



Datenschutzbeauftragter
des Kantons Zug

Tätigkeitsbericht 2000 [Nr. 2]

Datenschutzbeauftragter des Kantons Zug

Tätigkeitsbericht 2000 [Nr. 2]

Der vorliegende Tätigkeitsbericht deckt den Zeitraum zwischen 1. Januar 2000 und 31. Dezember 2000 ab.

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

Zug, 15. Mai 2001

Datenschutzbeauftragter des Kantons Zug
Dr. iur. René Huber

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

Ein paar häufig verwendete Abkürzungen:

Abs.	Absatz
BGS	Bereinigte Gesetzes- sammlung [Kt. Zug]
Bst.	Buchstabe
DS	Datenschutz
DSB	Datenschutzbeauftragter
DSG	Datenschutzgesetz
EDSB	Eidg. Datenschutz- beauftragter
E-DSG	Eidg. Datenschutzgesetz
IT	Informatik-, Informations- technologie
SR	Systematische Sammlung des Bundesrechts

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 [Krankenkassen/Versicherer, Banken, Arbeitgeber etc.] sowie der Bundesverwaltung ist der Eidg. Datenschutzbeauftragte¹ zuständig.

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

ISSN 1424-4756

Inhaltsverzeichnis

2	Datenschutz – wozu eigentlich?
3	Kleine Gebrauchsanweisung ...
4	In Eile? – Die Highlights des Jahres 2000
5	I. Grundlagen
5	1. Rechtliches
5	1.1 Ausgangslage
5	1.2 Der Weg zum Zuger Datenschutzgesetz
6	1.3 Samstag, 9. Dezember 2000 ...
7	1.4 Was fehlt im Zuger Datenschutzgesetz?
8	2. Die Rolle des DSB – acht Fragen
10	3. Zur Datensicherheit
11	II. Berichterstattung 2000
11	1. Arbeitszeit – Übersicht des Aufwandes für die verschiedenen Tätigkeitsbereiche
12	2. Fälle aus der Beratungspraxis
12	2.1 Ausgangspunkt
13	2.2 Übersichtstabelle der Fälle
14	2.3 Grundlegende Problemstellungen
20	2.4 Kantonale Behörden
26	2.5 Einwohnergemeinden
27	2.6 Bürgergemeinden
27	2.7 Korporationsgemeinden
28	2.8 Wenn Private Verwaltungsaufgaben übernehmen
28	3. Öffentlichkeitsarbeit
28	3.1 Internet-Auftritt
28	3.2 Mailing-Liste
29	3.3 Medienarbeit
29	3.4 Datenschutz im Weiterbildungsangebot der kantonalen Verwaltung
29	3.5 DSB-Vortragstätigkeit
29	4. Mitarbeit bei der Gesetzgebung
29	4.1 Datenschutzgesetz des Kantons Zug
29	4.2 Archivgesetzgebung
30	4.3 Revision des Steuergesetzes
30	4.4 Vernehmlassungen
30	5. Register der Datensammlungen
30	6. Kontrolle
31	7. Zusammenarbeit mit dem Eidg. und den kantonalen Datenschutzbeauftragten
31	8. Näheres zur Datenschutzstelle
32	III. Ein paar Tipps für Sie als ...
32	1. Bürgerin/Bürger
32	2. Mitarbeiterin/Mitarbeiter der Verwaltung
33	IV. Ausblick 2001
33	1. Zur Arbeit des Datenschutzbeauftragten
33	2. Zur Lage im Kanton Zug
34	3. Sind bald andere Dimensionen angesagt?
35	Dank!
36	Sachregister
37	Datenschutzgesetz des Kantons Zug
41	Nützliche Adressen

Datenschutz – wozu eigentlich?

Stellen Sie sich vor ...

da hat man jahrelang gespart, um eine Wohnung oder ein Haus zu kaufen, das Gewünschte lässt sich finden, leider aber ist keine Bank dazu bereit, eine Hypothek zu gewähren – obwohl doch die Voraussetzungen eigentlich erfüllt wären.

Oder:

Jemand wird bei der Bewerbung von interessanten und vielversprechenden Arbeitsstellen trotz scheinbar besten Qualifikationen und Voraussetzungen nicht berücksichtigt.

Oder:

Zur finanziellen Absicherung der Familie sollte eine Lebensversicherung abgeschlossen werden. Jedoch findet sich kein Versicherer, der dazu bereit wäre.

Was läuft bei den Betroffenen in diesen drei Fällen falsch?

In allen Fällen hatte die Gegenpartei Kenntnis von den Resultaten einer Gen-Analyse. Eine solche Analyse kann Aussagen über den zukünftigen Gesundheitszustand eines Menschen machen. Kommt dabei heraus, dass mit grosser Wahrscheinlichkeit beispielsweise mit einer Krebserkrankung innerhalb der nächsten fünf bis zehn Jahre zu rechnen ist, so ist weder der Abschluss einer Lebensversicherung, noch die Einstellung und Förderung eines neuen Kadermitarbeiters – noch der Abschluss einer Hypothek kommerziell interessant.

Die zu beobachtende Tendenz, DNA-Analysen zu verlangen² oder vorzunehmen³, darf nicht einfach hingenommen werden. Die Erhebung solcher Gen-Daten trifft den Betroffenen im Kern seines Menschseins. Zu viel steht für den Einzelnen auf dem Spiel. Neben der ethischen Dimension ist auch deutlich auf die praktischen Gefahren hinzuweisen. So können DNA-Analysen fehlerhaft sein, Irrtümer oder Verwechslungen können nie ausgeschlossen werden, insbesondere muss aber mit Kenntnisnahme durch Unbefugte gerechnet werden. Durch wirtschaftliche Zusammenschlüsse können Gen-Daten plötzlich ganz neuen Kreisen bekannt werden.⁴

Kritisch muss man auch die in den USA zu beobachtende Tendenz zur «freiwilligen» Zustimmung zu einer DNA-Analyse beobachten. Was ist von einer «freiwilligen» Zustimmung zu halten – wenn man

bei Verweigerung der Zustimmung die Versicherung nicht abschliessen kann oder die langgesuchte Arbeitsstelle nicht erhält?

Es darf nicht übersehen werden, dass die DNA-Analyse im polizeilichen Bereich Erfolge vermelden kann. Trotzdem sind auch hier klare und auch enge gesetzliche Grenzen abzustecken. Nur bei schwerwiegenden Delikten soll dieses Instrument in Erwägung gezogen werden. Andernfalls steht bald die Gefahr der flächendeckenden Erfassung im Raum.

Die Datenerhebung im Bereich DNA-Analyse wird für Staat und Gesellschaft in den kommenden Jahren ganz zentrale Fragen aufwerfen. Noch sind die drei einleitend geschilderten Fälle in der Schweiz glücklicherweise nicht Realität. In verschiedenen europäischen Staaten⁵ und den USA hingegen durchaus. Teilweise werden von Heiratswilligen bereits DNA-Analysen des Partners als Vorbedingung für den Gang zum Standesamt verlangt.

Der Datenschutz ist gefordert – aber auch Sie als Bürgerin, als Bürger.

2 Z.B. im Versicherungs- oder Arbeitsbereich.

3 Im Rahmen der Strafverfolgung.

4 Verfügt ein Versicherer über Gen-Daten und fusioniert dieser mit einer Bank, so kann nicht ausgeschlossen werden, dass innerhalb des neuen Unternehmens der Bankbereich auch auf vorhandene Daten des Versicherungsbereichs greifen kann. Die Daten werden dann ja nur innerhalb der gleichen Firma bekanntgegeben ...

5 Im Versicherungsbereich sind DNA-Analysen in Irland, Grossbritannien und Portugal erlaubt. In Belgien, Dänemark, Frankreich und Schweden darf dagegen weder ein Test verlangt, noch nach einem evtl. vorhandenen Test gefragt werden.

Kleine Gebrauchsanweisung ...

Sehr geehrte Leserin

Sehr geehrter Leser

Der vorliegende Bericht gibt Auskunft über die Tätigkeiten des Datenschutzbeauftragten des Kantons Zug im Kalenderjahr 2000. Es waren einige Aufgaben zu lösen, Projekte anzugehen, Auskunft und Beratung zu erteilen. Darüber soll Sie dieser Bericht informieren. Er soll aber auch kommentieren und Stellung beziehen. Gleichzeitig sollen Sie für das Thema Datenschutz sensibilisiert werden.

Der Bericht richtet sich sowohl an die Mitarbeitenden der Verwaltung, in ihrer Funktion als Datenbearbeiter, als auch an die Bürgerinnen und Bürger, die von der Datenbearbeitung betroffen sind. Sie sollen einen Einblick erhalten, wie die Zuger Behörden Ihre Daten verwaltet.

Ich habe versucht, den Inhalt möglichst praxisorientiert darzustellen. Da nicht alle Lesenden die gleichen Bedürfnisse haben, befinden sich weiterführende Hinweise in den Fussnoten. Wenn Sie nicht auf Detailinformationen angewiesen sind, können sie beiseite gelassen werden.

An Ihrem Feedback bin ich sehr interessiert – wie beurteilen Sie Nutzen, Qualität, Quantität und Lesbarkeit des vorliegenden Berichts? Nehmen Sie sich nach der Durchsicht ein paar Minuten Zeit, um kurz den Feedback-Talon auszufüllen. Er befindet sich in der hinteren Umschlag-Klappe. Ich danke Ihnen schon jetzt sehr herzlich für Ihre Rückmeldung. Sie wird eine wichtige Grundlage für den nächsten Bericht sein.

Selbstverständlich stehe ich Ihnen für Anregungen, Kritik oder Hinweise jederzeit gerne zur Verfügung.⁶

Nun wünsche ich Ihnen eine anregende Lektüre beim datenschutzrechtlichen Rundgang durch das Jahr 2000.



Dr. iur. René Huber
Datenschutzbeauftragter des Kantons Zug

In Eile? – Die Highlights des Jahres 2000

Zuger Datenschutzgesetz

Am 9. Dezember 2000 ist das Datenschutzgesetz [im Folgenden: DSG] in Kraft getreten. Es ist abstrakt formuliert und enthält in nur 27 Paragraphen die Grundsätze. Den Gesetzestext finden Sie hinten auf S. 37.

Näheres › S. 5 ff.

Datensicherheit

Der DSB gab Anstoss zu einer umfassenden Überprüfung der Sicherheit der kantonalen Informatik. Gleichzeitig wurde abgeklärt, wie das Thema Informationssicherheit in der kantonalen Verwaltung verankert ist. Die konkreten Abklärungen begannen im Dezember und wurden durch ein spezialisiertes externes Unternehmen durchgeführt. Der Schlussbericht ist bei Redaktionsschluss des vorliegenden Berichts noch nicht abgenommen.

Näheres › S. 10

Register der vorhandenen Datensammlungen

Damit die Bevölkerung weiss, welche Daten über sie in der kantonalen und gemeindlichen Verwaltung vorhanden sind, müssen Kanton und Gemeinden ein Register aller durch sie geführten Datensammlungen erstellen [vgl. § 12 DSG]. Die Einwohnergemeinden haben diese Aufgabe sehr initiativ, professionell und vorbildlich angegangen: sämtliche Einwohnergemeinden haben sich im November zu einem gemeinsamen Projekt zusammengeschlossen.

Näheres › S. 30

Internet-Auftritt und «Mailing-Liste» des Datenschutzbeauftragten

Der DSB überarbeitete im Juni seine Web-Site unter «www.datenschutz-zug.ch» vollständig. Gleichzeitig lancierte er eine sogenannte Mailing-Liste. Wer interessiert ist, erhält per E-Mail kostenlos Kurznachrichten aus dem Bereich Datenschutz und Datensicherheit.

Näheres › S. 28

Revision des Steuergesetzes

Der DSB hat in verschiedenen Stellungnahmen klar zum Ausdruck gebracht, dass die Nichtöffentlichkeit des Steuerregisters aus datenschutzrechtlicher Sicht zu begrüssen ist.

Näheres › S. 30

Zusammenschluss der Schweizer Datenschützer

Im März haben sich die Datenschutzbeauftragten von 25 Kantonen sowie der Eidg. Datenschutzbeauftragte in einem Verein zusammengeschlossen. Näheres › S. 31

Ein kritischer Punkt ...

Das Pensum des DSB betrug 65%. In Anbetracht von Breite und Vielfältigkeit der zu bewältigenden Aufgaben sind diese personellen Ressourcen absolut ungenügend. Der DSB ist insbesondere zwingend darauf angewiesen, über einen MitarbeiterIn mit Informatikkenntnissen zu verfügen.

Näheres › S. 9

Schliesslich – der Flop des Jahres ...

Der DSB hat zwei halbtägige Datenschutzkurse für Kadermitglieder angeboten. Mangels InteressentInnen seitens der Verwaltung musste der eine Kurs abgesagt werden, der andere wurde mit nur sechs Teilnehmenden abgehalten. Deren Feedback war sehr positiv. O-Ton: «Das war spannend – wieso ist der Kurs nicht für alle obligatorisch?». Fazit: Für Datenschutz würden sich viele interessieren, wenn sie nur wüssten, worum es beim Datenschutz eigentlich geht ...

Näheres › S. 29

1. Rechtliches

1.1 Ausgangslage

Das Bundesrecht schreibt den Kantonen vor, ein «Kontrollorgan»⁸ für den Datenschutz zu schaffen. Diese Bestimmung ist seit dem 1. Juni 1993 in Kraft. Mit der Wahl des Datenschutzbeauftragten ist der Kanton Zug seit März 1999 diesen bundesrechtlichen Minimalvorgaben nachgekommen. Jedoch fehlten bis gegen Ende 2000 die Datenschutzbestimmungen, da die Arbeiten an einem kantonalen Datenschutzgesetz erst im Jahre 1998 an die Hand genommen wurden.⁹ Hier ist darauf hinzuweisen, dass in der neuen Bundesverfassung der Datenschutz nun ausdrücklich verankert ist.¹⁰

Datenschutz in Europa

In der in Nizza am 7. Dezember 2000 verabschiedeten EU-Grundrechtscharta wird der Datenschutz als eigenständiges Grundrecht verankert.¹¹ Der Datenschutz wird dadurch nicht mehr nur als Teil des Grundrechts der Achtung der Privatsphäre¹² betrachtet. Es ist jedoch zu beachten, dass der EU-Grundrechtscharta zurzeit noch keine verbindliche Kraft zukommt. Sie ist nur, aber immerhin, Ausdruck des politischen Willens.

1.2 Der Weg zum Zuger Datenschutzgesetz

Ende 1999 leitete der Regierungsrat die Gesetzesvorlage und den erläuternden Bericht¹³ zu einem Datenschutzgesetz an den Kantonsrat.

Die kantonsrätliche Kommission hat den Entwurf unter dem Vorsitz von Rechtsanwalt Dr. Willi Wismer an drei Halbtagesitzungen mit grossem Interesse, Sorgfalt und Engagement beraten. Als Experten begleiteten der Landschreiber Dr. Tino Jorio und der Datenschutzbeauftragte die Kommissionssitzungen. Die Kommission ist den Vorschlägen des Regierungsrates im Wesentlichen gefolgt.

1.2.1 Erste Lesung im Kantonsrat

Die Erste Lesung im Kantonsrat fand am 6. Juli 2000 statt.¹⁴ Eintreten war unbestritten. Aufgrund der sorgfältigen Vorbereitung durch die kantonsrätliche Kommission löste die Vorlage keine grossen Diskussionen aus. In der Detailberatung wurde lediglich über die folgenden vier Punkte abgestimmt:

Geburtsdatum – voraussetzungslos zugänglich?

Es ging darum, ob das Geburtsdatum bei der Ein-

wohnerkontrolle sowohl bei Einzel- als auch bei Sammelauskünften voraussetzungslos zugänglich sein sollte.¹⁵ Der Regierungsrat und die Kommission vertraten die Auffassung, dass das Geburtsdatum zu einem engeren Bereich der Privatsphäre gehört. Es soll nicht jedermann grund- und voraussetzungslos möglich sein, beispielsweise das Geburtsdatum der Nachbarin oder einer Gemeindeangestellten zu erhalten. Der Kantonsrat schloss sich dem regierungsrätlichen Vorschlag an.¹⁶

Sperrung von Daten – voraussetzungslos?

Bestimmte Daten sind bei der Einwohnerkontrolle auch für Private voraussetzungslos erhältlich.¹⁷ Als Gegenstück zu dieser freien Zugänglichkeit gewisser Daten über Privatpersonen durch Private hat der Regierungsrat die Möglichkeit einer voraussetzungslosen Sperrung¹⁸ vorgesehen. Der Kantonsrat schloss sich dem an.

Einfügen einer allgemeinen Strafbestimmung?

Beantragt wurde, eine allgemeine¹⁹ Strafbestimmung²⁰ in das Gesetz einzufügen. Der Kantonsrat folgte jedoch dem Regierungsrat,²¹ der darauf verzichtet hatte. Auch wenn das DSG nun keine allgemeine Strafbestimmung enthält, bleiben nicht etwa sämtliche Verstösse gegen das DSG sanktionslos: Je nach konkretem Fall stellt sich die Frage, ob aufgrund des Personalrechts, des Zivilrechts oder des Strafrechts vorzugehen ist.

Datenbekanntgabe – Sonderregelung zugunsten der Kirchgemeinden?

