stand dieser Projekte finden Sie vorne im Abschnitt «Datensicherheit in der kantonalen Informatik».⁹⁴

3.3 Polizeigesetz

Das Zuger Polizeigesetz⁹⁵ soll einer Totalrevision unterzogen werden. Dieses Gesetzesprojekt hat eine bedeutende datenschutzrechtliche Relevanz: Welche Daten dürfen durch die Polizei wie erhoben werden? Ist die Weitergabe von Daten zulässig? Gegebenenfalls: An wen? Wie sieht die Archivierung aus? Wann werden Polizeidaten gelöscht?

Der Regierungsrat wird die Vorlage im Jahr 2006 in zweiter Lesung beraten, anschliessend ist vorgesehen, dem Kantonsrat den Entwurf vorzulegen. Wir werden an dieser Stelle im nächsten DSB-Tätigkeitsbericht⁹⁶ darüber berichten.

3.4 Vernehmlassungen

Falls Sie sich für die ausführlichen Stellungnahmen des Datenschutzbeauftragten bezüglich der unten stehenden Rechtserlasse interessieren, wenden Sie sich an den DSB. Er wird sie Ihnen gerne zustellen.

Bundesrecht

Der DSB hat zu folgenden Vorlagen im Rahmen von *Mitberichtsverfahren* Stellung genommen. Der Regierungsrat hat die Hinweise des DSB

89 S. dazu die Hinweise im letztjährigen Tätigkeitsbericht: DSB TB 2004 S. 26/27.

90 Sitzung vom 27. Oktober 2005, Vorlage 1322.4 [Laufnummer 11848].

91 Vgl. das Protokoll der 51. Sitzung vom 27. Oktober 2005, S. 1471 und S. 1472.

92 § 9 Abs. 1 und Abs. 2 Datenschutzgesetz lauten:
«¹ Eine betroffene Person kann voraussetzungslos vom Organ verlangen, dass Daten nur an Organe bekannt gegeben werden dürfen.
² Die Sperrung wird nach Eintreffen des Gesuches sofort wirksam. Das Gesuch muss schriftlich erfolgen und sich auf bestimmte zu sperrende Datensammlungen beziehen. Die Sperrung ist schriftlich zu bestätigen.»

93 Hinweise zur dieser Dienstleistung s. vorne S. 19.

94 Kapitel I Ziff. 4, S. 6.

95 Gesetz über die Kantonspolizei (BGS 512.11).

96 Aktuelles wird zudem umgehend im elektronischen Newsletter des DSB vermeldet werden.

jeweils vollständig [beziehungsweise weitestgehend] in seine Vernehmlassung gegenüber dem Bund integriert.

- *Parlamentarische Initiative betr. Änderung des Bundesgesetzes über Erwerb und Verlust des Schweizer Bürgerrechts* [Bürgerrechtsgesetz, BüG]

Der Datenschutzbeauftragte empfahl, die Datenbearbeitung im Einbürgerungsverfahren im Bundesrecht klar und abschliessend zu definieren, somit den Kantonen diesbezüglich einheitliche Vorgaben zu machen. Zudem soll ausdrücklich ausgeschlossen werden, dass die vorgegebenen Datenerhebungen mittels «freiwilliger» Zustimmung Betroffener umgangen werden können.

- *Bundesgesetz über die polizeilichen Informationssysteme des Bundes*
Der Bund plant die Einführung eines nationalen «Polizei-Indexes». Darunter ist ein gesamtschweizerisches polizeiliches Personendaten-system zu verstehen.
- *Bundesgesetz über die Ausweise für Schweizer Staatsangehörige* [sowie der diesbezüglichen Verordnung]
Schwerpunkt der Gesetzesänderung: Einführung des biometrischen Reisepasses. Der Datenschutzbeauftragte wies auf verschiedene heikle Punkte hin, insbesondere bezüglich den technischen Aspekten dieses Vorhabens.
- *Bundesgesetz über die eingetragene Partnerschaft gleichgeschlechtlicher Paare*
Hier stellte sich die Frage nach dem Anpassungsbedarf im kantonalen Recht.
- *Bundesgesetz über Massnahmen gegen Gewaltpropaganda und Gewalt anlässlich von Sportveranstaltungen.*

Kantonales Recht

Im Berichtsjahr hat der DSB insbesondere zu folgenden Vorlagen Stellung genommen:

- «2. Paket der Zuger Finanz- und Aufgabenreform / ZFA»
Im Rahmen der ZFA wird eine ganze Reihe kantonalen Rechtserlasse geändert. Die Empfehlungen des DSB wurden grundsätzlich alle berücksichtigt.

- *Änderung des Steuergesetzes*

Der wichtige Hinweis des DSB, keine Online-Zugriffe durch Dritte auf Datenbanken der Steuerverwaltung zuzulassen, wurde – unverständlicherweise – nicht berücksichtigt.⁹⁷

- *Teilrevision Sozialhilfegesetz*

Das SHG regelt viele heikle Datenbearbeitungen. Der DSB hat verschiedene Ergänzungen und Präzisierungen vorgeschlagen, die nur teilweise berücksichtigt wurden.