Die Frage drehte sich darum, ob die öffentlichrechtlich anerkannten Kirchgemeinden von der Einwohnerkontrolle nicht nur die Daten über ihre eigenen Mitglieder [was unbestritten war], sondern zudem auch diejenigen über die Familienangehörigen anderer Konfessionen erhalten sollten.²² Begründet wurde dieses Anliegen damit, dass es für die seelsorgerische Tätigkeit wichtig sei, die Konfessionszusammensetzung einer Familie zu kennen. Angaben über die Religion sind besonders schützenswerte Personendaten. In der entsprechenden Gesetzesbestimmung²³ werden sie sogar an erster Stelle aufgeführt. Es geht um die Daten von Personen, die nicht Angehörige der anfragenden Kirchgemeinde sind. Es geht auch um Personen, die aus der betreffenden Kirche ausgetreten sind. Die Angaben über solche Personen dürfen den Kirchgemeinden nicht automatisch gemeldet werden.

7 Art. 37 Abs. 2 des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG, SR 235.11) lautet: «Die Kantone bestimmen ein Kontrollorgan, welches für die Einhaltung des Datenschutzes sorgt.»

8 Darunter ist ein unabhängiger Datenschutzbeauftragter oder eine Datenschutzkommission zu verstehen.

9 Vgl. zur Vorgeschichte: Tätigkeitsbericht des DSB Zug 1999 S. 4.

10 Seit dem 1. Januar 2000 in Kraft. Art. 13 Abs. 2 BV lautet: «Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.»

11 Art. 8 Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000 (2000 C 364/01).

12 EU-Charta Art. 7 [vgl. vorstehende FNI bzw. EMRK Art. 8.

13 Diese Dokumente finden Sie im Internet: «www.datenschutz-zug.ch» [Rubrik: Kanton Zug/Gesetze].

14 Vgl. dazu Protokoll des Kantonsrates (26. Sitzung): 6. Juli 2000, S. 877-890.

15 Vgl. § 8 Abs. 3 Bst. a lbzw. Bst. b) DSG.

16 Mit 39:33 Stimmen.

17 Vgl. § 8 Abs. 3 Bst. a DSG.

18 Näheres dazu s. hinten S. 6.

19 Beauftragte stehen unter der besonderen Strafbestimmung von § 24 DSG.

20 Der Antrag lautete: «Wer gegen Bestimmungen dieses Gesetzes verstösst, wird mit Haft oder Busse bestraft.»

21 Mit 58:11 Stimmen.

22 Der Antrag lautete: «Die römisch-katholischen und die evangelisch-reformierte Kirchgemeinden erhalten die zur Ausübung ihrer Aufgaben erforderlichen Daten der eigenen Mitglieder sowie jene der im selben Haushalt lebenden Familienangehörigen anderer Konfession.»

23 Vgl. § 2 Bst. b DSG.

Zudem gibt es datenschutzkonforme Möglichkeiten, wie die Kirchgemeinden die fraglichen Daten erhalten können: Die eigenen Mitglieder können angefragt werden, ob in der betreffenden Familie Personen leben, die der Kirche ihre Angaben mitteilen wollen. Naheliegend ist insbesondere auch die Anfrage der Betroffenen im konkreten seelsorgerischen Einzelfall. Der Antrag auf Einfügen einer Ausnahmebestimmung zugunsten der Kirchen wurde mit 52:19 Stimmen abgelehnt.²⁴

1.2.2 Zweite Lesung im Kantonsrat

Diese fand am 28. September 2000 statt.²⁵ Sie gab nicht zu grossen Diskussionen Anlass. Mit einer Ausnahme²⁶ wurden die sprachlichen Bereinigungen gemäss den Vorschlägen der kantonsrätlichen Redaktionskommission angenommen. Schlussabstimmung: Mit 61:0 stimmt der Kantonsrat der Vorlage zu.

1.3 Samstag, 9. Dezember 2000 ...

der grosse Tag des Zuger Datenschutzes: Das Datenschutzgesetz/DSG tritt in Kraft.

Das DSG ist die Grundlage des Datenschutzes und der Datensicherheit für die Zuger Verwaltung. Auf den Erlass einer Datenschutz-Verordnung wurde übrigens verzichtet. Es lohnt sich, hier kurz auf das Gesetz einzugehen. Besonders die folgenden zentralen Punkte sind zu erwähnen:

Abgrenzung

Das Gesetz ist grundsätzlich nur anwendbar auf die Datenbearbeitung kantonaler und gemeindlicher Verwaltungen. Für die Datenbearbeitung von Privaten ist dagegen das Eidg. Datenschutzgesetz²⁷ anwendbar.

Datensicherheit [§ 7 DSG]

Jegliche Datenbearbeitung muss in einem sicheren Rahmen stattfinden. Datenschutz macht nur Sinn, wenn auch die Datensicherheit in jeder Beziehung garantiert ist. Der Regierungsrat ist beauftragt, bis Ende 2001 eine Informationssicherheits-Verordnung zu erlassen.

Zweckbindung [§ 4 Bst. c DSG]

Daten dürfen grundsätzlich ausschliesslich für den Zweck bearbeitet werden, der bei der Beschaffung angegeben worden ist. Beispielsweise dürfen die Daten der Einwohnerkontrolle nicht für Marketingzwecke verwendet werden. Dem liegt der Grundsatz der Transparenz bei der Datenbearbeitung zugrunde.

Dem Betroffenen ist bei der Anmeldung auf der Einwohnerkontrolle klar, für welche Zwecke seine Daten erhoben werden [hier: für das Meldewesen]. Eine andere Nutzung der Daten ist grundsätzlich unzulässig.

Datenherkunft [§ 4 Bst. b DSG]

Ebenfalls ein zentraler Grundsatz der Transparenz: Daten sind in der Regel bei der betroffenen Person zu beschaffen – nicht bei Dritten, nicht im Geheimen. Die Bevölkerung soll grundsätzlich wissen, über welche persönlichen Informationen der Staat verfügt. Diese Transparenz ist wichtig. Sie kann nur erreicht werden, wenn Daten direkt bei der betroffenen Person erhoben werden.

Sperrrecht [§ 9 DSG]

Betroffene Personen können ihre Daten voraussetzungslos und kostenlos sperren lassen. Dies hat zur Folge, dass Private grundsätzlich keine Auskünfte über andere Private erhalten. Darüber wurde auch in den Medien berichtet. Allerdings wurde dieses Sperrrecht nicht immer ganz korrekt kommuniziert. Dies haben etliche Bürgeranfragen gezeigt. Es sei hier deshalb auf die folgenden wesentlichen Punkte hingewiesen:

– Gesperrte Daten werden nicht an Private bekanntgegeben. Behörden hingegen, die für die Erfüllung ihrer Tätigkeit auf diese Daten angewiesen sind, erhalten auch gesperrte Daten.

– Es gibt keine zentrale Verwaltungsstelle, bei der man sämtliche persönlichen Daten sperren lassen könnte. Vielmehr müssen Daten bei der entsprechenden datenbearbeitenden Behörde gesperrt werden. Der Grund liegt darin, dass es weder bei Kanton noch Gemeinden eine einzige Stelle gibt, die sämtliche öffentlichen Daten verwaltet.

– In diesem Zusammenhang ist zu beachten, dass die Tätigkeit der Verwaltung im Kanton Zug grundsätzlich nicht öffentlich ist. Somit erhalten Private grundsätzlich keinerlei Kenntnisse von Daten anderer Privatpersonen. Beispielsweise ist es deshalb weder sinnvoll noch notwendig, seine Daten beim Sozialdienst, im öffentlichen Spital, beim Zivilschutz oder der Polizei zu sperren.

– Eine Sperrung von Daten ist zudem in den Bereichen nicht möglich, in denen das DSG keine Anwendung findet bzw. andere Gesetze den Zugang

24 Protokoll des Kantonsrates [26. Sitzung]: 6. Juli 2000, S. 888/889.

25 Vgl. dazu Protokoll des Kantonsrates [29. Sitzung]: 28. September 2000, S. 992/993.

26 Betr. § 10 DSG: Die nun geltende Fassung soll gemäss allgemeiner Übereinstimmung materiell dem regierungsrätlichen Entwurf entsprechen. Zur Diskussion stand nur, «ob das Glas halbvoll oder halbleer sei».

27 SR 235.1.

zu den Daten ausdrücklich vorsehen. Erinnert sei etwa an das Grundbuch, das Betreibungsregister oder das Handelsregister. Hier sehen besondere Bestimmungen den öffentlichen und allgemeinen Zugang zu Daten vor. Es ist somit ausgeschlossen, als Grundeigentümer seine Daten beim Grundbuchamt sperren zu lassen.²⁸

_ Was bleibt denn vom Sperrrecht überhaupt noch übrig? Der Hauptanwendungsbereich liegt bei der Einwohnerkontrolle. Aufgrund von § 8 Abs. 3 erhalten Private gewisse Daten über andere Private sofern eben die Daten nicht gesperrt sind. Wichtig ist hier zu erwähnen, dass gesperrte Daten auch bei Sammelauskünften²⁹ nicht bekannt gegeben werden dürfen. Ebenfalls beim Strassenverkehrsamt³⁰ dürfen über Motorfahrzeughalter, die ihre Daten gesperrt haben, keinerlei Auskünfte an Private erteilt werden.

_ Die Sperrung erfolgt voraussetzungs- und kostenlos. Eine schriftliche Mitteilung an die entsprechende Amtsstelle mit dem Hinweis: «Bitte sperren Sie meine Daten» ist ausreichend.

Register [§ 12 DSG]

Kanton und Gemeinden müssen ein Register erstellen, in dem bekanntgegeben wird, welche Datensammlungen die Verwaltungen führen. Dies ist insbesondere ein Hilfsmittel für die Bevölkerung. Denn nur wenn bekannt ist, welche Datensammlungen überhaupt vorhanden sind, können Betroffene das Einsichtsrecht sinnvoll ausüben. Weiteres dazu s. hinten S. 30.

Meldepflicht für neue/geänderte Datensammlungen [§ 12 Abs. 4 DSG]

Das Gesetz schreibt den öffentlichen Verwaltungen vor: «Neue Datensammlungen und Änderungen bestehender Datensammlungen sind sofort der Datenschutzstelle zu melden.» Diese Bestimmung ermöglicht einerseits, das Register der Datensammlungen à jour zu halten, andererseits dem DSB, Stellung zu neuen oder geänderten Datensammlungen nehmen zu können. Allerdings ist es vorteilhafter, wenn der DSB bereits in der Planungsphase neuer Projekte miteinbezogen wird. So können frühzeitig, gemeinsam und konstruktiv datenschutzkonforme Lösungen erarbeitet werden. Sind Änderungen nach Abschluss der Projekte angesagt, wird es teuer – und sorgt bei allen Beteiligten nur für rote Köpfe ...

Datenbekanntgabe durch die Einwohnerkontrolle [§ 8 DSG]

In der Praxis erhalten die Einwohnerkontrollen sehr viele Anfragen über bei ihnen gemeldete Personen. Was bekannt gegeben werden darf und was nicht, wurde in dieser Vorschrift nun exakt festgelegt.

Auskunft/Einsicht [§ 13 DSG]

Jede Bürgerin, jeder Bürger hat grundsätzlich das Recht, voraussetzungslos und kostenlos Einsicht in die bei Kanton und Gemeinden geführten eigenen Daten zu erhalten.

Datenschutzstellen in Gemeinden und kantonalen Direktionen

Gemeinden und kantonale Direktionen haben das Recht, nicht aber die Pflicht, eigene Datenschutzbeauftragte für ihren Bereich einzusetzen.³¹ Diese üben sinngemäss dieselben Aufgaben wie der kantonale DSB aus.³² Sie müssen deshalb zwingend den gleichen unabhängigen Status wie der kantonale DSB haben.³³ Bis anhin wurde nirgends von dieser Möglichkeit Gebrauch gemacht.

Internet [§ 26 Abs. 2 Bst. b DSG]

In der Internetausgabe des Amtsblatts sind besonders schützenswerte Daten nicht zu veröffentlichen. Zudem ist das Internet-Amtsblatt regelmässig zu löschen. Es wird hier am Beispiel des kantonalen Amtsblattes anerkannt, dass eine Publikation im Internet nicht gleich zu beurteilen ist, wie eine Veröffentlichung in Papierform; sind doch Informationen, die im Internet sind, weltweit zugänglich und können somit gespeichert, verknüpft, gegebenenfalls aber auch verfälscht werden.

1.4 Was fehlt im Zuger Datenschutzgesetz?

Der Zuger Gesetzgeber hat sich zum ersten Mal mit den nicht ganz einfachen Materien Datenschutz und Datensicherheit beschäftigt. Nicht sämtliche Fragestellungen konnten behandelt werden. Hier einige Themen, die in Zukunft [möglicherweise] zu regeln sein werden.

Allgemeine Strafnorm

Das Thema einer allgemeinen Strafnorm bezüglich datenschutzrelevanter Verstösse fand zu einem späten Zeitpunkt des Gesetzgebungsverfahrens Eingang in die Diskussion. Der Kantonsrat mochte sich für eine solche Bestimmung jedoch nicht erwärmen. Dies ist zu bedauern, auch wenn vom Strafrecht

28 Art. 970 ZGB steht dem entgegen.

29 Gemäss § 8 Abs. 3 Bst. c DSG.

30 Zurzeit ist eine diesbezügliche Revision des Strassenverkehrsgesetzes immer noch pendent. Der Bundesrat will die Zugänglichkeit Privater zu diesen Daten ausschliessen.

31 § 18 Abs. 3 DSG.

32 § 19 Abs. 2 DSG.

33 § 18 Abs. 2 DSG.

nicht erwartet werden kann, jegliche Verstösse verhindern zu können. Eine gewisse Verstärkung von gesetzlichen Geboten und Verboten bietet das Strafrecht jedoch unbestrittenermassen.

Finanzielle Ressourcen des DSB

Die kantonsrätliche Kommission hat die im regierungsrätlichen Entwurf enthaltene Bestimmung, wonach der DSB über ein eigenes Budget verfügt, gestrichen.³⁴ Der Grund lag nicht darin, dass der DSB nicht über eigene finanzielle Mittel verfügen soll – vielmehr herrschte Einigkeit, dass durch die Einsetzung der Datenschutzstelle diese auch mit den entsprechenden finanziellen Mitteln auszustatten ist. Die kantonsrätliche Kommission wollte keine Selbstverständlichkeiten ins Gesetz schreiben.

Fehlende Regelungen bezüglich ...

Im Gegensatz etwa zu deutschen Gesetzen werden die Themen genetische und biometrische Daten, Online-Zugriffe auf Datenbanken und Videoüberwachung³⁵ nicht explizit behandelt.

Befugnisse des DSB

Im Gegensatz zur Europäischen Datenschutzrichtlinie³⁶, die den Datenschutzbehörden «wirksame Einwirkungsbefugnisse» in die Hand gibt,³⁷ fehlen in Zug wirkungsvolle Möglichkeiten – beispielsweise ein Verbot der Datenverarbeitung anzuordnen oder Bussen bei Widerhandlungen zu verhängen.

Datenschutz-Audit von Behörden

Ein Datenschutz-Audit könnte so aussehen: Eine öffentliche Verwaltung lässt durch einen externen Auditor [eine dafür spezialisierte und besonders zugelassene Firma] ihr Datenschutz- und Datensicherheitskonzept einer förmlichen Prüfung unterziehen. Ein solcher Audit bedeutet Kosten und Arbeit. Für die Verwaltung liegt der Gewinn darin, die Sicherheit zu haben, dass Datenschutz und Datensicherheit professionell gehandhabt werden. Zudem darf die erfolgreiche Auditierung in der Öffentlichkeit bekannt gemacht werden. Durch einen erheblichen Gewinn an Vertrauen in das Datenhandling entsteht ein Standortvorteil bei Wirtschaft und Bevölkerung.

Beim Datenschutz-Audit handelt es sich nicht etwa um eine utopische Idee. Das deutsche Bundesdatenschutzgesetz und auch das entsprechende Gesetz im Bundesland Schleswig-Holstein machen es vor. Dort ist der Audit gesetzlich vorgesehen. Ein Audit kann sich auch auf ein Unternehmen, eine Dienst-

leistung oder ein Produkt beziehen. Audit und Vergabe von Labels kennt auch das schweizerische Recht übrigens seit Jahren – im Umweltrecht.³⁹

Verbandsbeschwerderecht

Es wird gelegentlich zu prüfen sein – sinnvollerweise wohl schweizweit – ob ähnlich wie im Umweltrecht, gewissen Verbänden auf dem vorliegenden Gebiet ein Verbandsbeschwerderecht zu erteilen ist. Der Hauptgrund liegt darin, dass der Einzelne sowohl als Bürger, wie auch als Konsument, gegenüber der Datenbearbeitung durch Staat und Wirtschaft ziemlich hilf- und machtlos ist.

2. Die Rolle des DSB – acht Fragen

1. Ist der Datenschutzbeauftragte für alle Datenschutzprobleme zuständig? – Nein!

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

Für die Datenbearbeitung von privaten Unternehmen [Krankenkassen/Versicherer, Banken, Arbeitgeber etc.] sowie der Bundesverwaltung ist der Eidg. Datenschutzbeauftragte⁴⁰ zuständig.

2. Ist der Datenschutzbeauftragte ein Datenpolizist, ein Spielverderber und Verhinderer? – Selten ...

Der DSB versteht sich als Dienstleistungsstelle, die der Bevölkerung, der Verwaltung und den Medien für Information, Beratung und als Ansprechperson in Sachen Datenschutz und Datensicherheit kostenlos zur Verfügung steht.

Datenschutz und Datensicherheit müssen für eine kundenorientierte, kompetente moderne Verwaltung zur Selbstverständlichkeit werden.

Zugegeben: In gewissen Fällen können Arbeitsabläufe wegen des Datenschutzes etwas komplizierter werden. Zentral ist aber, dass Bevölkerung und Wirtschaft Vertrauen haben können, dass die öffentliche Verwaltung die Privatsphäre respektiert und die Datenbearbeitung in sicherem Rahmen durchführt. Dieses Vertrauen ist ein Standortvorteil – oder: «Privacy sells!».

3. Welche Aufgaben hat der Datenschutzbeauftragte? – Einige ...

Der DSB hat ein breitgefassetes Aufgabengebiet. Konkret wird es im umfangreichen § 19 DSG umschrieben [s. dazu hinten im Datenschutzgesetz].

34 Vgl. § 18 Abs. 2/Stand 7.12.99 [zugänglich auf «www.datenschutz-zug.ch», Rubrik Zug/Gesetze].

35 Vgl. dazu § 6 b des [deutschen] Bundesdatenschutzgesetzes vom 9. April 2001.

36 Vgl. Art. 28 EG-Datenschutzrichtlinie 95/46/EG. Hinweis dazu: Diese wichtige Richtlinie beinhaltet nicht direkt anwendbares Gemeinschaftsrecht. Vielmehr wurden die Mitgliedsländer dadurch verpflichtet, die verbindlichen Vorgaben der Richtlinie fristgemäss in innerstaatliches Recht umzusetzen.

37 Vgl. dazu Zeitschrift Datenschutz und Datensicherheit/DuD, 5/2001 S. 263 ff.

38 § 9 a BDSG 2001 bzw. § 43 Abs. 2 DSG Schleswig-Holstein [Näheres dazu: «www.datenschutz-zentrum.de/audit/»].

39 Art. 43a BG über den Umweltschutz [SR 814.0]. Auch die Umweltverträglichkeitsprüfung [UVP] gehört in einem weiteren Sinn ebenfalls in diesen Bereich. Hauptunterschied zum Audit: die UVP ist für bestimmte Vorhaben gesetzlich vorgeschrieben.

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

4. Ist der Datenschutzbeauftragte denn unabhängig? – Ja

Der DSB wird vom Regierungsrat gewählt⁴¹, nicht wie zum Teil an anderen Orten durch das Parlament. Er ist administrativ der Staatskanzlei⁴² zugeordnet. Zuordnung bedeutet, dass der Datenschutzbeauftragte bei der Staatskanzlei «Kost und Logis» hat. Mehr nicht. Denn seine Tätigkeit übt er fachlich unabhängig, also nicht weisungsgebunden aus. Der DSB ist somit zwar formell ein Teil der kantonalen Verwaltung, in der Ausübung seiner Arbeit jedoch unabhängig. Diese fachliche Unabhängigkeit ist absolut zentral, denn nur sie garantiert einen glaubwürdigen Datenschutz in der Öffentlichkeit.

Die bisherigen Erfahrungen haben gezeigt, dass die fachliche Unabhängigkeit in jeder Beziehung und sämtlichen Stellen gegenüber absolut gewährleistet ist. In jeder Hinsicht hat sich auch die administrative Anbindung bei der Staatskanzlei bewährt.

5. Welche Sanktionsmittel stehen dem DSB zur Verfügung? – Keine!?

Im Falle von datenschutzrechtlichen Streitigkeiten zwischen Betroffenen und Verwaltungsstellen kann der Datenschutzbeauftragte nur Empfehlungen abgeben, nicht aber verbindliche Weisungen erteilen. Im Weiteren kann er die vorgesetzte Behörde orientieren, in letzter Instanz den Regierungsrat, in gemeindlichen Angelegenheiten den Gemeinderat. Er hat jedoch nicht das Recht, Entscheide dieser Gremien, mit denen er nicht einverstanden ist, anzufechten.

Ähnlich wie ein Ombudsmann kann der DSB im Falle von datenschutzrechtlichen Problemen in erster Linie zwischen Betroffenen und Verwaltungsstellen vermitteln. Leider verfügt der Kanton Zug nicht über einen Ombudsmann. Dies bedeutet für den DSB einiges an zusätzlicher Arbeit, werden doch recht häufig Anfragen von Privaten an den DSB gerichtet, die nur am Rande etwas mit Datenschutz zu tun haben – und teilweise grundsätzliche Konflikte mit der Verwaltung zum Ausdruck bringen.

Verfügt der DSB somit über stumpfe Waffen? Nicht unbedingt. Werden Verstösse gegen das Datenschutzrecht festgestellt, so ist es Pflicht der vorgesetzten Stellen, den rechtmässigen Zustand herzustellen. Es ist davon auszugehen, dass die vorgesetzten Behörden dieser Pflicht nachkommen. Die bisherigen Erfahrungen haben dies denn auch bestätigt.

Die Interventionsmöglichkeiten des DSB sehen zusammengefasst folgendermassen aus: vermittelndes Gespräch → Empfehlung → Meldung an vorgesetzte Behörde → Bericht an Regierungsrat/Gemeinderat.

Es besteht ohne weiteres auch die Möglichkeit, das Gespräch mit Regierungsrat, Kantonsrat oder gegebenenfalls mit zuständigen Bundesbehörden zu suchen. Nicht zuletzt hat der Datenschutzbeauftragte auch die Möglichkeit, die Öffentlichkeit über die Medien über wichtige Angelegenheiten des Datenschutzes zu informieren.

6. Wie ist das Verhältnis zu den Gemeinden? – Sehr gut

Gemäss dem zugerischen DSG ist das Gesetz auch auf die Gemeinden anwendbar. Damit unterstehen auch sie der Aufsicht des DSB. Bis jetzt haben die Gemeinden ganz unterschiedlich Gebrauch vom Dienstleistungsangebot des DSB gemacht.

7. Welche Ressourcen stehen dem Datenschutzbeauftragten zur Verfügung? – Zuwenig ...

Das Pensum hat im Berichtsjahr 65% betragen. Mit diesen knappen Ressourcen können die vom Gesetz her vorgeschriebenen Aufgaben nicht erfüllt werden. Um alle Geschäfte innert nützlicher Frist erledigen zu können, müsste eine zusätzliche juristische Fachkraft mit einem 50%-Pensum zur Verfügung stehen. Schliesslich geht es um die Bearbeitung von Daten von 93 000 Zugerinnen und Zuger durch rund 1300 kantonale Mitarbeitende und 11 Gemeinden. Damit auch – wie es der gesetzliche Auftrag umschreibt – die technische Seite genügend abgedeckt werden könnte, müsste beim DSB zudem eine Informatik-Sicherheitsperson eingestellt werden. Dem DSB fehlen die technischen Detail-Kenntnisse, um diesen Bereich, der je länger je wichtiger, zudem auch komplexer wird, kompetent abdecken zu können.

8. Welche «Grundstimmung» wird der Arbeit des Datenschutzbeauftragten entgegengebracht? – Eine sehr positive!

Die bisherigen Erfahrungen haben gezeigt, dass viele Verwaltungsstellen froh sind, Hinweise zu einem korrekten Datenhandling zu erhalten. Eine negative Einstellung dem Thema Datenschutz gegenüber konnte kaum festgestellt werden. Die Mitarbeitenden der Verwaltung wollen ihre Arbeit gut machen – dazu gehört auch der Datenschutz.

41 § 18 Abs. 1 DSG.

42 § 18 Abs. 2 DSG.

3. Zur Datensicherheit

Die Verwaltung stellt keine Produkte her und verkauft nichts – sie verwaltet Daten. Daten, die Bürgerinnen und Bürger aufgrund von Rechtsvorschriften der Verwaltung bekannt geben müssen. Viele davon sind besonders schützenswert, da in ganz entscheidender Weise mit der Privatsphäre verknüpft: Gesundheitsdaten, Angaben über soziale Hilfe, religiöse, weltanschauliche oder politische Ansichten oder Tätigkeiten.⁴³ Diese Verpflichtung zur Datenbekanntgabe löst bei der Verwaltung eine ganz besondere Verantwortung aus, mit den Daten in jeder Beziehung sicher umzugehen. Wer auf diesem Gebiet die gebotenen Sicherheitsvorkehrungen nicht trifft, muss bei Eintritt eines Schadens – neben der zivilrechtlichen Haftung – auch und insbesondere mit kaum mehr wieder gut zu machendem Vertrauensverlust rechnen.

Die folgenden zwei Punkte können deshalb nicht genug betont werden:

_Datensicherheit ist die Grundlage des Datenschutzes: Es hat keinen Sinn, Datenschutz [im engeren Sinn] zu betreiben, wenn die Daten nicht in jeder Beziehung sicher verwaltet werden. Datensicherheit ist deshalb das A und O jeglichen Datenschutzes.

_Datensicherheit ist Chefsache: Auf diesem Hintergrund organisierte der DSB im April eine Präsentation für den Regierungsrat im Rahmen der regierungsrätlichen Klausurtagung 2000 in Appenzell zum Thema Informationssicherheit [Hauptreferent: Prof. B. Hämmerli/HTA Luzern]. Der Regierungsrat ist verantwortlich, dass die Daten von Zugerinnen und Zugern sicher bearbeitet werden – der Kantonsrat, dass die dafür notwendigen Ressourcen vorhanden sind.

Sicherheitsüberprüfung der kantonalen Informatik

Informatik-Infrastrukturen sind aufgrund der weltweiten Vernetzung ständig zunehmenden Gefahren und Risiken ausgesetzt. Der Regierungsrat beschloss deshalb im Mai, die kantonale Informatik einer Sicherheitsüberprüfung durch ein spezialisiertes Unternehmen zu unterziehen. Es sollte umfassend abgeklärt werden, ob die kantonale Informatik den heute geforderten Sicherheitsan-

sprüchen genügt. Unter der Projektleitung der Leiterin Stabsbereich Ressourcen/FD wurde das Projekt zwischen Herbst und Frühjahr 2001 zügig umgesetzt [DSB im Projektausschuss]. Der Schlussbericht wird im Frühsommer 2001 vorliegen.

Vorweg kann gesagt werden: Das kantonale Netzwerk, Hard- und Softwarekonfiguration können als sicher bezeichnet werden.⁴⁴ Dagegen wurde eine Reihe von organisatorischen bzw. strukturellen Defiziten geortet. Das Bewusstsein für und der Umgang mit dem Thema IT-Sicherheit bei den Mitarbeitenden der kantonalen Verwaltung muss deutlich gefördert werden.

Fachgruppe Informatik-Sicherheit

Im Herbst wurde zudem die Einsetzung einer Informatik-Security-Fachgruppe [Zusammensetzung: Finanzdirektion, ITL, DSB sowie externer Sicherheitsexperte] beschlossen. Sie wird die Aufgabe haben, das Thema Informatiksicherheit bezüglich der kantonalen Informatik kontinuierlich zu begleiten und die entsprechend notwendigen Massnahmen umzusetzen.

43 § 2 Bst. b DSG.

44 Die Tatsache, dass keine Möglichkeit der verschlüsselten, somit sicheren Internet-E-Mail Kommunikation besteht, wird hier ausgeklammert. S. dazu hinten Fall Nr. 9 S. 16.

II. Berichterstattung 2000

1. Arbeitszeit – Übersicht des Aufwandes für die verschiedenen Tätigkeitsbereiche

Was hat der DSB 2000 eigentlich gearbeitet? Statistische Angaben wie Anzahl der Anfragen, der geführten Telefongespräche, der verfassten Stellungnahmen etc. sind nicht sehr sinnvoll, da nur beschränkt aussagekräftig. Der Arbeitsaufwand für ein einzelnes Geschäft kann je nach Komplexität zwischen 20 Minuten und 20 Stunden betragen. Im Folgenden deshalb eine Aufstellung der aufgewendeten Arbeitszeit nach thematischen Schwerpunkten:

Bereich	2000*	[1999]	Anmerkungen
Beratung/Auskunft/Information	34%	[35%]	aufgeteilt nach: kantonale Verwaltung 24% [25%] Gemeinden 5% [5%] Private 5% [5%]
Ausbildungsangebote	6%	–	Betr. kantonale und gemeindliche Verwaltungen [DSB-Kurs, Referate, Präsentationen etc.]
Betreuung div. grösserer Projekte	17%	[8%]	Volkszählung 2000, Register Datensammlungen, Verfassen Tätigkeitsbericht 1999
Begleitung Datenschutzgesetz	8%	[15%]	div. Grundlagenarbeiten, Weiterbearbeitung Gesetz, Begleitung der kantonsrätlichen Kommission etc.
Öffentlichkeitsarbeit	13%	[13%]	Internet-Auftritt, Medienarbeit, Mailing-Liste
Zusammenarbeit mit Eidg. DSB und kt. DSB	4%	[8%]	Erfahrungs- und Informationsaustausch, kantonsübergreifende Bearbeitung von wichtigen Themen
Weiterbildung	5%	[3%]	Datenschutz [DSB-Symposium, GIS-Tagung, Informatik/DS-Recht-Tagung des Bundes], Informatik [PKI-Swiskey, Groupwise], Verwaltung [Zielvereinbarungen]
Diverses	13%	[18%]	allg. Korrespondenz, Rechnungswesen, Aufbau/Betreuung EDV-Infrastruktur, Bibliothek, Besprechungen – soweit nicht direkt einzelnen Projekten zuweisbar
total	100%	[100%]	

* In % der Arbeitszeit [Pensum 65%]

2. Fälle aus der Beratungspraxis

2.1 Ausgangspunkt

Es ist immer wieder festzustellen: Wenn Nichtjuristinnen und Nichtjuristen das Datenschutzgesetz durchlesen oder zu Rate ziehen, bleiben sie meist ziemlich ratlos – oder auch: frustriert zurück. Sie wollten doch nur ihre Frage beantwortet haben: «Dürfen die Standorte der Mobilfunkantennen im Internet veröffentlicht werden?», «Muss der Sozialdienst der Polizei Daten über möglicherweise Schwarzarbeitende bekannt geben?» oder etwa «Muss die Polizei Anzeige erstattende Personen den Angezeigten bekannt geben?». Das Gesetz erwähnt solche Fragestellungen jedoch mit keinem Wort. Juristinnen und Juristen sind sich gewohnt, dass Gesetze Tatbestände nur in abstrakter Weise regeln. Erst die Auslegung der Gesetzesbestimmung bringt die Lösung an den Tag.

Um Ihnen Sinn und Zweck des Datenschutzgesetzes näher zu bringen, Sie für die Anliegen des Datenschutzes und der Datensicherheit etwas zu sensibilisieren, soll im Folgenden der Schritt in die Praxis gemacht werden. Wir wollen eine Auswahl konkreter Fälle aus der DSB-Beratungspraxis aus verschiedenen Rechtsgebieten, von verschiedenen Verwaltungsstellen, näher betrachten.⁴⁵ Für die Zuordnung zu den jeweiligen Behörden war übrigens entscheidend, von welcher Stelle die Anfrage ausging.

Die Fälle werden so dargestellt, dass keinerlei Rückschlüsse auf die betroffenen Personen gezogen werden können.⁴⁶

In diesem Zusammenhang ist darauf hinzuweisen, dass Anfragen von Privaten an den DSB selbstverständlich streng vertraulich behandelt werden. Dies bedeutet z.B. auch, dass der DSB erst nach Erhalt einer schriftlichen Bestätigung durch die Betroffenen in ihrem Namen bei Verwaltungsstellen vorstellig wird. Die Betroffenen haben somit stets die Sicherheit, Herr über ihre Anfragen zu sein.

45 Die Fälle sind mit einer Nummer versehen. Mit dieser können sie zitiert werden.

46 Gewisse Anfragen können hier nicht vorgestellt werden, da aufgrund der Problemstellung Rückschlüsse auf betroffene Personen möglich sein könnten.

2.2 Übersichtstabelle der Fälle

Thema	Problem	Fall Nr.
Akteneinsicht	Einsicht in das eigene Personaldossier	15
	Grundsätze zur Einsicht in die eigenen Akten	14
Aktenübergabe	An NachfolgerIn oder an die neu zuständige Stelle	18
Briefzustellung	Wann soll die Verwaltung neutrale Briefumschläge verwenden?	2
Datensperre: s. Sperre		
Dokumentenverwaltung	Was ist in der Gemeinde zu beachten?	38
E-Government	Sicherheitsaspekte bei Zweiweg-Kommunikation	6
Einbürgerung	Datenschutz im Einbürgerungsverfahren	42
	Welche Informationen benötigt der Kantonsrat?	24
Einkommen	Datenbekanntgabe an verwaltungsexterne Personen?	35
Einwohnerkontrolle	Welche Daten können an Private bekannt gegeben werden?	40
E-Mail [Intranet]	Sicherheitshinweise betreffend Intranet	10
E-Mail	Verschlüsselung	9
E-Mail [via Internet]	Kein Versenden von Personendaten	8
Fax	Sicherheitsaspekte	1
Finanzkontrolle	Datenbekanntgabe zur Überprüfung von geleisteten Beiträgen?	34
Forschung	Datenbekanntgabe ist zu anonymisieren	13
Fotos	Dürfen Fotos von Personen in Jahresberichten etc. veröffentlicht werden?	19
Gebäudeversicherung	An wen können Daten bekannt gegeben werden?	30
Grundbuch	Zum Online-Zugriff des Leiters des Landwirtschaftsamtes	26
Handelsregister	Umfang der Datenbekanntgabe	27
Internet	Was haben Schülerinnen und Schüler zu beachten?	25
Internet-Auftritt	Grundsätzliches	3
	Was müssen Schulen speziell beachten?	4
	Zur Verwendung von Web-Cameras	5
Internet-Nutzung	Internet-Nutzung durch Arbeitnehmende für private Zwecke?	7
Korporationsgemeinde	Grundsätze betr. Sammelauskunft	43
Krankengeschichte	Zur Herausgabe von Originalakten durch das Spital	32
Mütter-/Väterberatungsstelle	Zur Bekanntgabe von Geburten	41
Personensicherheitsüberprüfung	Betr. beauftragten externen Unternehmen	17
	Betr. Verwaltungsmitarbeitenden	16
Postversand	Outsourcen der Frankierung und Spedition der Verwaltungskorrespondenz?	37
Referendum	Bekanntgabe von Name/Adresse von Unterzeichnenden an Amtsstellen?	21
Sammelauskunft	Welche Daten können an Private bekannt gegeben werden?	40
Schule	Welche Angaben gehören in eine Klassenliste?	39
Sperre	Datensperre bei den Wasserwerken?	44
	Betr. Fahrzeughalterdaten beim Strassenverkehrsamt?	31
Staatskalender	Welche Angaben über Personen sind zu publizieren?	22
Statistik	Datenbekanntgabe ist zu anonymisieren	13
Steuerregister	Zur Öffentlichkeit des Steuerregisters	36
Strafanzeige	Recht auf Anonymität des Anzeigerstattenden?	29
Studierende	Welche Unterstützung kann der DSB bieten?	12
Verkehrsplanung	Datenbekanntgabe durch die Zivilschutzbehörde?	28
Video- und Tonaufnahmen	Wann dürfen solche zu Ausbildungszwecken angefertigt werden?	20
Videoüberwachung	Sind öffentliche Räume wegen Velo-Vandalismus zu überwachen?	11
Volkszählung 2000	Zur Durchführung im Kanton Zug	23
Zwangsmassnahmen	Datenbekanntgabe an den Kantonsarzt?	33

2.3 Grundlegende Problemstellungen

Es hat sich gezeigt, dass sich gewisse Probleme sowohl in den Gemeinden, als auch direktionsübergreifend in der kantonalen Verwaltung gleichermaßen stellen.