- *Erläss betr. Verzicht auf die Veröffentlichung von Grundbuchdaten bei Handänderungen an Grundstücken*

Aufgrund der Änderung des entsprechenden Bundesrechts haben die Kantone neu die Kompetenz erhalten, selber zu bestimmen, ob Handänderungen an Grundstücken wie bis anhin im Amtsblatt zu veröffentlichen sind. Der DSB hat sich klar gegen die Publikation solcher Informationen ausgesprochen. Der Regierungsrat scheint diese Auffassung grundsätzlich zu teilen, hat aber im Berichtsjahr noch nicht definitiv über das weitere Vorgehen in dieser Angelegenheit entschieden.

- *Reglement über die Führung des Personaldossiers*
Personalunterlagen enthalten oft viele besonders schützenswerte Daten von Mitarbeitenden. Zu denken ist an Gesundheitsdaten, Gutachten, Referenzen, Qualifikationen, Auswertung von Assessments oder Handschriftenproben etc. Der Regierungsrat will deshalb die Führung von Personalunterlagen umfassend regeln: von der Eröffnung eines Dossiers bei Stellenbewerbenden bis zur allfälligen Übergabe von Personalunterlagen an das Staatsarchiv. Der DSB hat eine ganze Reihe von Empfehlungen abgegeben. Das Geschäft ist bei Drucklegung des vorliegenden Berichts noch nicht verabschiedet.
- *Regierungsratsbeschluss betr. Rauchverbot in der kantonalen Verwaltung*
- *Verordnung über die amtliche Vermessung*
Die Hinweise des DSB bezüglich dieser Verordnung und der beiden folgenden Erlasse wurden berücksichtigt.
- *Totalrevision des Gesetzes über den Gebährentarif im Grundbuchwesen*
- *Revision des Beurkundungsgesetzes*

97 Betr. § 110bis Abs. 2 Satz 2 Steuergesetz [StG, BGS 632.1].

4. Register der Datensammlungen

Grundsätzliches

Die Organe des Kantons und der Gemeinden sind verpflichtet, ein Register ihrer Datensammlungen zu führen.⁹⁸ Dies schafft Transparenz, weil dadurch für jedermann ersichtlich ist, welche Daten bei welcher Verwaltungsstelle bearbeitet werden. Das Register ist denn auch *die notwendige Grundlage für das Einsichtsrecht*⁹⁹: Wer Einsicht in seine eigenen Daten erhalten möchte, erfährt im Register, welche Datensammlungen überhaupt vorhanden sind, welchen Inhalt sie grundsätzlich haben und bei welcher Verwaltungsstelle man sich melden muss, um Einsicht in die eigenen Daten zu nehmen.

Das Register dient aber auch den Organen des Kantons und der Gemeinden. Diese erhalten einen besseren Überblick über die bei ihnen vorhandenen Datensammlungen und auch über die Datenflüsse zwischen den Verwaltungsstellen. Das Register bietet zudem die Möglichkeit, kritisch zu überprüfen, ob die vorhandenen Datensammlungen zu Recht geführt werden, inhaltlich in Ordnung und sachlich erforderlich sind.

Das Register selbst enthält *keinerlei Personendaten*. Ersichtlich ist nur, unter welcher Bezeichnung eine Verwaltungsstelle eine Datensammlung führt und welche *Art* von Daten vorhanden sind.

Zuständigkeiten und Projektleitung

Die Datenschutzstelle ist zuständig für das Register der Datensammlungen kantonaler Verwaltungsstellen. Die Gemeinden¹⁰⁰ führen ihre Register gemäss Datenschutzgesetz selber.¹⁰¹ Um die Einheitlichkeit des Registers bei Kanton und Gemeinden zu ermöglichen, führt und betreut die Datenschutzstelle [zurzeit] auch das Register der gemeindlichen Datensammlungen.

Bei der Datenschutzstelle ist Rechtsanwalt Lothar Sidler für alle Fragen rund um das Register zuständig.

Die Verwaltungsstellen sind für Richtigkeit, Vollständigkeit und Aktualisierung ihres Registers verantwortlich.

Stand des Projekts:

1'328 Zuger Datensammlungen!

Ende 2005 umfasste das Register 313 Datensammlungen [im Folgenden DS] der kantonalen Verwaltung, 895 DS von Einwohnergemeinden, 112 DS von Bürgergemeinden, 6 DS einer Korporationsgemeinde sowie 2 DS von externen Beauftragten. Insgesamt sind somit *1'328 Zuger Datensammlungen* registriert.

Die Datensammlungen der Kirch- und Korporationsgemeinden sind noch nicht vollständig erhoben.

Das Register ist im Internet auf der Homepage des DSB online verfügbar.¹⁰² Es stehen sehr effiziente Suchhilfen zur Verfügung. Seit Dezember 2004 haben die Gemeinden die Möglichkeit, ihren Registerbereich in ihren eigenen gemeindlichen Web-Auftritt zu integrieren.