An dieser Stelle wurden im letztjährigen Tätigkeitsbericht 1999 grundlegende Hinweise zu folgenden Themen veröffentlicht: Geltungsbereich des Datenschutzrechts [Fall Nr. 1/S. 12]; Amtsgeheimnis [Fall Nr. 2/S. 12]; Nutzung von Fax [Fall Nr. 3/S. 13], Telefon [Fall Nr. 4/S. 13], Internet [Fall Nr. 5-7/S. 13 f.], E-Mail [Fall Nr. 8/S. 14 ff.]; Sinn und Zweck von Verpflichtungserklärungen [Fall Nr. 11/S. 16].

Diese Hinweise beanspruchen nach wie vor Geltung. Haben Sie in diesem Zusammenhang Fragen, konsultieren Sie doch die entsprechenden Fälle.⁴⁷

1 Fax

Die Bedeutung des Faxes hat in Zeiten des E-Mails deutlich abgenommen. Trotzdem stellen sich auch diesbezüglich Fragen. Amtsstellen erkundigten sich, ob es sinnvoll sei, auf dem Deckblatt eines Faxes einen Verhaltens-Hinweis⁴⁸ anzubringen, um sich dadurch einer möglichen Haftung für Schäden aufgrund eines fehlgeleiteten Faxes entziehen zu können. Solche Hinweise sind übrigens oft auf durch Rechtsanwälte verschickten Fax-Formularen oder in E-Mails anzutreffen.

Grundsätzlich liegt die Verantwortung bei der absendenden Stelle. Sie hat alles zu unternehmen, um Fehler zu vermeiden. Erhält ein Unberechtigter den Fax, so kann ein entsprechender Hinweis nützlich sein, da eine klare Handlungsanweisung angegeben wird. Dadurch kann möglicherweise weiterer Schaden verhindert werden. Grundsätzlich kann der Absender jedoch durch einen solchen Hinweis die Verantwortung für entstandenen Schaden nicht auf den Empfänger abschieben.

Fazit: Sorgfalt im Umgang mit dem Faxgerät lohnt sich. Besonders schützenswerte Personendaten oder anderweitig vertrauliche Informationen sind nicht per Fax zu übermitteln.

2 Postzustellung – in neutralem Briefumschlag?

Private haben sich darüber beklagt, dass Amtsstellen ihre Post in Briefumschlägen verschicken, die gross und deutlich den amtlichen Absender kundtun. Dadurch sei es für die Mitarbeitenden der Post, ins-

besondere den Zustelldienst, aber auch Hausbewohnern möglich, auf gewisse Sachverhalte schliessen zu können.

Es ist zu prüfen, ob es sich um eine Amtsstelle handelt, bei der tatsächlich mehr oder weniger direkte Rückschlüsse auf möglicherweise vorliegende Sachverhalte gezogen werden können – und deren Vorliegen für die Betroffenen nachteilig sein können. Zu bejahen ist dies etwa bei der Alkohol- oder Drogenberatungsstelle oder der verantwortlichen Stelle für die Heroinabgabe. In diesen Fällen ist die Korrespondenz in neutralen Briefumschlägen zu versenden. Als Absender kann eine neutrale Adresse angegeben werden [z.B. Ort und Postfach]. Man kennt dieses Vorgehen von den Banken, die ausschliesslich neutrale Couverts verwenden.

Kann objektiv betrachtet aufgrund des Absenders nicht auf den Inhalt geschlossen werden, vertritt ein Betroffener jedoch die gegenteilige Ansicht, so ist dem ausdrücklichen Wunsch zu entsprechen.

3 Internet

Mit dem Thema Internet sind einige datenschutzrechtliche Fragen verknüpft. Zwei Hauptbereiche sind zu unterscheiden: Das Anbieten von Informationen im Web und der Bezug von Informationen aus dem Web.

Einige Anfragen kamen von Stellen, die einen Auftritt im Internet planen. Man wollte wissen, ob hier aus Gründen des Datenschutzes Grenzen zu beachten sind.

Ganz zentral ist der Ausgangspunkt, dass eine Veröffentlichung von Informationen im Internet nicht gleich zu beurteilen ist, wie eine Publikation der exakt gleichen Information auf Papier. Die Gründe: Internet-Informationen stehen potentiell der ganzen Welt zur Verfügung. Sie können überall und für immer abgespeichert werden und sie können in Verbindung mit anderen Daten oder Datenbeständen analysiert werden, und dadurch Informationen liefern, die über den ursprünglichen Informationsgehalt hinausgehen. Der Zuger Gesetzgeber hat diese Gewichtung denn im DSG auch vorgenommen: Besonders schützenswerte Daten dürfen im Amtsblatt nur in der gedruckten Ausgabe, nicht jedoch in der Internet-Version veröffentlicht werden.⁴⁹

4 Was ist beim Internet-Auftritt einer Schule zu beachten?

Es ist hier besonders darauf hinzuweisen, dass von Schülerinnen und Schülern aus Sicherheitsgründen

47 Die gedruckte Version des Tätigkeitsberichts 1999 ist leider vergriffen. Sie finden den Bericht jedoch layoutgetreu im Internet unter: «www.datenschutz-zug.ch» [Rubrik «Tätigkeiten»].

48 Etwa: «Dieser Telefax ist streng vertraulich und einzig für den Adressaten bestimmt. Einem anderen als dem adressierten Empfänger ist es deshalb nicht gestattet, die Folgeseiten zu lesen, diese Sendung zu kopieren, zu verbreiten oder anderweitig zu verwenden. Sind Sie nicht der Fax-Adressat, benachrichtigen Sie bitte den Absender.»

49 Zudem ist die Internet-Version des Amtl. Teils regelmässig zu löschen, vgl. § 26 Abs. 2 Bst. b DSG.

keinesfalls Fotos, Namen oder Privatadressen publiziert werden dürfen – selbst nicht mit Einwilligung der Betroffenen. Gewisse zusätzliche Informationen können u. U. in einem passwortgeschützten Bereich, somit für einen geschlossenen Nutzerkreis veröffentlicht werden.

Der DSB des Kantons Basel-Landschaft hat ein sehr nützliches Merkblatt zum vorliegenden Bereich verfasst. Es steht Ihnen auf der Web-Site des DSB-Zug zur Verfügung.

5 Web-Cameras im Internet

Beliebt sind auch sogenannte Web-Cams. Diese Kameras ermöglichen es den Internet-Nutzenden, einen Blick auf die Gemeinde, den See oder die Aussicht zu werfen. Gegen solche Kameras ist solange nichts einzuwenden, als die Kamera so platziert und eingestellt ist, dass es nicht möglich ist, Personen oder Fahrzeug-Schilder etc. zu erkennen. Auch darf nicht auf die Lebensgewohnheiten oder anhand der sichtbaren Wohnungsbeleuchtung die An- und Abwesenheit von Hausbewohnern geschlossen werden können.⁵⁰

6 Internet und E-Government

E-Government ist zu einem Lieblingswort von Politik und Verwaltung geworden. Der Staat soll sich modern geben. Die Schalter sind für Wirtschaft und Bevölkerung während 24 Stunden am Tag, an 365 Tagen im Jahr offen zu halten. Dabei gibt man sich nicht damit zufrieden, Informationen ins Internet zu stellen. Zweiseitige Kommunikation, die Abwicklung von Geschäftsvorgängen⁵¹ über das Internet soll möglich sein.

Verschiedene Gemeinden gelangten im Zusammenhang mit der Überarbeitung ihres Internet-Auftritts an den DSB. Dabei stellten sich insbesondere auch Fragen der Kommunikation. Die Antwort ist klar: Die unverschlüsselte Übermittlung von Daten über das Internet ist in jeder Hinsicht unsicher. Es kommt somit nur eine verschlüsselte Übertragung in Frage. Damit ist aber noch nicht gesichert, dass es die Verwaltung auch tatsächlich mit dem Absender zu tun hat, den dieser vorgibt zu sein. Es müssen deshalb technische Massnahmen ergriffen werden, die auch die Authentizität des Absenders auf zweifelsfreie Art sicherstellen. Das Einrichten derartiger Sicherheitsmechanismen dürfte die Gemeinden in aller Regel überfordern.

Fazit: Solange die Sicherheit der Übertragung und die Authentizität des Absenders nicht gewährleistet

sind, dürfen keinerlei Personendaten via Internet übertragen werden. Die Gemeinden haben sich in der Zwischenzeit somit auf konventionelle Web-Auftritte zu beschränken: Bereitstellen von nützlichen Informationen, auch von Formularen etc. Der Feedback der Bevölkerung hat jedoch auf konventionellen Wegen zu erfolgen.

7 Was ist bei der Benützung des Internets zu beachten?

Für Arbeitgeber wie Mitarbeitende stellt sich hier insbesondere die Frage nach der Zulässigkeit der privaten Nutzung. Empfehlenswert ist eine klare Abmachung! Es kann vorgesehen werden, dass während der Arbeitszeit private Nutzung in einem gewissen Ausmass zulässig ist – es kann aber auch jegliche Privatnutzung verboten⁵² sein.

Oft wissen die Mitarbeitenden nicht, dass jeder Internet-Klick, jede einzelne aufgerufene Seite beim IT-Betreiber zusammen mit weiteren Angaben [Datum, Zeit, Arbeitsstation etc.] in sogenannten «log-files» aufgezeichnet werden – und auch einsehbar sind.

Anzumerken ist jedoch, dass der Arbeitgeber grundsätzlich kein Recht hat, diese log-files personenbezogen auszuwerten und kontrollieren zu lassen. Etwas anderes gilt nur, wenn die private Nutzung vollständig verboten ist, die Mitarbeitenden schriftlich darauf – und auch über mögliche diesbezügliche Kontrollen und Konsequenzen – aufmerksam gemacht worden sind. Eine Auswertung der log-files ist auch bei dringendem Verdacht strafbarer Handlungen zulässig.

In allen anderen Fällen dürfen die log-files der Mitarbeitenden jedoch nicht personenbezogen ausgewertet werden.

Der Regierungsrat hat im Herbst 2000 eine Arbeitsgruppe⁵³ eingesetzt, die eine Weisung über den Gebrauch von Internet und E-Mail in der kantonalen Verwaltung auszuarbeiten hat. Soweit darin Vorgaben zur Informatiksicherheit gemacht werden, sind diese aufgrund von § 7 Abs. 2 DSG auch auf die Gemeinden anwendbar. Was jedoch die Aspekte des Arbeitsverhältnisses betrifft – z.B. die Frage nach der Zulässigkeit der Internet-Nutzung zu privaten Zwecken –, können die Gemeinden in eigener Regie regeln.

8 E-Mail via Internet

Wohl die meisten Nutzer des Mail-Dienstes gehen

50 Vgl. dazu den Fall eines durch eine Web-Cam beobachteten Hauses in Dürnten/ZH, Tages-Anzeiger, 12.08.2000 S. 13 [der Bericht ist im Archiv der DSB-Mailing-Liste zugänglich].

51 Z.B. An- oder Abmeldung bei der Einwohnerkontrolle, Eingabe der Steuererklärung, einer Baubewilligung etc.

52 Aus Gründen der betrieblichen Datensicherheit in besonderen Bereichen – oder falls ein Netz mit geringer Bandbreite wegen privater Nutzung überlastet werden könnte.

53 Zusammensetzung: Direktionssekretariat/FD, Personalteilung, Informatik/ITL und DSB.

davon aus, die Nachrichtenübermittlung via E-Mail sei mindestens so sicher wie die Zustellung per Briefpost

Diese Ansicht ist vollkommen falsch! Die Übermittlung unverschlüsselter E-Mails ist in jeder Hinsicht unsicher. Mails können mit geringstem Aufwand auf dem Weg zum Adressaten von Unberechtigten eingesehen, abgeändert, kopiert, umgeleitet oder gelöscht werden. Fachleute bezeichnen den Versand unverschlüsselter Mails denn auch als weniger vertraulich als denjenigen von Postkarten. Das Mail kommt auf seiner Reise zum Empfänger an verschiedenen Stellen vorbei, an denen es mit geringstem Aufwand gelesen werden kann. Der Absender kann auch mit einfachsten Mitteln die Absenderbezeichnung manipulieren. Der Empfänger kann grundsätzlich keinerlei Sicherheit darüber haben, von wem das Mail wirklich stammt.

Es ist zudem bekannt, dass verschiedene Staaten systematisch, vollständig flächendeckend, also weltweit den ganzen Mail-Verkehr überwachen und auswerten. Wir haben es hier insgesamt mit einem Gefahrenpotential zu tun, von dem die Mail-Nutzer meist keinerlei Kenntnisse haben – weil die Vorgänge und Hintergründe für die Nutzenden unsichtbar sind.

Der Regierungsrat hat deshalb zum Zeitpunkt der Öffnung des Zugangs zu den Internet-Diensten wohlweislich die folgende Weisung vom 19. Januar 1999 erlassen:

«1. Die Mitarbeitenden der kantonalen Verwaltung und Schulen dürfen Personendaten über E-Mail (Internet) nur chiffriert übermitteln. Sofern dies nicht möglich ist, ist vor der Übermittlung das Einverständnis der betroffenen Person einzuholen.

2. Personendaten dürfen nur über den zentralen E-Mail-Server des Kantons übermittelt werden. Die entsprechenden Verkehrsdaten dürfen nur dort gespeichert werden (keine Verwendung privater PC). Zulässig sind die bisherigen stand-alone PC der kantonalen Verwaltung.

3. Der Empfänger einer Nachricht muss in geeigneter Weise die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen prüfen.»

Vor Inkrafttreten des DSG war diese Weisung für die gesamte kantonale Verwaltung [inkl. kantonale Schulen und Gebäudeversicherung] verbindlich.

Seit Inkrafttreten des DSG ist diese Weisung als Formulierung eines allgemeinen Grundsatzes der Verpflichtung zur sicheren Datenbearbeitung im Sinne von § 7 DSG zu betrachten. Damit ist sie auf sämtliche dem DSG unterworfenen Organe, somit insbesondere auch auf Gemeinden [Gerichte, Pensionskasse etc.] anzuwenden.

Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbar natürliche oder juristische Person beziehen.⁵⁴ Dies bedeutet, dass grundsätzlich keinerlei Personendaten⁵⁵ unverschlüsselt via E-Mail übermittelt werden dürfen. Das Einverständnis der betroffenen Person wird man nur selten haben – zudem muss diese darüber informiert werden, wie unsicher das Übermittlungsverfahren ist.

Somit können Personendaten nur verschlüsselt übermittelt werden. Wenden wir uns im Folgenden kurz diesem Thema zu.

9 Chiffrierung

Ausgangspunkt: Zurzeit⁵⁶ steht den Kantonsmitarbeitenden noch keine Möglichkeit zur Verschlüsselung von E-Mails via Internet zur Verfügung. Der Regierungsrat hat jedoch am 23. Mai 2000 den zuständigen Stellen den Auftrag erteilt, die Planung zur Chiffrierung von externen E-Mails «unverzögerlich aufzunehmen». Dieser Auftrag ist durch die verantwortlichen Stellen ohne weitere Verzögerungen umzusetzen. Solange die Verschlüsselung nicht möglich ist, gilt für die Verwaltungsmitarbeitenden die folgende Anweisung:

Via Internet-E-Mail dürfen keinerlei Personendaten übermittelt werden!

Es ist hier klar festzuhalten, dass es Aufgabe des Datenschutzbeauftragten ist, darauf hinzuweisen, dass das Arbeitsinstrument «E-Mail» nur für gewisse Inhalte verwendet werden darf. Die Technik hat uns ein Instrument bereitgestellt, das nicht über die elementarsten Sicherheitsmassnahmen verfügt. Beim Kassenschrank wird ein Schloss eingebaut, der Postversand wird mit Hilfe von Briefumschlägen abgewickelt – die Technik ist gefordert, uns praxistaugliche Mittel für einen sicheren E-Mail-Verkehr zur Verfügung zu stellen.

54 Vgl. die etwas ausführlichere Definition in § 2 Bst. a DSG. Der Begriff «Personendaten» wird vielleicht noch klarer, wenn wir ihn dem Begriff «Sachdaten» gegenüberstellen. Sachdaten sind Daten, die nicht einer bestimmten oder bestimmbar Person zugeordnet werden können. Beispielsweise das Register archäologisch untersuchter Objekte, Angaben zum Fischbestand des Zugersees oder Messreihen der Luftbelastung in der Zuger Innenstadt. Ebenfalls Sachdaten sind rechts-genügend anonymisierte Personendaten. Fazit: Sachdaten haben keinerlei Zusammenhang zu Personen. Angaben des Grundbuchs, Altlastenkataster oder etwa eine polizeiliche Liste gestohlener Fahrzeuge sind dagegen keine Sachdaten. Sie weisen einen mehr oder weniger direkten Bezug zur Person des Eigentümers auf.