Wie oft wird das Register im Internet konsultiert?

Die anonymisiert vorgenommene statistische Auswertung der Besuchenden¹⁰³ zeigt Folgendes:

| | 2005 | 2004 |
|--|--------------|------------|
| Monatliche Besuche | 120 bis 220 | 25 bis 190 |
| Anzahl der konsultierten Seiten pro Besucher | 5 | 9 |
| Verweildauer im Register | 2 bis 3 Min. | 5 Min. |

Viele Besucher tätigten mehrmals Abfragen im Register. Im Vergleich zum Vorjahr¹⁰⁴ ist somit insgesamt eine *Zunahme* der Nutzung des Registers im Internet festzustellen.

Die Zahlen machen deutlich, dass Bevölkerung und Verwaltungsstellen ein *erhebliches* Interesse am Register zeigen.

Ausblick

Die Umverteilung von Aufgaben und Kompetenzen zwischen Bund, Kanton und Gemeinden, aber auch kantons- und gemeindeinterne Neuorganisationen führen zu Änderungen der rechtlichen Grundlagen, des Inhalts von und der Zuständigkeit für Datensammlungen. Der Aufwand für die *Aktualisierung* der Datensammlungen dürfte daher auch nach Abschluss der Erfassungsarbeiten nicht unerheblich ausfallen.

98 § 12 Datenschutzgesetz [sowie zur Umsetzungsfrist § 26 Abs. 1 DSG]. Ausgenommen von der Registrierungspflicht sind gemäss § 12 Abs. 2 DSG Datensammlungen, die nur bis maximal sechs Monate geführt werden und Hilfsdatensammlungen. Ebenfalls nicht in das Register aufgenommen werden Datensammlungen, die keine Personendaten, sondern ausschliesslich *Sachdaten* beinhalten.

99 § 13 Datenschutzgesetz.

100 Einwohnergemeinden, Bürgergemeinden, Kirchgemeinden sowie Korporationsgemeinden.

101 § 12 Abs. 5 bzw. § 19 Abs. 1 Bst. i Datenschutzgesetz.

102 «www.datenschutz-zug.ch», Rubrik «Register der Datensammlungen».

103 Besuche, die nicht berücksichtigt wurden: DSB-Administrationszugriffe, Suchmaschinen, «Web-Crawlers», Besuche aus fremen Ländern oder zu Nachtzeiten etc.

104 Vgl. die zusätzlichen Hinweise im DSB TB 2004 S. 28 f.

5. Weiterbildung

5.1 Unser Weiterbildungsangebot

«Die Zuger Verwaltung kennen lernen»

Die Zuger Verwaltung als Arbeitgeberin macht neue Mitarbeitende im Rahmen einer obligatorischen eintägigen Veranstaltung mit ihren Strukturen und ihrer «Philosophie» bekannt. Das Personalamt führt diese Veranstaltung zweibis dreimal pro Jahr durch. Es nehmen jeweils etwa 30 bis 40 Personen teil. Die Datenschutzstelle informiert im Rahmen dieser Veranstaltung kurz über die Grundlagen von Datenschutz und Datensicherheit und über die zentralen Rechte und Pflichten der Mitarbeitenden. Das Ziel einer solchen Veranstaltung kann nicht in der Ausbildung in Datenschutz und Datensicherheit bestehen. Wichtig ist vielmehr, dass die neuen Mitarbeitenden aller Stufen einen ersten persönlichen Kontakt mit den Mitarbeitern der Datenschutzstelle haben und wissen, welche Dienstleistungen die Datenschutzstelle anbietet, um bei Bedarf Hilfe erhalten zu können.

«Schulrecht und Datenschutz – das müssen Sie wissen!»

So lautete der Titel eines Weiterbildungskurses für Lehrpersonen aller Stufen, der durch das «Didaktisches Zentrum Zug» an drei Abenden durchgeführt wurde. Schulrecht und Datenschutz – die beiden Rechtsbereiche wurden gemeinsam angeboten, weil sie viel miteinander zu tun haben.

Am ersten Abend präsentierte Dr. iur. Hanspeter Büchler [Direktionssekretär der DBK] aktuelle Probleme aus dem Schulrecht, am zweiten Abend stellte der DSB die wichtigsten Grundlagen von Datenschutz und Datensicherheit vor und diskutierte die Fragen des Plenums. Am dritten Abend gingen die beiden Referenten noch vertiefter auf praxisbezogene Fragen aus Schulrecht und Datenschutz ein.

Nachdem beim DSB in diesem Jahr eine rekordverdächtige Anzahl von Anfragen aus dem Schulbereich einging, war es nicht erstaunlich, dass der Kurs nicht nur ausgebucht, sondern sogar überbucht war, gingen doch über 30 Anmeldungen ein. Voraussichtlich wird deshalb auch in Zukunft eine solche Veranstaltungsreihe für Lehrpersonen angeboten.

Datenschutzkurs für die Gemeindeverwaltung

Von den beiden Gemeinden Menzingen und Walchwil kam je eine Anfrage auf Durchführung eines Datenschutzkurses für die Verwaltungsmitarbeitenden. Die Datenschutzstelle stellte deshalb im Rahmen einer je halbtägigen Weiterbildungsveranstaltung das Wichtigste aus Datenschutz und Datensicherheit vor und besprach mit den Mitarbeitenden deren Fragen aus der Praxis. Die Erfahrung hat gezeigt, dass im Rahmen eines Nachmittags aus zeitlichen Gründen auf viele Fragen nicht eingegangen werden kann. Der DSB steht deshalb den Gemeinden gerne auch für spätere «follow-up»-Veranstaltungen zur Verfügung. Wenn die Grundlagen bereits vermittelt sind, steht die ganze Kurszeit von zwei Stunden für Beantwortung und Diskussion aktueller Fragen zur Verfügung. Solche Veranstaltungen sind hoffentlich gewinnbringend für die Teilnehmenden – der Einblick in die Verwaltungspraxis und der Gedankenaustausch mit ihnen ist aber auch für den DSB stets sehr wichtig und wertvoll.

«Der gläserne Mensch»

Die Frauenzentrale Zug veranstaltete am «Internationalen Tag der Frau» eine spannende Abendveranstaltung zum Thema «Der gläserne Mensch», zu der auch der DSB eingeladen war, sich im Rahmen einer kurzen Präsentation und der anschliessenden Podiums- und Publikumsdiskussion zu äussern.

Präsentationen und Kurz-Veranstaltungen

Der DSB stand auch in diesem Jahre zahlreichen Stellen und Institutionen für die Präsentation von Datenschutzgrundlagen zur Verfügung.

5.2 Auch der Datenschutzbeauftragte muss sich weiterbilden

Teilnahme an Veranstaltungen im IT-Bereich

Datenschutz hat einen immer enger werdenden Bezug zur Informationstechnologie. Und diese entwickelt sich ununterbrochen weiter und macht damit auch dem Schutz der Privatsphäre Vorgaben. Für den DSB ist es darum wichtig, über technische Entwicklungen und Tendenzen

im Bild zu sein. Er nahm deshalb in diesem Jahr an verschiedenen wichtigen Konferenzen und Kursen im Bereich Informations-/Informatik-technologie teil.

Internationale Konferenzen

Die Schweiz ist im Bereiche des Datenschutzes nicht führend. Datenschutz und Datensicherheit werden international diskutiert, entwickelt und entschieden. Der DSB muss deshalb im Bild sein, was insbesondere in Europa, aber auch weltweit passiert. Um einen Einblick in das aktuelle Geschehen zu erhalten, bieten internationale Treffen ideale Möglichkeiten. Welche Tendenzen sind absehbar? Welche Themen kommen durch internationale Vorgaben bald auch auf die Schweiz zu? Wie können wir uns vorbereiten? Was hat sich bereits in anderen Staaten bewährt, was nicht?

Neben Referaten, Workshops und Diskussionen geben stets auch Gespräche mit Kolleginnen und Kollegen im informellen Rahmen viele Anstösse für die tägliche Arbeit und auch die Möglichkeit, bei Bedarf unter dem Jahr auf ausländisches Fachwissen zurückgreifen zu können. Die Zuger Datenschutzstelle kann dadurch vom international vorhandenen Know-how profitieren. Das kommt auch direkt der Zuger Bevölkerung zugute.

[Hinweis: An den Konferenzen, die im Ausland stattfinden, nimmt der DSB jeweils in seiner Freizeit teil und kommt für Kosten und Spesen vollumfänglich selber auf.]

Konferenz der europäischen Datenschutzbeauftragten

Die europäischen DSB treffen sich jeweils einmal jährlich. Die polnische Datenschutzbeauftragte hat dieses Jahr die Konferenz am 25. und 26. April 2005 in Krakau durchgeführt. Teilgenommen haben gegen 90 Personen. Vertreten waren 32 Staaten, verschiedene europäische Gremien, Organisationen und Institutionen.

Aus den Themen:

- Auswirkung der EU-Datenschutzrichtlinie 95/46 auf den Datenschutz in der EU und in Drittstaaten?
- Bedeutung der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften auf die Anwendung der EU-Datenschutzrichtlinie?

- Wie ist der Datenschutz bei Datentransfer in Drittstaaten zu gewährleisten?
- Funktion und Bedeutung von betrieblichen Datenschutzbeauftragten?
- Sensibilisierung und Weiterbildung
- Welchen Datenschutz für Europa im «dritten Pfeiler»¹⁰⁵?

Internationale Konferenz der Datenschutzbeauftragten

27th International Conference on Privacy and Personal Data Protection: «The protection of personal data and privacy in a globalised world: A universal right respecting diversities»

Diesen Titel trug die internationale Konferenz der DSB, die durch den EDSB organisiert wurde. Sie fand vom 14. bis 16. September 2005 in Montreux statt. Teilgenommen haben Vertreterinnen und Vertreter von Datenschutzstellen aus über 40 Nationen sowie zahlreiche Personen aus den Bereichen Wirtschaft, Advokatur, Organisationen und Wissenschaft [insgesamt über 300 Anwesende].