55 Die Weisung ist sinngemäss auch auf die E-Mail-Übermittlung vertraulicher/geheimer Sachdaten anzuwenden, somit auf Daten, die dem Amtsgeheimnis unterstehen.

56 Stand: Mai 2001.

10 E-Mail via Intranet

Die Mitarbeitenden der öffentlichen Verwaltungen sind in der Regel an ein internes Datennetz angeschlossen. Sie haben die Möglichkeit, an andere Mitarbeitende der öffentlichen Verwaltung auf diesem internen, gegen aussen abgeschlossenen Netz Mitteilungen zu versenden. Dieser Intranet-Mail-Verkehr kann in technischer Hinsicht bei der Zuger Kantonsverwaltung als sicher betrachtet werden.

Jedoch ist eine gravierende Sicherheitslücke aufgrund der Möglichkeit, welche die Mail-Software dem einzelnen Anwender bietet, vorhanden. Anwenderinnen und Anwender können nämlich einkommende Mails automatisch auf eine andere Mail-Adresse umleiten lassen. Die Umleitung kann netzintern und auch an externe Mail-Adressen [Zustellung via Internet-E-Mail] erfolgen. Der Absender hat von einer solchen Umleitung keinerlei Kenntnis.

Aus Gründen des Datenschutzes und der Datensicherheit ist eine Umleitung von internen Mails an Drittadressen via Internet klar unzulässig, verlangt doch das DSG: «Daten sind insbesondere vor Verlust, Fälschung, Entwendung, Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte zu sichern.»⁵⁷ Unverschlüsselte E-Mails via Internet können auf dem Übermittlungsweg problemlos kopiert, verändert, gelöscht oder gefälscht werden. An der privaten Zieladresse besteht zudem die Gefahr, dass unbefugte Personen [Familienangehörige etc.] von umgeleiteten Mails Kenntnis erhalten.

Der Regierungsrat hat deshalb denn auch vorgeschrieben,⁵⁸ dass Personendaten mittels E-Mail via Internet nur chiffriert übermittelt werden dürfen. Solange keine Verschlüsselungsmöglichkeit zur Verfügung steht, dürfen somit keine Personendaten via Internet-E-Mail übermittelt werden.

Der kantonsinterne Absender muss sich mit absoluter Sicherheit darauf verlassen können, dass sein an einen internen Adressaten gerichtetes Mail das sichere kantonale Netz keinesfalls verlässt.

Fazit: Solange nicht mit technischen Massnahmen sichergestellt ist, dass die Umleitung an externe Mailadressen verhindert wird, dürfen besonders schützenswerte bzw. dem Amtsgeheimnis unterstehende Daten nicht auf dem Intranet übermittelt werden.

11 Videoüberwachung – gegen Vandalismus?

In diesem Jahr nahm der Velo-Vandalismus rund um den Bahnhof Zug zu. Eine Privatperson machte deshalb den Vorschlag, den Bahnhofplatz zur Bekämpfung des Fahrrad-Vandalismus mit einer Video-Überwachungsanlage auszurüsten.

Der DSB kam in seiner Stellungnahme zum Schluss, dass diese Massnahme im vorliegenden Fall ungeeignet ist, in Anbetracht des gefährdeten Rechtsgutes als unverhältnismässig zu bezeichnen ist – zudem weicht der Vandalismus in der Regel auf andere Örtlichkeiten aus.

Sie sind an der rechtlichen Vertiefung interessiert? – Hier ein Auszug aus der Begründung

Weder im kantonalen noch im eidgenössischen Recht ist die Zulässigkeit oder Unzulässigkeit der Video-Überwachung ausdrücklich geregelt. Besteht die Möglichkeit, dass durch auf öffentlichen Plätzen installierte polizeiliche Videokameras Personen erfasst werden, so handelt es sich um eine Datenbearbeitung durch Behörden.⁵⁹ Das Datenschutzgesetz ist anwendbar. Es kommen die darin festgelegten Grundsätze zur Anwendung.

Das Datenschutzgesetz hat zum Ziel, die Privatsphäre der Bürgerinnen und Bürger vor unrechtmässiger staatlicher Datenbearbeitung zu schützen. Es handelt sich somit um ein Abwehrrecht des Bürgers gegenüber dem Staat.

Der Staat soll dementsprechend nur dann Daten erheben dürfen, wenn eine gesetzliche Grundlage besteht oder es für eine in einer gesetzlichen Grundlage umschriebene Aufgabe unentbehrlich ist.

⁶⁰Diese ausdrücklich geforderte Unentbehrlichkeit stellt einen strengen Massstab dar. Der Kanton Zug ist diesbezüglich strenger als gewisse andere Kantone. Zudem ist stets zu beachten, dass eine staatliche Massnahme verhältnismässig und notwendig sein muss.⁶¹

Videoüberwachung – ein taugliches Instrument?

In England, Frankreich und Deutschland⁶² werden zum Teil ganze Stadtteile im Kampf gegen die Kriminalität flächendeckend mit Videoüberwachungskameras überzogen. Untersuchungen haben nun gezeigt, dass diese Massnahme an den fraglichen Orten tatsächlich gewisse Erfolge brachten – allerdings um den Preis der Zunahme der Kriminalität an anderen Orten. Die Kriminalität insgesamt kann mit dieser Massnahme nicht reduziert werden, es wird einfach örtlich ausgewichen.

57 § 7 Abs. 1 DSG.

58 Abgedruckt vorne bei Fall Nr. 8 S. 16.

59 § 3 in Verbindung mit § 2 Bst. a und Bst. c DSG.

60 § 5 Abs. 1 Bst. a und Bst. b DSG.

61 Vgl. dazu etwa BGE 93 I 219.

62 Vgl. zur Lage in Bayern: NZZ, 21.05.2001, S. 5.

Die flächendeckende Bestückung des öffentlichen Raums mit Videoüberwachungskameras ist keine Perspektive. Videoüberwachung kann ein taugliches Instrument bei ganz punktuell zu schützenden Personen [z.B. Schalterpersonal bei Post und Bank] oder Sachwerten [z.B. Postomat] sein.

Bedrohte Privatsphäre – bedrohte Freiheit: Ein wichtiger Teil unserer persönlichen Freiheit besteht darin, sich in der Öffentlichkeit unbeobachtet und unverfolgt von staatlichen Überwachungsmaßnahmen, somit unbeschwert, bewegen zu dürfen.

Gefährdetes Rechtsgut – Velo: Bei der Güterabwägung spielt das gefährdete Rechtsgut eine wichtige Rolle. Geht es um den Schutz von Leib und Leben, sieht die Beurteilung anders aus als bei Velos.

Alternative Sicherheitsmassnahmen? Zu prüfen ist im Rahmen der Verhältnismässigkeit auch, ob es nicht weniger einschneidende Alternativen gibt. Vorliegendenfalls ist davon auszugehen, dass wohl mit planerischen bzw. baulichen Massnahmen einiges erreicht werden könnte: Abstellplätze sind in viel begangenen, gut überwachten und beleuchteten Gebieten anzulegen; gegebenenfalls können abschliessbare Velo-Boxen [wie z.B. beim Bahnhof Zürich] etc. eingerichtet werden.

Fazit: Es ist der Schutz der Privatsphäre der Bürgerinnen und Bürger im Auge zu behalten, die sich zu 98% korrekt verhalten und sich deshalb keine Videoüberwachung gefallen lassen müssen. Dass es einen Personenkreis gibt, der sich nicht an die Regeln hält, ist bedauerlich. Tröstlich ist, dass dieser Kreis insgesamt sehr gering ist, und dass zudem verhältnismässige Massnahmen zur Bekämpfung vorhanden und umsetzbar sind.

Die Videoüberwachung des Bahnhofplatzes zur Verhinderung von Velo-Vandalismus ist somit unzulässig, da sie unverhältnismässig ist.

Nachbemerkung ...

Der DSB versteht die Verärgerung über die Velo-Vandalen gut, wurde doch sein Drahtesel im Sommer 2000 am Bahnhofplatz in Zug ebenfalls ein Opfer des Vandalismus – Fazit: Totalschaden.

12 Betreuung von Arbeiten Studierender

Verschiedentlich wandten sich Studierende im Zusammenhang mit Seminararbeiten zu den The-

men Datenschutz/Datensicherheit an den DSB. Dieser vermittelte im Rahmen von Besprechungen, Hinweisen oder Zustellung von Informations-Material Input.

13 Datenbekanntgabe für wissenschaftliche Forschung/Statistik

Die Datenbearbeitung für Forschung, Planung und Statistik ist im Datenschutzgesetz ausdrücklich geregelt.⁶³ Demgemäss ist die Datenbearbeitung zulässig, sofern die Daten sobald als möglich anonymisiert werden, wenn die Daten nicht weitergegeben werden und wenn die Ergebnisse so veröffentlicht werden, dass keinerlei Rückschlüsse auf betroffene Personen möglich sind.

Bezüglich einer ausserkantonale durchgeführten medizinischen Statistik im Behindertenbereich musste der DSB feststellen, dass den gesetzlichen Vorgaben nicht nachgekommen wurde. Die Zuger Amtsstelle [als Datenlieferantin] übermittelte erhobene Fragebögen mit besonders schützenswerten Daten – ohne dass die Statistikbearbeitenden auf die persönlichen Angaben angewiesen wären. Der Grundsatz der möglichst frühzeitigen Anonymisierung wurde verletzt. Die Zuger Amtsstelle hätte anonymisierte Daten an die ausserkantonale Forschungsstelle übermitteln sollen. Dadurch wird der Kreis derjenigen Personen, die von den besonders schützenswerten Daten Kenntnis erhalten, kleiner gehalten.

14 Einsicht in die eigenen Akten – die Grundsätze

Viele Privatpersonen wenden sich an den Datenschutzbeauftragten, weil sie erfahren möchten, welche Daten bei Gemeinde oder kantonaler Verwaltung über sie vorhanden sind.

Voraussetzung einer datenschutzrechtlichen Einsicht in eigene Daten ist die Anwendbarkeit des DSG. Kommt das DSG nicht zur Anwendung,⁶⁴ so ist zu prüfen, wie das Einsichtsrecht aufgrund des diesfalls anwendbaren Rechts umschrieben ist. Hier ist insbesondere darauf hinzuweisen, dass das DSG auf hängige Zivil-, Verwaltungs- und Strafverfahren nicht anwendbar ist.

Ist das DSG anwendbar, so richtet sich das Einsichtsrecht nach § 13 f. DSG. Betroffene haben demnach grundsätzlich volle Einsicht in alle sie betreffenden Akten. Auskunft und Einsicht sind kostenlos⁶⁵, Kopien können in der Regel ebenfalls

63 Vgl. § 4 Bst. d DSG.

64 Aufgrund der in § 3 Abs. 2 DSG aufgeführten Gründe.

65 Vgl. § 17 Abs. 1 DSG.

kostenlos verlangt werden.⁶⁶ Kopiekosten können verrechnet werden, wenn die betroffene Person in der gleichen Sache bereits im gleichen Jahr kostenlose Kopien erhalten hat.⁶⁷

Befinden sich im Dossier Angaben über Drittpersonen, so ist deren Schutz zu gewährleisten, z. B. durch Abdecken oder Schwärzen der entsprechenden Stellen in den Kopien.

15 Einsicht einer Mitarbeiterin der Verwaltung in das eigene Personaldossier

Eine Verwaltungsangestellte möchte in Erfahrung bringen, welche Informationen in ihrem Personaldossier vorhanden sind.

Die Einsichtnahme in das eigene Personaldossier ist jederzeit grundsätzlich vollumfänglich möglich.⁶⁸ Zu beachten ist, dass das Personaldossier in der kantonalen Verwaltung in der Regel doppelt geführt wird. Das Personalamt, das für die Abwicklung der administrativen Belange⁶⁹ zuständig ist, führt eines, zudem die vorgesetzte Stelle⁷⁰ der Mitarbeitenden. Transparenter wäre die zentrale Führung nur eines einzigen Dossiers. Unzulässig ist es, «Geheimakten» anzulegen, die für Mitarbeitende nicht zugänglich sind.

Das Dossier kann beim zuständigen Vorgesetzten bzw. der Personalabteilung während der Arbeitszeit eingesehen werden. Es dürfen unentgeltlich⁷¹ Fotokopien gemacht werden.

Sind in einem Personaldossier Unterlagen von Dritten, ist zu prüfen, ob diese aufgrund eines überwiegenden eigenen Interesses einen Anspruch auf Geheimhaltung beanspruchen können.

16 Sicherheitsüberprüfung der eigenen Verwaltungsmitarbeitenden

Mitarbeitende der öffentlichen Verwaltung können, je nach Funktion und Stellung, Einsicht in sehr viele sensible oder heikle Daten haben. Es fragt sich, welche Vorkehrungen der Arbeitgeber bei der Anstellung, aber auch während des laufenden Arbeitsverhältnisses, ergreifen kann [bzw. auch: darf, muss oder soll?], um die Gewissheit zu haben, dass die eigenen Mitarbeitenden kein Sicherheitsrisiko darstellen. Wir befinden uns im Spannungsfeld zwischen den Sicherheitsbedürfnissen der Verwaltung und dem Recht auf Privatsphäre des Arbeitnehmers. Im Gegensatz zum Bund⁷² ist diese Frage im Zuger Recht nicht ausdrücklich geregelt. Es kommt das auf das Arbeitsverhältnis⁷³ anwendbare Recht zur Anwendung. Es ist hier darauf hinzuweisen, dass der

im Polizeigesetz verankerte allgemeine Polizeiauftrag⁷⁴ keine Grundlage für Sicherheitsüberprüfungen bietet.

Anlässlich der Anstellung besteht, je nach Sicherheitsrelevanz der zu besetzenden Stelle aufgrund des geltenden Arbeitsrechts die Möglichkeit, vom Stellenbewerber selber diesbezügliche Dokumente bzw. Angaben einzufordern. Der Bewerber kann den zukünftigen Arbeitgeber auch autorisieren, gewisse Informationen beschaffen zu dürfen. Nicht erlaubt ist die Datenbeschaffung ohne Zustimmung des Bewerbenden.

Eine Überprüfung während des Anstellungsverhältnisses muss in gewissen Fällen ebenfalls möglich sein. Auch hier steht die Frage nach der Sicherheitsrelevanz, somit nach der Verhältnismässigkeit, im Vordergrund.

Es wäre abschliessend zu begrüssen, wenn diesbezügliche kantonale Vorschriften die vorliegende Frage regeln würden.

17 Sicherheitsüberprüfung von Mitarbeitenden beauftragter externer Unternehmen

Mitarbeitende von Firmen, die Aufträge der öffentlichen Verwaltung erfüllen, können – je nach Auftrag, Funktion und Stellung – Einsicht in sehr viele sensible oder heikle Daten der Verwaltung nehmen. Es fragt sich, welche Vorkehrungen die Verwaltung bei der Vergabe, aber auch während des laufenden Auftragsverhältnisses, ergreifen kann [darf, muss oder soll?], um sicher sein zu können, dass die Mitarbeitenden von beauftragten Firmen kein Sicherheitsrisiko darstellen. Je nach Sicherheitsrelevanz der zu erledigenden Aufgabe sind hier Auftraggeber, Beauftragter und Arbeitnehmer des Beauftragten gefordert.

Auftraggeber: Er ist verpflichtet, mit organisatorischen und technischen Massnahmen dafür zu sorgen, dass der Beauftragte möglichst keinen Zugang zu sicherheitskritischen Daten erhält.

Soweit dies aufgrund des Auftrags nicht möglich ist, ist das beauftragte Unternehmen entsprechend schriftlich zu informieren und zu instruieren [mit explizitem Hinweis auf strafrechtliche Sanktionen⁷⁵ bzw. zivilrechtlicher Haftung im Falle von Verstössen]. Eine Verstärkung kann u. U. durch Vereinbarung einer Konventionalstrafe erreicht werden. Der DSB verfügt über entsprechende Muster-Verpflichtungserklärungen.

66 Vgl. § 17 Abs. 2 DSG.

67 Es gilt sinngemäss die in der Verordnung zum Eid, DSG ISR 235.111 in Art. 2 getroffene Lösung.

68 § 13/14 DSG.

69 Geführt werden grundsätzlich nur Unterlagen im Zusammenhang mit der Begründung des Anstellungsverhältnisses, der Auszahlung des Lohnes, der Abwicklung von Versicherungsfällen bei Unfällen etc.

70 Betreffend Leistung und Verhalten.

71 § 17 Abs. 2 DSG.

72 Vgl. Art. 19 f. Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit [BWIS, SR 120] sowie Verordnung über die Personensicherheitsprüfungen [PSPV, SR 120.4].

73 Bei Zusammenarbeit mit Externen: Auftrags- bzw. Werkvertragsrecht.

74 § 1 Gesetz über die Kantonspolizei [BGS 512.11].

75 Vgl. § 24 DSG.

Beauftragtes Unternehmen: Dieses hat seine Arbeitnehmenden den Anforderungen des Auftrags gemäss auszuwählen und zu instruieren.

Arbeitnehmerinnen des Beauftragten: Sie sind durch den Auftraggeber ebenfalls schriftlich auf die Sicherheitsaspekte aufmerksam zu machen [mit explizitem Hinweis auf strafrechtliche Sanktionen bzw. zivilrechtliche Haftung im Falle von Verstössen]. Diesbezüglich verfügt der DSB ebenfalls über Muster-Verpflichtungserklärungen.