Schwerpunkte:

- Ein einziges Datenschutzrecht weltweit – eine Utopie?
- Ist der Datenschutz im Hinblick auf die Wirtschaft zu vereinfachen?
- Zehn Jahre seit Verabschiedung der EU-Datenschutzrichtlinie 95/46 – Wo stehen wir? Wohin geht die Reise?
- Datenschutz und Terrorismusbekämpfung – unversöhnliche Gegensätze?

Durch die DSB wurden verschiedene Resolutionen beraten und verabschiedet. Besonders ist die «Erklärung von Montreux» zu erwähnen: Sie hat zum Ziel, auf internationaler Ebene ein *universelles Recht auf Datenschutz* zu etablieren. Konferenzprogramm, Referate und Resolutionen stehen Ihnen auf der Homepage der Konferenz zur Verfügung.¹⁰⁶

Ergänzender Hinweis: Der Zuger DSB hat zu dieser Konferenz ebenfalls inhaltliche Beiträge beigesteuert, Näheres s. hinten S. 26.

105 Die EU trifft Entscheidungen in drei unterschiedlichen «Politikbereichen», die als die drei «Pfeiler» der EU bezeichnet werden:

Der *erste Pfeiler* ist der «Gemeinschaftsbereich», der die meisten gemeinsamen Politikbereiche umfasst, in denen Entscheidungen im Rahmen der «Gemeinschaftsmethode» unter Beteiligung von Kommission, Parlament und Rat getroffen werden.

Der *zweite Pfeiler* ist die gemeinsame Aussen- und Sicherheitspolitik, bei der die Entscheidungen alleine vom Rat getroffen werden.

Der *dritte Pfeiler* ist die «Zusammenarbeit der Polizei- und Justizbehörden in Strafsachen», wo ebenfalls der Rat die Entscheidungen trifft. Im Rahmen des ersten Pfeilers fasst der Rat in der Regel Beschlüsse mit qualifizierter Mehrheit. Im Rahmen der anderen Pfeiler erfolgt der Ratsbeschluss einstimmig und kann daher durch das Veto eines Staates blockiert werden.

106 «www.privacyconference2005.org».

6. Zusammenarbeit mit dem Eidgenössischen und mit den kantonalen Datenschutzbeauftragten

Allgemeines

Die Datenschutzbeauftragten aller Kantone sind gemeinsam mit dem Eidgenössischen Datenschutzbeauftragten [EDSB] im Verein «DSB+CPD.CH» zusammengeschlossen.¹⁰⁷

Ziel ist die Bündelung der knappen Ressourcen.¹⁰⁸ Im Vordergrund der Zusammenarbeit stand im Berichtsjahr: Verfassen von Vernehmlassungen [Bundesgesetz über Massnahmen gegen Gewaltpropaganda und Gewalt anlässlich von Sportveranstaltungen; Einführung des biometrischen Passes] und Stellungnahmen [Erklärung zum Datenschutz im Gesundheits- und Sozialversicherungsbereich], Informationsaustausch, Weiterbildung sowie gemeinsames Auftreten gegenüber den Medien. Ein grosser Teil dieser Arbeit wurde von den jeweiligen Arbeitsgruppen geleistet.¹⁰⁹

Konferenzen der schweizerischen Datenschutzbeauftragten

Die Frühjahrskonferenz fand am 2. Juni 2005 in St. Gallen statt. Als Gastreferent machte Beat Rudin, Geschäftsführer der «Stiftung für Datenschutz und Informationssicherheit», Ausführungen zu den neuen Tendenzen des Datenschutzes im Gesundheits- und Sozialversicherungsbereich.

Am 10. November 2005 wurde das Herbstplenum in Fribourg durchgeführt. Durch die leitenden Verantwortlichen der Berner Kantonspolizei wurde dabei das «Violent Crime Linkage Analysis System / VICLAS» vorgestellt und diskutiert. Dieses polizeiliche Informationssystem soll durch eine weltweit standardisierte Datenerfassung die Klärungsrate von Gewaltverbrechen erhöhen. Es kann aber [u. a.] wegen der zeitlich unbeschränkten Speicherung von Informationen zu Konflikten mit Datenschutzanliegen kommen.

Diese Treffen dienen nicht nur der fachlichen Weiterbildung, sondern stärken auch den Informationsaustausch und die Vernetzung der kantonalen DSB untereinander.

«Montreux 2005»

Der Eidg. DSB führte vom 14. bis 16. September 2005 die «27. Internationale Konferenz der Datenschutzbeauftragten» in Montreux durch.¹¹⁰ Zur Vorbereitung dieser Konferenz wurde ein beratendes Gremium eingesetzt. Neben dem DSB ZH war auch der Zuger DSB in diesem «Comité consultatif» vertreten.

Der Zuger DSB organisierte und leitete zudem an dieser Konferenz das Panel «Die polizeiliche Zusammenarbeit im föderalen Staat». Da weltweit betrachtet die Mehrheit der Staaten zentralistisch organisiert sind, die Konferenz aber in der Schweiz stattfand, war es nahe liegend, das internationale Publikum mit Aspekten des Föderalismus vertraut zu machen.

Der Austausch von Daten im Bereiche der Polizei gestaltet sich in einem föderalen Staat grundsätzlich anders als im Zentralstaat: In der Schweiz liegt die Polizeihöheit schwergewichtig bei den Kantonen, in Deutschland bei den 16 Bundesländern. Ausgangspunkt für die Diskussion bildete die Präsentation der aktuellen Rechtslage in Deutschland und der Schweiz.

Die Rechtslage in Deutschland beleuchtete Dr. Thilo Weichert, Datenschutzbeauftragter Schleswig-Holsteins¹¹¹ in seinem Referat «Datenschutz bei föderaler Polizeikooperation in Deutschland – und in Europa». Auf die Rechtslage in der Schweiz ging Regierungsrat Hanspeter Uster mit seinen Ausführungen «Datenschutz und Polizeiarbeit: Fünf Thesen zur föderalen Zusammenarbeit aus der Sicht eines Kantons» ein.¹¹²

Referate und Diskussion haben aufgezeigt, dass der zunehmende Austausch von Polizeidaten zwischen den verschiedenen föderalen Stellen die Vorgänge für Betroffene und Datenschutzstellen je länger je intransparenter und damit unkontrollierbarer machen. Die europäische Dimension verstärkt diese Tendenz massiv. Nur durch das Zusammenspiel von technisch-organisatorischer Massnahmen, Aufsichtstätigkeit durch entsprechend ausgestattete Datenschutzstellen sowie parlamentarischer Gremien kann es gelingen, hier ein gewisses Gegengewicht zu schaffen.

In der Zeitschrift «digma»¹¹³ veröffentlichte der DSB einen Beitrag über die wichtigsten Erkenntnisse dieses Panels.

107 Näheres dazu finden Sie unter «www.dsb-cpd.ch».

108 Die Statuten führen die folgenden Zwecke des Zusammenschlusses an: den Anliegen des Datenschutzes im öffentlichen Bereich Nachdruck zu verschaffen, die Zusammenarbeit unter den Kantonen und mit dem Bund auf dem Gebiete des Datenschutzes im öffentlichen Bereich zu fördern, die Kompetenz der Mitglieder zu erhöhen, die Ressourcen der Mitglieder wirkungsvoller einzusetzen und Ansprechpartner für Behörden und die Öffentlichkeit zu sein.

109 Folgende Arbeitsgruppen sind zurzeit aktiv: «AG Gesundheit», «AG Einwohnerkontrolle» sowie «AG Innere Sicherheit».

110 Näheres dazu s. vorne S. 25.

111 Die korrekte Bezeichnung lautet: Landesbeauftragter für den Datenschutz Schleswig-Holsteins und Leiter des Unabhängigen Landes-zentrums für Datenschutz Schleswig-Holsteins [ULD].

112 Die beiden Referate sind auf der Homepage der Konferenz von Montreux veröffentlicht: «www.privacyconference2005.org».

113 S. «digma», Zeitschrift für Datenrecht und Informationssicherheit, 2005/Heft 4, S. 191–195.

7. Wir über uns

Allgemeines

Das Arbeitspensum von René Huber betrug im Berichtsjahr 70%, dasjenige von Rechtsanwalt lic. iur. Lothar Sidler 50%¹¹⁴.

Bereits seit sieben Jahren wird das DSB-Sekretariat durch Hildegard Steiner von der Staatskanzlei betreut.

der verfassten Stellungnahmen oder der geführten Telefongespräche sind nur beschränkt aussagekräftig. Denn je nach Komplexität kann der Arbeitsaufwand für ein einzelnes Geschäft zwischen 30 Minuten und 10 Stunden betragen. Hier deshalb eine Aufstellung der aufgewendeten Arbeitszeit nach thematischen Schwerpunkten:

Übersicht des Aufwandes für die verschiedenen Tätigkeitsbereiche

Die folgende Übersicht zeigt, wofür die Datenschutzstelle [René Huber/RH, Lothar Sidler/LS] ihre Arbeitszeit eingesetzt hat. Statistische Angaben wie Anzahl der behandelten Anfragen,