18 Aktenübergabe an NachfolgerIn oder neu zuständige Stelle

Es stellte sich die Frage, wie ein Dossier an die Nachfolgerin, an den Nachfolger oder an die analoge Amtsstelle in einer anderen Gemeinde, einem anderen Kanton zu übergeben ist.

Neben den allgemeinen Grundsätzen der Verwaltung über die Geschäftsführung hilft § 4 DSG weiter. Demgemäss müssen Daten aktuell, richtig und vollständig sein. Dies bedeutet, dass ein Dossier grundsätzlich vollständig zu übergeben ist. Zu entfernen sind doppelt vorhandene Akten; alles Weitere ist zu belassen. Dies gilt insbesondere auch für Handakten.⁷⁶

Es ist vorgängig zu prüfen, ob gegebenenfalls besondere gesetzliche Regelungen anwendbar sind.

19 Veröffentlichung von Personenfotos

Institutionen haben sich erkundigt, ob es Bestimmungen gibt, welche die Publikation von Personenfotos regeln. Als Verwendungszweck wurde die Publikation in Jahresberichten oder Jubiläumsschriften genannt.

Es ist davon auszugehen, dass es sich um eine Institution handelt, die dem DSG untersteht.

Bei der Veröffentlichung von Personenfotos handelt es sich um eine Datenbearbeitung. Damit sie rechtmässig ist, bedarf sie einer gesetzlichen Grundlage. Eine solche dürfte sich wohl kaum finden.

Rechtmässig ist die Publikation jedoch auch dann, wenn die betroffene Person ausdrücklich in die Datenbearbeitung einwilligt. Aus Beweisgründen sollte die Einwilligung schriftlich erfolgen. Besondere Zurückhaltung bei der Publikation von Fotos ist bei Institutionen, die behinderte oder ältere, gebrechliche Personen betreuen, zu fordern. Die Fotos sollten möglichst aus höflicher Distanz aufgenommen werden, damit Einzelpersonen nicht oder nur schwer erkennbar sind.

20 Veröffentlichung von Video- oder Tonaufnahmen von Personen

Zu Ausbildungszwecken kann es geboten sein, Video- oder Tonaufnahmen in therapeutischen Bereichen anzufertigen. Hier ist besondere Vorsicht geboten, handelt es sich doch um besonders schützenswerte Daten. Die ausdrückliche Einwilligung der Betroffenen [ggfs. der gesetzlichen Vertreter] ist notwendig. Die Aufnahmen sind so vorzunehmen, dass möglichst schonend vorgegangen wird.⁷⁷

2.4 Kantonale Behörden

Staatskanzlei

21 Politische Rechte – Amtsgeheimnis bezüglich Referendumsunterzeichnenden

Die Staatskanzlei wurde von einer Verwaltungsstelle angefragt, ob ihr Name und Adresse der Unterzeichnenden eines Referendums bekanntgegeben werden können. Die betreffende Amtsstelle wollte eruieren, wie sich die Gegnerschaft der fraglichen Vorlage zusammensetzt. Interessiert hätte etwa, aus welchen Kreisen und Schichten sowie aus welchen Kantonsgegenden die Unterzeichnenden stammen. Aufgrund dieser Kenntnisse hätte über die Vorlage zielgruppenorientierter informiert werden können. Der DSB kam auf entsprechende Anfrage zum Schluss, dass die fraglichen Angaben nicht bekannt gegeben werden dürfen.

Die Ausübung der politischen Rechte untersteht einem strikten Amtsgeheimnis. Wer ein Referendum unterzeichnet, muss sicher gehen können, dass niemand⁷⁸ von der Ausübung seiner politischen Rechte Kenntnis erhält. Das Unterzeichnen muss in Freiheit erfolgen können. Mögliche Nachteile oder gar Repressionen müssen mit absoluter Sicherheit ausgeschlossen werden. Die Abgabe einer Unterschrift für ein Referendum ist ein Teilaspekt des Abstimmungsgeheimnisses. Im kantonalen Recht ist die vorliegende Frage nicht ausdrücklich geregelt. Der Grund dürfte wohl darin liegen, dass das Abstimmungsgeheimnis in einer freiheitlichen Demokratie derart grundlegend ist, dass es sich dabei um eine nicht weiter zu regelnde Selbstverständlichkeit handelt. Im Bundesrecht ist die Frage bezüglich der Unterschriftenliste von Volksinitiativen explizit geregelt – jegliche Einsicht ist unzulässig.⁷⁹

Das Abstimmungs- und Wahlgeheimnis wird zudem auch durch das Strafrecht geschützt: «Wer sich durch

76 Diese sind scharf zu unterscheiden von Arbeitsinstrumenten gemäss § 3 Abs. 2 Bst. d DSG. Letztere dienen ausschliesslich dem persönlichen Gebrauch und werden nicht an Dritte weitergegeben. Darunter fällt etwa die persönliche Geschäftsagenda, das persönliche Adressverzeichnis. Zum Schutz von Betroffenen ist die letzte Kategorie sehr eng zu fassen.

77 Falls möglich: Aufnahmen von hinten, Detailaufnahme – je nach Situation.

78 Mit Ausnahme derjenigen gesetzlich vorgesehenen Stellen [Einwohnerkontrolle, ggfs. Staatskanzlei], die zu überprüfen haben, ob die Vorschriften bezüglich der Unterzeichnung von Referenden erfüllt sind.

79 Vgl. Art. 71 Abs. 2 Bundesgesetz über die politischen Rechte [SR 161.1]: «Eingereichte Unterschriftenlisten werden nicht zurückgegeben und können nicht eingesehen werden.»

unrechtmässiges Vorgehen Kenntnis davon verschafft, wie einzelne Berechtigte stimmen oder wählen, wird mit Gefängnis oder mit Busse bestraft.»⁸⁰

Hinzuweisen ist schliesslich auch auf den datenschutzrechtlichen Grundsatz der Zweckbindung⁸¹. Die Unterzeichnung eines Referendums dient ausschliesslich der Äusserung des politischen Willens. Keinesfalls sind dabei irgendwelche andere Zwecke abgedeckt.

Das Amtsgeheimnis ist hier strikte zu beachten, es kann keine Bekanntgabe der gewünschten Informationen stattfinden.

Nach durchgeführter Abstimmung werden die unterzeichneten Referendumsbögen übrigens vernichtet.

22 Neuauflage des Staatskalenders – was ist zu veröffentlichen?

Der Staatskalender soll Bürgerinnen und Bürgern darüber Auskunft geben, wer die Mitarbeitenden in der kantonalen Verwaltung sind und wie und wo sie zu erreichen sind. Daneben ist die Zusammensetzung von diversen politischen Institutionen aufgeführt. Anlässlich der Neuauflage 2001/2002 wurde der DSB aufgefordert, seine Stellungnahme zu verschiedenen Fragen abzugeben.

Wohnort der Mitarbeitenden: Diese Information fand sich bis anhin im Staatskalender. Da sie keinen Zusammenhang mit Tätigkeit oder Funktion der Mitarbeitenden hat, war sie zu streichen.

Jahrgang, Beruf und Titel von Kantons- und Regierungsrat: Es handelt sich hier um Personen, die sich freiwillig in der Öffentlichkeit exponieren. In einem gewissen Ausmass haben sie zu dulden, dass Daten aus ihrer Privatsphäre in die Öffentlichkeit gelangen. Der Jahrgang kann für die Frage der Wählbarkeit eine Rolle spielen. Es ist deshalb zulässig, von Kantons- und Regierungsrat die Jahrgänge im Staatskalender zu publizieren.

E-Mail-Adresse von Mitarbeitenden: Es bestand der Wunsch, die E-Mail-Adresse von Mitarbeitenden zu veröffentlichen. Dies ist aus verschiedenen Gründen nicht unproblematisch: unverschlüsselte E-Mails sind nicht sicher, die Verwaltung hat keinerlei Sicherheit bezüglich der Absender⁸², Absender sind fälschlicherweise der Meinung, eine Eingabe per E-Mail hätte den Charakter einer per Post zugestellten Eingabe, Absender mailen in Unkenntnis der Sachlage Vertrauliches oder sensitive Daten etc.

Der DSB verschliesst sich nicht der Tatsache, dass das E-Mail für kurze Nachrichten bezüglich einer Sachfrage ein effizientes und nützliches Arbeitsinstrument ist. Er hat deshalb empfohlen, an gut sichtbarer Stelle im Staatskalender einen entsprechenden Sicherheitshinweis⁸³ anzubringen.

Direktion des Innern

23 Volkszählung 2000

Am 5. Dezember 2000 fand in der Schweiz die Volkszählung statt. Bei der Volkszählung handelt es sich um ein sehr sensibles datenschutzrechtliches Thema, das insbesondere auch von der Öffentlichkeit und den Medien stets mit kritischem Auge beobachtet wurde. Auch wenn kaum jemand Sinn und Zweck von statistischen Erhebungen für Planungszwecke in Frage stellt, so steht doch zuerst einmal im Vordergrund, dass bis zum Zeitpunkt der Anonymisierung der Daten der Staat einen ganzen Strauss von Informationen aus dem Privatbereich der Bevölkerung erhält.

Der DSB wurde mit Regierungsratsbeschluss vom 26. September 2000 als Kontrollorgan⁸⁴ eingesetzt. Gewisse Kontakte mit den verantwortlichen Stellen bestanden seit Ende 1999. Zwei Gemeinden hatten sich dafür entschieden, die Datenbearbeitung der vom Bundesamt für Statistik beauftragten Firma DCL in Kriens zu übertragen. Diese Firma unterstand diversen Aufsichts- und Kontrollinstanzen seitens des Bundesamtes für Statistik, des Eidg. DSB sowie der kantonalen DSB. Der Zuger DSB hat in dieser Konstellation bezüglich dieser beiden Gemeinden keine Kontrollfunktion auszuüben.

Anders verhielt es sich mit den übrigen neun Zuger Gemeinden. Diese übertrugen mit Einverständnis des Regierungsrates gewisse Aufgaben einer kleinen Firma in Zürich. Dem DSB fehlten die Ressourcen, das Projekt im notwendigen Ausmass begleiten zu können. Verschiedentlich zeigte es sich, dass die Sicherheitsaspekte nicht mit der gebotenen Sorgfalt beachtet wurden. Anlässlich einer durchgeführten Kontrolle vor Ort – unter Beizug eines externen Experten – zeigten sich gravierende Sicherheitsmängel. Diese wurden in der Folge aufgrund der Intervention des DSB umgehend von den zuständigen Stellen behoben.

Es hat sich klar gezeigt, dass ein Projekt in dieser Dimension bezüglich Datenschutz und Datensicherheit hätte professionell begleitet werden müssen. Ebenso klar hat sich gezeigt, dass der DSB mit

80 Art. 283 des Strafgesetzbuches ISR 311.01.

81 § 4 Bst. c DSG.

82 Bereits 1993 erschien im «New Yorker» der berühmte Cartoon, in dem ein Hund einem anderen Hund die Vorteile des Internets so erklärt: «On the internet, nobody knows you're a dog».

83 Vgl. Staatskalender, Umschlagseite: «Wichtiger Hinweis Benützung des E-Mails für die Übermittlung von Meldungen Beachten Sie bitte Folgendes: – Meldungen mittels E-Mail zwischen Privaten und der kantonalen Verwaltung und umgekehrt können zurzeit noch nicht verschlüsselt versandt werden. Denken Sie deshalb daran: solche Meldungen können von Dritten gelesen und schlimmstenfalls verändert werden. – Benützen Sie deshalb das E-Mail nicht für die Übermittlung von vertraulichen Meldungen. – In jedem Fall dürfen Meldungen, die Rückschlüsse auf Personen und ihre Daten ermöglichen, nicht elektronisch übermittelt werden. – Weder Private noch die kantonale Verwaltung sind rechtlich an die per E-Mail übermittelten Äusserungen gebunden.»

84 Im Sinne von Art. 35 der Verordnung über die eidg. Volkszählung 2000 ISR 431.112.11.

seinem Arbeitspensum von 65% dazu nicht in der Lage war. Zum Vergleich: die Datenschutzbeauftragten der Kantone Zürich und Fribourg haben für diese Aufgabe je eine auf drei Jahre beschränkte Juristenstelle mit einem 50%-Pensum bewilligt erhalten. Fazit: In Zukunft müssen beim DSB für eine solche Zusatzaufgabe auch zusätzliche personelle Ressourcen zur Verfügung stehen. Auch denkbar ist die Auslagerung bestimmter Kontrollaufgaben durch den DSB an ein spezialisiertes externes Unternehmen. Tröstlich: Die nächste Volkszählung, die uns für 2010 ins Haus steht, wird voraussichtlich nur noch «registertgestützt» durchgeführt werden. Damit wird das Ausfüllen der Papierformulare entfallen und ebenfalls sämtliche Sicherheitsfragen, die mit dem Handling dieser Formulare verbunden sind.⁸⁵

24 Einbürgerungsgesuche: Welche Informationen muss der Kantonsrat haben?

Es war im Rahmen einer Interpellation⁸⁶ zu prüfen, ob der Versand sämtlicher Informationen über einzubürgernde Personen an den Kantonsrat [mit den kantonsrätlichen Vorlagen] rechtmässig ist.⁸⁷

Das Einbürgerungsdossier umfasst Unterlagen aus sehr vielen verschiedenen Persönlichkeitsbereichen der einbürgerungswilligen Person. Viele Daten sind besonders schützenswert, insgesamt handelt es sich um ein Persönlichkeitsprofil. Die Kantonsratsvorlagen sind öffentlich. Würden die vollständigen Einbürgerungsdossiers mit den übrigen Kantonsratsunterlagen verschickt, so würden unzulässigerweise Informationen aus einem inneren Bereich der Privatsphäre an die Öffentlichkeit gelangen.

Eine solche Regelung ist somit aus datenschutz- und persönlichkeitsrechtlichen Gründen nicht rechtmässig. Es ist darauf hinzuweisen, dass die Kommissionen des Kantonsrates befugt sind, in sämtliche Akten eines Beratungsgegenstandes Einsicht zu nehmen und alle zur Erfüllung ihrer Aufgaben notwendigen Auskünfte zu verlangen. Der Persönlichkeitsschutz und die Geheimnisphäre sind dabei zu berücksichtigen, das Amtsgeheimnis zu wahren.⁸⁸

Direktion für Bildung und Kultur

25 Internetnutzung durch Schülerinnen und Schüler

Früher wurden die Grenzen des guten Geschmacks in der Maturazeitung überschritten – heutzutage findet solches im Internet statt.

Was ist davon zu halten, wenn Schüler im Internet Kolleginnen oder Lehrerinnen und Lehrer in mehr oder weniger geschmackloser Art durch den Kakao ziehen oder sogar anzüglich diffamieren? Wie ist die Rechtslage, wenn dies auf Schulservern gemacht wird? Und wenn die Daten auf Servern in den USA gespeichert werden? Detaillierte Antworten können hier nicht gegeben werden; die Grundsätze sind aufzuführen.

Werden Schulserver freigegeben, so sind Nutzung, Kontrolle und Sanktionen bei Verstössen klar zu regeln, entsprechend zu kommunizieren und unterschriftlich zu bestätigen.

Begehen Schülerinnen oder Schüler auf eigenen Web-Sites Persönlichkeitsverletzungen oder gar strafbare Handlungen, so stehen den Betroffenen Rechtsbehelfe zur Verfügung: Klage wegen Persönlichkeitsverletzung bzw. Strafanzeige. Bei Vorfällen in der Kantonschule kann unabhängig davon auch eine Disziplinar massnahme in Frage kommen. Die Kantonschüler haben nämlich die Pflicht, «dem Lehrer und den Mitschülern mit Anstand zu begegnen»⁸⁹. Verstösse dagegen, [wohl] auch wenn in der Freizeit begangen, können Anlass zu Disziplinar massnahmen geben.⁹⁰ Bevor solche Massnahmen ergriffen werden, ist zu bedenken, dass das Internet ein neues Medium ist – auch für die Schule. Information und Ausbildung, nicht Strafen, muss im Vordergrund stehen.

Volkswirtschaftsdirektion

26 EDV-Grundbuch: Zugriff auf sämtliche Daten durch den Leiter des Landwirtschaftsamts?

Die Urkundspersonen benötigen für ihre Arbeit verschiedene Daten aus dem Grundbuch. Sie erhielten diese Angaben früher auf Bestellung beim Grundbuchamt in Papierform. Nachdem der Kanton Zug über ein elektronisches Grundbuch verfügt, wurde geprüft, ob nicht eine elektronische Bestellung mit einer anschliessend automatisierten Daten-Auslieferung eingerichtet werden könnte. Näheres zu diesem Projekt wurde im letzten Tätigkeitsbericht dargelegt.⁹¹

Nun stellte sich die Frage, ob dieser Zugriff auch dem Leiter des Landwirtschaftsamtes gewährt werden kann.

Das Thema ist rechtlich relativ komplex, da verschiedene bundesrechtliche Sonderbestimmungen zur Anwendung kommen. Der DSB gelangt aufgrund der Auslegung der einschlägigen Regelungen

85 Versand/Einsammeln der ausgefüllten Fragebögen, Kontrolle des Rücklaufs, Vollständigkeitskontrolle, Aufbewahrungsprobleme der ausgefüllten Bögen, Mahnwesen etc.

86 Interpellation 837.1-10348 vom 17. Oktober 2000.

87 Vgl. auch die Antwort des Regierungsrates 837.2-10375 vom 21. November 2000.

88 Vgl. § 24 der Geschäftsordnung des Kantonsrates IBGS 141.11.

89 § 9 Gesetz über die kantonalen Schulen IBGS 414.111.

90 § 10 Gesetz über die kantonalen Schulen IBGS 414.111.