| Bereich | 2005* RH + LS | [2004] RH | [2003] RH | Hinweise | | | | | | | | | | | | |
|---|------------------|----------------|----------------|---|----------------------|------|--------|--------|-----------|-----|-------|-------|---------|-----|-------|-------|
| Beratung/Auskunft/Information | 49 % | [42 %] | [48 %] | Aufgeteilt nach: <table border="1"> <tr> <td>Kantonale Verwaltung</td> <td>38 %</td> <td>[32 %]</td> <td>[35 %]</td> </tr> <tr> <td>Gemeinden</td> <td>5 %</td> <td>[4 %]</td> <td>[7 %]</td> </tr> <tr> <td>Private</td> <td>6 %</td> <td>[6 %]</td> <td>[6 %]</td> </tr> </table> | Kantonale Verwaltung | 38 % | [32 %] | [35 %] | Gemeinden | 5 % | [4 %] | [7 %] | Private | 6 % | [6 %] | [6 %] |
| Kantonale Verwaltung | 38 % | [32 %] | [35 %] | | | | | | | | | | | | | |
| Gemeinden | 5 % | [4 %] | [7 %] | | | | | | | | | | | | | |
| Private | 6 % | [6 %] | [6 %] | | | | | | | | | | | | | |
| Ausbildungsangebote | 7 % | [5 %] | [6 %] | Für kantonale und gemeindliche Verwaltungen [Schulungen, Referate und Präsentationen etc.] | | | | | | | | | | | | |
| Betreuung grösserer Projekte | 18 % | [14 %] | [13 %] | Register Datensammlungen, Tätigkeitsbericht, Rechenschaftsbericht und Beitrag GVP | | | | | | | | | | | | |
| Öffentlichkeitsarbeit | 7 % | [10 %] | [11 %] | Homepage, Medienarbeit, elektronischer Newsletter | | | | | | | | | | | | |
| Begleitung «Schengen/Dublin»** | 2 % | – | – | | | | | | | | | | | | | |
| Zusammenarbeit mit Eidg. DSB und kantonalen DSB | 5 % | [4 %] | [3 %] | Informationsaustausch, Teilnahme an den Veranstaltungen des Vereins «DSB+CPD.CH», Begleitkomitee «Internat. Konferenz Montreux 2005» | | | | | | | | | | | | |
| Betriebsinterne Weiterbildung | 2 % | [2 %] | [3 %] | Tagungsbesuche [insbesondere im IT-Bereich] | | | | | | | | | | | | |
| Diverses | 12 % | [20 %]*** | [15 %] | Allg. Korrespondenz, Rechnungswesen, Personelles, Betreuung der eigenen EDV-Infrastruktur, Bibliothek, Besprechungen – soweit nicht direkt einzelnen Projekten zuweisbar | | | | | | | | | | | | |
| Total | 100 % | [100 %] | [100 %] | | | | | | | | | | | | | |

* In % der Arbeitszeit bezogen auf ein 120%-Pensum [RH: 70%; LS: 50%]

** Dieser Aufgabenbereich kam 2005 neu dazu.

*** 2004 ergab sich nicht unbedeutender Zusatzaufwand für die Neubesetzung der Mitarbeiterstelle.

114 Aufteilung: 45 % befristete Aushilfsstelle; 5 % unbefristetes Anstellungsverhältnis.

Dank!

Es ist nicht der Datenschutzbeauftragte, der den Datenschutz gewährleistet. Vielmehr tun dies die Mitarbeiterinnen und Mitarbeiter der Verwaltung des Kantons und der Gemeinden bei ihrer täglichen Arbeit. Sie sind dafür verantwortlich, dass mit den Daten der Zuger Bevölkerung rechtmässig umgegangen wird. Sie sorgen dafür, dass das verfassungsmässige Grundrecht auf Achtung der Privatsphäre respektiert wird. Der Datenschutzbeauftragte unterstützt sie dabei mit seinen Dienstleistungen.

Stellen sich konkrete Probleme, so muss mit allen Beteiligten nach rechtmässigen Lösungen gesucht werden. Nicht immer ist dies einfach. Der Datenschutzbeauftragte ist deshalb auf eine gute Zusammenarbeit angewiesen. Es darf hier festgestellt werden: Die Kooperation mit den Mitarbeiterinnen und Mitarbeitern der Verwaltung funktioniert. Sie ist offen, konstruktiv, effizient und angenehm. Dafür bedanke ich mich sehr herzlich bei sämtlichen Personen, mit denen ich im Berichtsjahr zusammenarbeiten durfte.

Ein ganz besonderer Dank geht zudem an ...

- *Landschreiber Tino Jorio*, der die Anliegen des Datenschutzes immer mit grossem Interesse verfolgt und stets als ein sehr engagierter, wacher, aber auch kritischer Gesprächspartner zur Verfügung steht;
- *nicht zuletzt auch an alle kritischen Geister*, die bereit waren, interessiert, konstruktiv und offen an gesetzeskonformen Lösungen mitzuarbeiten.
- *sämtliche Mitarbeitende*, die Input bei der Erstellung des Registers der Datensammlungen geleistet haben;
- *alle Mitarbeitenden der Staatskanzlei*, bei der die Datenschutzstelle Gastrecht hat. Wir schätzen nicht nur die tatkräftige Unterstützung im administrativen Bereich, sondern auch die angenehme und kollegiale Zusammenarbeit;
- *Hildegard Steiner* für die administrative und an alle Mitarbeiterinnen der Telefonzentrale für die «telefonische» Betreuung der Datenschutzstelle;
- *Lothar Sidler*, ohne dessen kompetente, tatkräftige und kollegiale Unterstützung als Mitarbeiter auf der Datenschutzstelle es nicht möglich gewesen wäre, alle Anfragen zu beantworten, Projekte zu betreuen und Aufgaben zu lösen, die sich uns im Jahr 2005 stellten;