91 Vgl. DSB-TB 1999 S. 18 Fall Nr. 19.

im ZGB bzw. der Grundbuchverordnung zum Schluss, dass das geltende Bundesrecht diesen Online-Zugriff nicht zulässt. Der Regierungsrat hat sich dieser Rechtsauffassung nicht angeschlossen und erteilte dem Leiter des Landwirtschaftsamtes – nach Genehmigungserteilung durch die zuständige Bundesbehörde – den gewünschten Online-Zugriff.

27 Handelsregister – was ist alles öffentlich zugänglich?

Eine Firma erkundigte sich, ob es datenschutzrechtlich korrekt ist, wenn auch «gelöschte» bzw. «durchgestrichene» Eintragungen im Handelsregister öffentlich zugänglich sind.

Das DSG ist nicht anwendbar auf öffentliche Register des Privatrechtsverkehrs.⁹² Beim Handelsregister handelt es sich um ein solches. Folglich richtet sich die Bekanntgabe von Personendaten nach dem Handelsregisterrecht. Massgebend ist Art. 930 OR in Verbindung mit der Handelsregister-Verordnung [HRegV]. Sowohl Anmeldungen, Inhalt als auch alle Belege betr. die Eintragungen sind öffentlich. In Art. 12 der HRegV werden auch Löschungen als möglicher Inhalt des Registers erwähnt. Die Bekanntgabe gelöschter Einträge ist somit rechtmässig.

Baudirektion

28 Daten für die Verkehrsplanung: Wo wohnen wie viele Personen?

Das Amt für Verkehrsplanung muss regelmässig Verkehrskonzepte erarbeiten. Dafür sollten Informationen über mögliche Verkehrsströme vorliegen. Es werden Angaben über Wohn- und Arbeitsort benötigt. Wo gewohnt wird bzw. wie viele Personen in jedem Gebäude wohnen, dies weiss die gemeindliche Zivilschutzbehörde. Das Amt für Verkehrsplanung möchte diese Daten, wobei keine Namen benötigt werden.

Gemäss DSG⁹³ dürfen Daten zu Planungszwecken bearbeitet werden, wenn sie anonymisiert werden [sobald es der Zweck des Bearbeitens erlaubt], wenn sie nicht weitergegeben werden und wenn die Publikation der Ergebnisse keine Rückschlüsse auf bestimmte Personen zulässt. Hier werden der Verkehrsplanung bereits anonymisierte Rohdaten geliefert. Die Datenbekanntgabe ist rechtmässig.

92 § 3 Abs. 2 Bst. c DSG.

93 § 4 Bst. d DSG.

94 § 10 Abs. 4/§ 32 Strafprozessordnung (BGS 321.1).

95 DSB Zug TB 1999 S. 20 Fall Nr. 25.

96 DSB Zug 1999 S. 19 Fall Nr. 24.

97 § 9 Abs. 1 DSG.

Sicherheitsdirektion

29 Wenn Private Strafanzeige erstatten: Anspruch auf Anonymität?

Wenn Privatpersonen andere Personen wegen vermuteter Verfehlungen bei der Polizei anzeigen, so stellt sich die Frage, ob der Name des Anzeigenden dem Angezeigten bekannt gegeben werden darf.

Wird eine Anzeige erstattet, so eröffnet die Polizei ein Dossier, das auf den Namen des Angezeigten lautet. Angaben zur Person des Anzeigers werden festgehalten und gehören in das Dossier. Im Verlaufe des Verfahrens wird der Angezeigte ein Recht auf Einsicht in seine Akten haben.⁹⁴ Spätestens dann wird er erfahren, wer die Anzeige gegen ihn eingereicht hat. Diese Offenlegung ist grundsätzlich zu begrüssen. Sie soll verhindern, dass Personen andere Personen anonym denunzieren können.

30 Gebäudeversicherung: Wer erhält die Gebäudedaten?

Im letztjährigen Tätigkeitsbericht⁹⁵ wurde bereits auf dieses Thema eingegangen. Es kann hier nun nachgetragen werden, dass die Versicherten durch den folgenden Hinweis auf der Police informiert werden:

«Die folgenden Daten stellen wir den Einwohnergemeinden zur Verfügung: Name, Vorname und Adresse der Eigentümerschaft sowie allenfalls der beauftragten Verwaltung, Assekuranz- und Grundstücksnummer, Gebäudekubatur, Gebäudebeschreibung [Nutzung, Ausbau, Brandschutzanlagen usw.]. Das Vermessungs- und das Grundbuchamt erhalten ausser diesen Angaben noch den Versicherungswert. Mit der Steuerverwaltung besteht kein Datenaustausch.»

31 Strassenverkehrsamt – Sperrung der Fahrzeughalterdaten?

Die Frage, ob man als Fahrzeughalter seine Daten beim Strassenverkehrsamt sperren lassen kann, wurde an dieser Stelle auch schon letztes Jahr aufgeworfen.⁹⁶ Die Fortsetzung dieses Themas wurde damals versprochen. Dies sei hiermit eingelöst.

Da unterdessen das DSG in Kraft getreten ist, kann jedermann voraussetzungslos – somit: ohne Nennung eines Grundes – seine Daten sperren lassen.⁹⁷ Hingewiesen sei darauf, dass die vorliegende Angelegenheit noch nicht ganz abgeschlossen werden kann. Noch ist eine entsprechende Revision des Strassenverkehrsgesetzes pendent. Der Bundesrat

vertritt die Ansicht, dass die Fahrzeughalterdaten weder an Private bekannt zu geben noch zu veröffentlichen sind.

Gesundheitsdirektion

32 Spital/Klinik: Zur Herausgabe des Originals der Krankengeschichte an Patienten

Wie verhält es sich, wenn Patienten die Originale ihrer eigenen Krankengeschichte [KG] vom Spital herausverlangen? Zu betonen ist, dass es weder um die Herausgabe von Kopien noch um die Einsicht in die KG geht.

Wir betrachten die Rechtslage bezüglich eines Spitals, auf welches das Zuger Datenschutzgesetz anwendbar ist.⁹⁸ Die folgenden Überlegungen können somit nicht ungeprüft auf eine Privatklinik, die nicht dem DSG untersteht, angewendet werden. Es wird im Weiteren davon ausgegangen, dass die Behandlung abgeschlossen ist. Es fragt sich nun – können [dürfen?] die Originalakten herausgegeben werden?

Auszugehen ist von § 11 DSG:

«§ 11 Anonymisieren und Vernichten von Daten
Organe müssen Daten, die sie nicht mehr benötigen, anonymisieren oder vernichten, soweit die Daten nicht unmittelbaren Beweis Zwecken dienen oder dem zuständigen Archiv abzuliefern sind.»

Hier können sich insbesondere beweisrechtliche Fragen stellen: Solange zivil-⁹⁹ oder strafrechtsrelevante¹⁰⁰ Fristen laufen, muss das Spital grundsätzlich über die Originalakten verfügen; somit längstens während 10 Jahren nach Abschluss des Falles. Sind sämtliche Fristen abgelaufen, so stellt sich die Frage nach der Archivierung. Falls nicht zu archivieren ist, sind die Daten zu vernichten. In diesem Fall können die Unterlagen natürlich auch den Betroffenen auf deren Wunsch herausgegeben werden.

Ausnahmsweise kann aber auch eine frühere Herausgabe der KG in Frage kommen. Verlässt jemand die Schweiz definitiv, so kann es durchaus sinnvoll sein, dass sämtliche Akten herausgegeben werden. Das Spital hat sich während des Laufs von Fristen jedoch schriftlich bestätigen zu lassen, dass die Aufbewahrungspflicht vom Patienten übernommen wird und dass zudem das Spital von jeder weiteren diesbezüglichen Verantwortung entbunden wird. Der Klinik ist diesfalls zu gestatten, Kopien von beweisrelevanten Akten während des Fristenlaufs zu behalten.

Ergänzender Hinweis: Der Rechtsdienst FMH hat Mustererklärungen zur Herausgabe von Originalakten ausgearbeitet.¹⁰¹

33 Zwangsmassnahmen im Gesundheitswesen: Zur Datenbekanntgabe an den Kantonsarzt

Anlässlich der Revision des Gesetzes über das Gesundheitswesen sollte der Bereich «Zwangsmassnahmen» ausdrücklich geregelt werden. Der Kantonsarzt sollte die Kompetenz zur Überprüfung der Anordnung von Zwangsmassnahmen erhalten. Es stellte sich nun die Frage, ob es datenschutzrechtlich zulässig sei, dass der Kantonsarzt Einsicht in das vollständige Patientendossier nehmen kann.

Bei der Krankengeschichte handelt es sich um besonders schützenswerte Daten. Diese dürfen bekannt gegeben werden,¹⁰² falls es (1) ein formelles Gesetz ausdrücklich vorsieht, (2) es für eine in einem formellen Gesetz umschriebene Aufgabe offensichtlich unentbehrlich ist oder (3) die betroffene Person im Einzelfall ausdrücklich einwilligt. Im vorliegenden Fall ist die Datenbekanntgabe im Gesetz über das Gesundheitswesen nicht ausdrücklich geregelt. Jedoch ist die Aufgabe, dass der Kantonsarzt angeordnete Zwangsmassnahmen umfassend überprüfen muss, im Gesetz festgelegt. Es leuchtet ein, dass dieser Auftrag nur ausgeübt werden kann, wenn der Kantonsarzt auch Zugang zur Krankengeschichte hat. Die im DSG¹⁰³ aufgestellte Voraussetzung ist hier somit erfüllt. Der Kantonsarzt hat volles Einsichtsrecht in die betreffenden Patientendossiers.

34 Spitalwesen: Ausserkantonale Finanzkontrolle verlangt Patienten-Adressen

Nicht alle Kantone in der Zentralschweiz verfügen über Kliniken, die sämtliche medizinischen Bereiche abdecken. Verschiedene Kantone haben deshalb im Rahmen eines Konkordates Abmachungen darüber getroffen, welche Leistungen an kantonsfremde Spitäler für im eigenen Kanton wohnhafte Personen geleistet werden.

Eine ausserkantonale Finanzkontrolle eines Konkordatskantons verlangt zur Überprüfung der Rechtmässigkeit von verrechneten Leistungen einer Zuger Klinik die Herausgabe von Patienten-Adressen [aufgeschlüsselt nach verschiedenen Gemeinden des eigenen Kantons]. Zu überprüfen ist, ob besagte Patienten tatsächlich im eigenen Kanton wohnhaft sind. Es stellt sich die Frage, ob die Bekanntgabe dieser Patientenadressen an die ausserkantonale Finanzkontrolle rechtmässig ist.

98 Dies ist dann der Fall, wenn es sich um eine öffentliche Aufgabe handelt und für den Kanton gehandelt wird, vgl. § 2 Bst. i DSG.

99 So kann auch nach Jahren noch die Frage nach einer möglichen Fehlbehandlung oder einer fehlerhaften Rechnungsstellung etc. aufgeworfen werden.

100 Falls erst nach Jahren ein Zusammenhang einer Behandlung mit einer strafbaren Handlung entdeckt wird. Die Verjährungsfrist beträgt in der Regel 10 Jahre [Art. 70 Strafgesetzbuch]; Ausnahmen dazu: Mord (20 Jahre, Art. 70 StGB) bzw. gewisse Taten, die unverjährbar sind [Art. 75bis StGB].

101 Diese sind im Internet veröffentlicht: «www.fmh.ch».

102 § 5 Abs. 2 DSG.

103 § 5 Abs. 2 Bst. b DSG.

Ausgangspunkt: Das Anliegen des Konkordatskantons, in geeigneter Weise stichprobenmässig zu überprüfen, ob erfolgte Zahlungen an Zuger Kliniken zu Recht erfolgt sind, ist absolut legitim.

Zu prüfen ist, wie diese Kontrolle rechtmässig durchzuführen ist. Es ist davon auszugehen, dass die fragliche Klinik dem Zuger DSG untersteht. Bei den Patientendaten handelt es sich um besonders schützenswerte Personendaten. Gelangen solche Daten in falsche Hände, können sehr gravierende Persönlichkeitsverletzungen resultieren [z. B. betr. Arbeitsverhältnis/Arbeitssuche eines Betroffenen etc.]. Die berechtigten Interessen der betroffenen Patienten sind zu schützen. Damit nicht zu vereinbaren wäre die direkte Herausgabe der Patientendaten [sortiert nach Gemeinden] an die Finanzkontrolle, welche die Adressen anschliessend bei der Einwohnerkontrolle verifiziert. Zum Schutz der Patienten ist eine Zwischenstelle einzuschalten.

Es wird deshalb empfohlen, die gewünschten Daten dem Kantonsarzt des Konkordatskantons bekannt zu geben. Dieser ist schriftlich zu verpflichten, die Angaben ausschliesslich für diese Überprüfung zu verwenden, sie an keine weiteren Personen bekannt zu geben und sie nach abgeschlossener Überprüfung der Klinik zu retournieren. Der Kantonsarzt nimmt somit die Überprüfung vor, ob die betreffenden Patienten in den entsprechenden Gemeinden wohnhaft sind und erstattet der Finanzkontrolle seines Kantons ohne Namensnennung Bericht.

Finanzdirektion

35 Angaben über Einkommensverhältnisse nach aussen «durchgesickert»?

Ein Staatsangestellter hatte den Verdacht, aufgrund einer Indiskretion seitens der kantonalen Verwaltung hätte seine frühere Ehefrau Angaben über seine Einkommensverhältnisse erhalten.

Abklärungen ergaben, dass keinerlei Indiskretion vorlag. Vielmehr hat die frühere Ehefrau das Personalgesetz¹⁰⁴ zu Rate gezogen: aufgrund der in § 44 aufgeführten Angaben zu den Gehaltsklassen können gewisse Vermutungen angestellt werden. Die Höhe der Familienzulage ist übrigens im Gesetz über die Kinderzulagen¹⁰⁵ veröffentlicht.

36 Steuerverwaltung: Zur Öffentlichkeit des Steuerregisters

Anlässlich der Revision des Zuger Steuergesetzes stellte sich die Frage, ob die Einkommens- und

Vermögensverhältnisse wie bis anhin¹⁰⁶ öffentlich zugänglich sein sollen.

Der DSB nahm im Rahmen einer Anfrage der Finanzdirektion und eines Fachbeitrags in der «Zuger Steuerpraxis» klar Stellung: Fragen des Einkommens und des Vermögens sollten nicht für jede Privatperson öffentlich zugänglich sein. Stichworte¹⁰⁷ zu den Gründen: aus dem steuerlichen Gesamtzusammenhang gerissen, sind diese Angaben nur beschränkt aussagekräftig; mögliche Vertragspartner können die entsprechenden Informationen bei den Betroffenen direkt beziehen; auch der Bund gewährt diesbezüglich keinerlei Einsicht; die Steuerverwaltung, die ihrerseits einer Aufsicht unterstellt ist, ist für den korrekten Vollzug des Steuergesetzes zuständig – nicht die Nachbarschaft.

37 Steuerverwaltung: Auslagerung des Postversands an eine private Firma

Nachdem die Pauschalfrankatur durch die Post nicht mehr angeboten wurde, war die Staatskanzlei beauftragt, zu prüfen, ob Versand und Frankierung der Korrespondenz der gesamten kantonalen Verwaltung nicht kostengünstiger durch ein privates Unternehmen erledigt werden könnte. Outsourcing ist somit das Stichwort. Die Steuerverwaltung hatte Bedenken, ihre Versände einem privaten Unternehmen zur Frankierung anzuvertrauen. Es stellte sich die Frage, ob das Amtsgeheimnis verletzt werden könnte, insbesondere weil die Steuerverwaltung aufgefordert werden sollte, besagter Firma Leercouverts zuzustellen. Damit hätte die Firma maschinenbeschädigte Briefumschläge ersetzen wollen.

Grundsätzlich teilte der DSB die Bedenken der Steuerverwaltung. Bis anhin erfolgten Verpackung und Versand von Steuerunterlagen und Steuerrechnungen verwaltungsintern. Damit war das Amtsgeheimnis optimal gewährleistet.

Nun darf man sich jedoch der Realität nicht verschliessen: gemäss heutigem Trend soll der Staat nicht jedes und alles selber machen. Im Rahmen des Outsourcings können gewisse Aufgaben auch an Private übertragen werden. Das Datenschutzgesetz kennt das Leben – und regelt deshalb die Grundsätze des Datenschutzes beim Outsourcing.¹⁰⁸

Vorliegendenfalls galt es insbesondere sicherzustellen, dass die beauftragte Firma die mit den Versänden befassten Mitarbeitenden entsprechend instruiert. Zudem muss die Firma sowie die mit den Arbeiten beschäftigten Personen eine entsprechende Verpflichtungserklärung¹⁰⁹ unterzeichnen.

Die Zustellung von Leercouverts erachtet der DSB

104 BGS 154.21.

105 § 10 Gesetz über die Kinderzulagen, BGS 844.4.

106 Vgl. § 56 StG – in Kraft bis 31. Dezember 2000.

107 Den Volltext des in der Zuger Steuer Praxis [Oktober 2000/Nr. 14, S. 11–18] erschienen Artikel finden Sie im Archiv der «Mailing-Liste» [via «www.datenschutz-zug.ch»].

108 Vgl. § 6, § 14 Abs. 2, § 24 und § 25 DSG.

109 Vgl. § 6 Abs. 2 DSG.

als unzulässig. Werden beim Frankierungsvorgang Briefumschläge beschädigt, so sind diese der Steuerverwaltung beschädigt zurückzugeben. Beschädigte Umschläge dürfen somit nicht durch die Firma geöffnet und neu verpackt werden.

Unter diesen Bedingungen erachtete der DSB dieses Outsourcing als rechtmässig.