| | | | |
|---|----|--|----|
| A | | L | |
| Ahnenforschung [Fall 17] | 14 | Lehrpersonen [Beachtung der Privatsphäre durch ~; Fall 7] | 11 |
| Amtsgeheimnis [zeitl. Dauer; Fall 4] | 10 | Leistungsvereinbarungen | 5 |
| Anzeigerstatter [Anspruch auf Anonymität? Fall 14] | 13 | M | |
| Archivierung [und Leistungsvereinbarung] | 6 | Mailing-Liste s. Newsletter des DSB | 19 |
| B | | Medienarbeit des DSB | 20 |
| Baugesuch [Registrierung der Einsichtnahme? Fall 21] | 16 | Montreux [Erklärung von ~] | 25 |
| Bürgergemeindeversammlung [Datenbekanntgabe an ~; Fall 25] | 17 | N | |
| C | | Neuzuzüger [Erhebung von Beruf und Arbeitgeber; Fall 24] | 17 |
| CH-Datenschutzbeauftragte [Zusammenarbeit] | 26 | Newsletter des DSB | 19 |
| D | | O | |
| Datenschutzbeauftragter s. Datenschutzstelle | | Online-Verordnung | 7 |
| Datenschutzgesetz [Änderung] | 21 | P | |
| Datenschutzstelle [Angaben zur ~] | 27 | Pfarrblatt [Publikation von Kollektenergebnis? Fall 27] | 17 |
| Datensicherheit [in der kant. Verwaltung] | 6 | Pfarrblatt [Publikation von Zivilstandsereignissen? Fall 26] | 17 |
| Datensicherheitsverordnung | 7 | Polizeigesetz [Totalrevision] | 21 |
| DNA-Probenahme [bei Jugendlichen; Fall 13] | 13 | R | |
| E | | Register der Datensammlungen [stat. Angaben zur Nutzung] | 23 |
| Einbürgerung [Datenbekanntgabe; Fall 25] | 17 | Registrierung [von Einsichtnahmen in Baugesuche? Fall 21] | 16 |
| Einsicht [in die eigenen Daten; Fall 1] | 9 | S | |
| E-Mail [Hinweise zur Verschlüsselung; Fall 8] | 11 | Schengen/Dublin [Auswirkungen auf DSB] | 4 |
| E-Mail [Weiterleitung; Fall 3] | 9 | Schule [Beachtung der Privatsphäre; Fall 7] | 11 |
| Erweiterte Personalien [Voraussetzungen der Bekanntgabe; Fall 20] | 15 | Schülerinnen und Schüler [zum Umfang ihrer Privatsphäre; Fall 6] | 11 |
| «eTax.zug» [Datensicherheit; Fall 18] | 15 | Schulfotograf [Fall 12] | 12 |
| F | | Sicherheitsüberprüfung [bei der kant. Informatik] | 6 |
| Fahrzeughalterdaten [Bekanntgabe an die Gemeinde? Fall 23] | 16 | T | |
| Forschung [Datenbekanntgabe an ~; Fall 15] | 14 | Tätigkeitsbericht 2004 des DSB | 20 |
| Forschung [Adressbekanntgabe für ~; Fall 16] | 14 | V | |
| Familienforschung [Fall 17] | 14 | Verein CH-DSB | 26 |
| Foto [von Mitarbeitenden im Internet? Fall 2] | 9 | Vernehmlassungen des DSB | 21 |
| G | | W | |
| Gerichts- und Verwaltungspraxis des Kantons Zug [GVV] | 20 | Weiterbildungsangebot des DSB | 24 |
| Gesetzgebung [Mitarbeit des DSB] | 21 | Z | |
| GVP [betr. DSB] | 20 | Zugriffsberechtigung [auf Schulservern; Fall 10] | 12 |
| H | | | |
| Homepage [betr. Schulen; Fall 9] | 11 | | |
| I | | | |
| Informanten [Gewährleistung der Anonymität? Fall 14] | 13 | | |
| Informatikverordnung [Umsetzung] | 6 | | |
| Internationale Konferenzen [Weiterbildung DSB] | 25 | | |
| Internet [Fotos von Mitarbeitenden? Fall 2] | 9 | | |
| Internetauftritt des DSB [Nutzerstatistik] | 19 | | |
| K | | | |
| Kindeswohl [~ gefährdet – Bekanntgabe an wen? Fall 5] | 10 | | |
| Kirchgemeinde [Publikation von Kollektenergebnis? Fall 27] | 17 | | |
| Kirchgemeinden [Publikation von Zivilstandsereignissen? Fall 26] | 17 | | |
| Konferenzen [Weiterbildung DSB] | 25 | | |

Gestaltung:
Christen Visuelle Gestaltung, Zug

Auflage: 3'000 Expl.

Druck: Speck Print AG, Baar

Gedruckt auf Cyclus-Recycling-
papier aus 100% speziell sortierten
Druckerei- und Büroabfällen