Nachtrag: Offenbar hat sich diese Auslagerung bewährt. Die Steuerverwaltung hat der Firma abmachungsgemäss keine Leercouverts zur Verfügung gestellt – beschädigte Couverts sind ihr bis anhin nicht zugestellt worden.

2.5 Einwohnergemeinden

38 Gemeindliche Dokumentenverwaltung

Eine Gemeinde beschäftigte sich mit einem neuen Dokumentenverwaltungssystem. Verschiedene Fragen sollten diesbezüglich durch den DSB geklärt werden. Es zeigte sich dabei, dass es den Verantwortlichen entgangen war, dass hier gewisse Grundsätze des DSGVO massgebend sind.

§ 11 DSGVO legt nämlich fest, dass Akten, die nicht mehr direkt benötigt werden, so lange bei der entsprechenden Stelle verbleiben, wie sie Beweis zwecken¹¹⁰ dienen. Sind diesbezügliche Fristen abgelaufen, sind die Akten dem zuständigen Archiv anzubieten. Ist dieses an den Akten nicht interessiert, so sind diese entweder zu anonymisieren – dies dürfte wohl die Ausnahme sein – oder zu vernichten. Einen dritten Weg gibt es nicht.¹¹¹ Unzulässig ist insbesondere, selbst ein Archiv anzulegen, Kopien anzufertigen – oder die Akten nicht zu vernichten.

39 Schule: Klassenliste der Schüleradressen

Eine Schule verfasste Klassenlisten, wobei neben der Adresse der Schülerinnen und Schüler auch die gesetzliche Vertretung aufgeführt war. Daraus konnte geschlossen werden, ob die Eltern einer Schülerin, eines Schülers, getrennt oder geschieden sind oder ein Jugendlicher bevormundet ist. Diese Daten sind besonders schützenswert und gehören deshalb nicht auf eine Klassenliste, die für sämtliche Eltern zugänglich ist. Die Schulleitung wird sich zukünftig auf die Adressen beschränken.

40 Einwohnerkontrolle: Welche Daten können an Private bekannt gegeben werden?

Ausgangslage: Die Einwohnerkontrolle [EK] in der Gemeinde verfügt über ein sehr breites Spektrum aktueller und wichtiger Daten über ihre Einwohner-

innen und Einwohner. Bei der Ausarbeitung des DSGVO war klar, dass es exakt festzulegen galt, wer unter welchen Umständen welche Daten von der EK erhalten kann. Keine andere Bestimmung des Gesetzes ist derart konkret und detailliert.¹¹² Trotzdem – es tauchen Fragen rund um die Auskunft an Private auf, insbesondere was die Sammelauskunft betrifft:

Sammelauskunft – gibt es Ausnahmen zur Regelung in § 8 DSGVO?

Nein – § 8 DSGVO enthält eine sehr detaillierte, konkrete und abschliessende Regelung der Sammelauskunft an Private. Es gibt dazu keine Ausnahmen.

Sammelauskunft – und gesperrte Daten?

Gesperrte Daten dürfen nicht in einer Sammelauskunft an Private¹¹³ bekannt gegeben werden.¹¹⁴

Sammelauskunft – kostet das etwas?

Für Sammelauskünfte kann eine Gebühr erhoben werden.¹¹⁵

Sammelauskunft – welche Daten werden bekannt gegeben?

Sammelauskünfte können sich nur auf die sogenannten einfachen Personalien beziehen.¹¹⁶ Festzuhalten ist, dass das Geburtsdatum nicht darunter fällt.

Sammelauskünfte an Banken, Versicherer und Verlagshäuser?

Sammelauskünfte dürfen [u.a.] nur beim Vorliegen schützenswerter ideeller Zwecke erteilt werden, nicht hingegen für wirtschaftliche Zwecke.

Sammelauskunft – Bekanntgabe von Neuzuzügern an Vereine oder politische Parteien?

Aufgrund eines schriftlichen Gesuchs können nicht gesperrte einfache Personalien bekannt gegeben werden. Es ist eine Verpflichtungserklärung zu unterzeichnen, wonach die Adressen ausschliesslich für den bewilligten Zweck verwendet werden. Derartige Auskünfte können ein- bis zweimal jährlich abgegeben werden.

41 Einwohnerkontrolle: Meldung der Geburten an die Mütter- und Väterberatungsstelle?

In der Regel sind diese Stellen in der Rechtsform von Vereinen, also als Subjekte des Privatrechts konstituiert. Da sie jedoch im Auftrag des Kantons öffentliche Aufgaben wahrnehmen,¹¹⁷ sind sie Orga-

110 Zu beachten sind mögliche verwaltungs-, zivil- bzw. strafrechtliche Verfahren. S. dazu auch vorne den Fall 32 auf S. 24.

111 Vorbehältlich ausdrücklicher anderslautender Archivbestimmungen (z.B. betr. Gerichtsakten).

112 Vgl. § 8 und § 9 DSGVO.

113 An andere Organe im Rahmen von § 8 Abs. 2 DSGVO jedoch schon (vgl. § 9 Abs. 1 DSGVO).

114 § 9 Abs. 1 DSGVO.

115 § 17 Abs. 3 DSGVO.

116 Name, Vorname, Geschlecht, aktuelle Adresse und Todestag; vgl. § 8 Abs. 3 Bst. a DSGVO.

ne.¹¹⁸ Die Bekanntgabe an Organe richtet sich nach § 8 Abs. 2 DSGVO – für die Erfüllung ihrer Aufgaben erhalten diese Stellen die Geburtsdaten.

2.6 Bürgergemeinden

42 Datenschutz im Einbürgerungsverfahren¹¹⁹

Welche Daten über Einbürgerungswillige sollen der Bürgergemeinde bekannt gegeben werden?

Im Rahmen des Einbürgerungsverfahrens wird eine grosse Zahl von teilweise sehr heiklen, besonders schützenswerten Personendaten¹²⁰ erhoben. Solche dürfen nur bearbeitet [d.h. erhoben bzw. bekannt gegeben] werden, wenn ein formelles Gesetz dies ausdrücklich vorsieht oder es für eine in einem formellen Gesetz umschriebene Aufgabe offensichtlich unentbehrlich ist.

Es gibt keine formellgesetzliche Grundlage, welche die Datenbearbeitung im Einbürgerungsverfahren explizit regelt. Der Bürgerrat darf jedoch auch besonders schützenswerte Daten erheben¹²¹ – andernfalls könnte er seine im Bürgerrechtsgesetz¹²² umschriebene Aufgabe nicht erfüllen.

Aufgrund des Verhältnismässigkeitsprinzips sind jedoch nur solche Daten zu erheben, die für die Einbürgerung geeignet und erforderlich sind.

Was nun die Bekanntgabe von besonders schützenswerten Daten an die Bürgergemeinde betrifft, so ist auch hier das Verhältnismässigkeitsprinzip zu beachten: es sollen nur diejenigen Daten automatisch bekannt gegeben werden, die für das Fällen eines Entscheides unbedingt notwendig sind. Konkret hiesse dies etwa: Name, Vorname, Adresse, Geburtsdatum, Zivilstand, Datum der Ersteinreise in die Schweiz, Aufenthaltsdauer in der Gemeinde und Beruf.

In der Bürgerversammlung können bei Zweifel an der Einbürgerungsfähigkeit Fragen zu bestimmten Punkten gestellt werden. Aus Gründen des Persönlichkeitsschutzes ist aber grundsätzlich bei der Bekanntgabe von besonders schützenswerten Daten Zurückhaltung zu üben.

Man kann sich fragen, wie sich die Lage verhält, wenn eine einbürgerungswillige Person ausdrücklich damit einverstanden wäre, dass ihre Daten der Bürgergemeinde bekannt gegeben würden. Datenschutzrechtlich dürfen nämlich auch besonders schützenswerte Daten bekannt gegeben werden,

wenn die betroffene Person damit einverstanden ist.¹²³ Diesbezüglich ist sorgfältig zu prüfen, ob damit nicht längerfristig auf indirektem Weg ein Zwang zur Bekanntgabe eingeleitet würde: Wer mit der Bekanntgabe einverstanden ist, hätte grössere Chancen, vor der Bürgergemeinde zu bestehen.

Sehr sinnvoll ist es, die Bürgergemeinde in allgemeiner Weise darüber zu informieren, welche Abklärungen getroffen, wie Informationen erhoben und welche Untersuchungen angestellt werden.

Wenn mit anderen Worten das methodische Prozedere transparent dargelegt wird, damit es für die BürgerInnen nachvollziehbar ist, worauf ein Entscheid des Bürgerrates beruht.

Abzulehnen ist dagegen aus datenschutzrechtlichen Überlegungen eine automatische und vollständige Offenlegung der konkreten Untersuchungsergebnisse im Einzelfall. Dazu ist anzumerken, dass die Form einer Bekanntgabe keine wesentliche Rolle spielt: ob das Dossier auf der Kanzlei einzusehen wäre, anlässlich der Bürgerversammlung auflage oder aber daraus Einzelheiten mündlich bekannt gegeben würden – es handelte sich dabei in jedem Fall um eine unverhältnismässige Datenbekanntgabe. Es genügt, wenn der Bürgerrat in Kenntnis aller erhobenen Informationen Antrag stellt und gegebenenfalls in der Bürgerversammlung punktuell zu Fragen Stellung nimmt.

Im Bürgerrechtsverfahren soll die Devise lauten: «So viel wie nötig – aber nicht mehr.» Zugegeben: Wo genau die Grenzen zu ziehen sind, wird ein Stück weit eine Gratwanderung bleiben.

2.7 Korporationsgemeinden

43 Sammelauskunft – für politische Werbung?

Bei korporationsinternen Wahlen hat sich die Frage gestellt, ob es zulässig ist, einem Korporationsmitglied die Adressliste aller Mitglieder zum Versenden von Wahlpropaganda abzugeben. Die Frage der Zulässigkeit von Sammelauskunften von Korporationsgemeinden richtet sich nach den gleichen Regeln wie sie für die Einwohnerkontrolle gelten.¹²⁴ Die vorstehend gemachten Ausführungen¹²⁵ sind somit auch hier zu beachten.

Fazit: Die Bekanntgabe ist zulässig – die Rahmenbedingungen¹²⁶ sind zu beachten.

117 Aufgrund von § 30 Gesundheitsgesetz (BGS 821.11).

118 Im Sinne von § 2 Bst. i DSGVO.

119 Vgl. dazu auch den Fall Nr. 24 auf S. 22.

120 § 2 Bst. b i.V.m. § 5 Abs. 2 DSGVO.

121 Gestützt auf § 5 Abs. 2 Bst. b DSGVO.

122 § 16 Abs. 1 Bürgerrechtsgesetz (BGS 121.31).

123 Vgl. § 5 Abs. 2 Bst. c DSGVO.

124 § 8 Abs. 4 DSGVO.

125 S. vorne S. 26.

126 § 8 Abs. 3 Bst. c DSGVO.

2.8 Wenn Private Verwaltungsaufgaben übernehmen

44 Wasserwerke Zug AG: Sperrungen von Daten?

Ein Privater verlangt von den WWZ, dass die über ihn vorhandenen Daten zu sperren seien.

Die WWZ sind zwar eine privatrechtliche AG, jedoch sind ihnen öffentliche Aufgaben¹²⁷ übertragen [§ 2 Bst. i DSG]. Sie unterstehen in diesem Bereich somit dem DSG. Jedoch dürfen sie keinerlei Personendaten¹²⁸ an Private weitergeben. Eine ausdrückliche Sperrung ist deshalb weder sinnvoll noch notwendig.¹²⁹

3. Öffentlichkeitsarbeit

3.1 Internet-Auftritt

«www.datenschutz-zug.ch» steht seit Juni 1999 als Datenschutz-Informationsplattform zur Verfügung. Die Web-Site macht die wichtigsten Informationen zugänglich. Der Inhalt wird etwa alle zwei Wochen überprüft und aktualisiert. Im Juni 2000 wurde der Web-Auftritt neu und übersichtlicher gestaltet. Das Echo auf dieses Facelifting war durchwegs positiv. Im Dezember veröffentlichte die Zeitung «Internet Standard» einen ausführlichen Bericht über den Umgang des DSB mit dem Medium Internet.¹³⁰ Eine positive Beurteilung von «www.datenschutz-zug.ch» fand sich auch in der Broschüre¹³¹ «500 nützliche Websites in der Schweiz».

Etwas Statistik ...

Es ist bekannt, zudem wurde auch in diesem Bericht darauf hingewiesen: Wer im Internet surft, macht dies keineswegs unbeobachtet. Grundsätzlich kann mit Hilfe einschlägiger Software jeder Aufruf einer Web-Seite festgehalten und analysiert werden. Auch die Besuchenden der DSB-Web-Site werden von einer Statistikauswertung erfasst. Selbstredend werden dabei nur anonymisierte Angaben ausgewertet.

Angaben statistischer Auswertungen von Web-Besuchen sind in der Regel nur mit allergrösster Zurückhaltung zu geniessen: Aus verschiedenen Gründen¹³² werden oft Besucherzahlen angegeben, die nichts mit der Wirklichkeit zu tun haben¹³³ – und deshalb ist hier der bekannte Satz «Traue keiner Statistik, die Du nicht selber gefälscht hast!» besonders zu beachten. Eine sehr konservative und kritische Analyse der statistischen Angaben hat ergeben,

dass pro Tag durchschnittlich etwa 20–30 einzelne Personen aus der Schweiz die DSB-Web-Site während durchschnittlich etwa 7 Min. besuchen.

Diese Zahl mag vielleicht auf den ersten Blick als eher gering erscheinen. Zu beachten ist jedoch, dass die Statistik kritisch analysiert wurde und zudem, dass es sich um eine sehr spezialisierte Materie handelt. Würde auch nur ein Viertel dieser Personen zum Telefonhörer greifen, um eine gewünschte Information direkt beim DSB zu erhalten, so würde die Warteschlange pender Anfragen noch um einiges länger ...

Fazit: Das DSB-Informationsangebot im Internet wird positiv beurteilt, wird von Interessierten zu Rate gezogen, reduziert die Arbeitsbelastung des DSB und stellt somit eine nützliche, kostenlose¹³⁴ und effiziente Dienstleistung dar.

3.2 Mailing-Liste

Im Juni 2000 wurde das Konzept des Internet-Auftritts geändert. Alle Informationen von grundsätzlicher Bedeutung und einer gewissen Stabilität werden auf der Web-Site veröffentlicht.¹³⁵ Alle aktuellen Informationen aus den Bereichen Datenschutz und Datensicherheit hingegen werden per E-Mail in der Form von Kurz-Hinweisen [versehen mit Links auf Fundstellen, wo sich ausführliche Informationen finden] verschickt.¹³⁶ Diese Dienstleistung kann auf einfachste Weise in Anspruch genommen werden. Es genügt, wenn man auf der entsprechenden Seite der DSB-Web-Site¹³⁷ seine eigene E-Mail-Adresse bekannt gibt.

Wer sich in der Mailing-Liste eingeschrieben hat, wird automatisch mit Kurzinformationen beliefert [zwischen zwei und fünf pro Woche] und ist damit immer auf dem Laufenden. Sämtliche verschickten Nachrichten werden zudem in einer Datenbank gespeichert. Soweit sinnvoll, sind dort zusätzliche Dokumente abgelegt. Die Datenbank ist übrigens via Web-Site auch für nicht eingeschriebene Personen zugänglich.

Der Feedback zu dieser kostenlosen Dienstleistung ist durchwegs positiv. Ohne grosse Werbung haben sich zwischen Juli und Dezember 220 Abonnierte eingeschrieben. In dieser Periode wurden rund 260 Kurz-Mitteilungen verschickt.

In diesem Zusammenhang geht ein spezieller Dank an «Neue Zürcher Zeitung Online», welche die Abspeicherung von NZZ-Beiträgen in der Datenbank der DSB-Mailing-Liste kostenlos erlaubt hat.¹³⁸

127 § 59 Abs. 1 Ziff. 2 Gemeindegesetz [BGS 171.11].

128 Es wäre denkbar, dass zu statistischen Zwecken anonymisierte Daten an Dritte weitergegeben werden.

129 Vgl. zum Sperrrecht S. 6 f.

130 Vgl. Internet Standard, 1. Dezember 2000/48 S. 27 [«In-Sites»] sowie 15. Dezember 2000/50 S. 19 [«Community»].

131 Herausgegeben durch die Zeitung «Internet Standard».

132 In der Werbung richten sich z. B. die Kosten der «Bannerwerbung» nach der Anzahl der Site-Besuchenden etc.

133 Suchmaschinen, eigene Nutzung etc. generieren «Besuche». Zudem werden oft fälschlicherweise «Hits» oder «Seitenimpressionen» anstatt «Sitzungen» ausgewiesen. Zudem ist es ein leichtes, mittels bestimmter Software künstlich Web-Besuche zu generieren, um die Statistik zu eigenen Gunsten zu verfälschen.

134 Für den DSB handelt es sich um eine kostengünstige Lösung.

135 Insbesondere Gesetze, Literatur, Adressen und Links.

136 Verschickt werden Hinweise zu Aktuellem aus Gesetzgebung, Rechtsprechung, Medienberichterstattung, Veranstaltungen und Literatur.

137 «www.datenschutz-zug.ch», Rubrik: «Mailing-Liste/Anmeldung».

138 Die NZZ veröffentlicht auf dem vorliegenden Gebiet regelmässig interessante Beiträge, auf die sich ein Hinweis lohnt. Weil das NZZ-Archiv jedoch – leider – nur während 30 Tagen öffentlich zugänglich ist, ist es nicht sinnvoll, in den E-Mails einen Link auf das NZZ-Archiv zu versenden. Dank der freundlichen Zustimmung von «NZZ Online» dürfen diese NZZ-Beiträge nun in der Datenbank der DSB-Mailing-Liste abgelegt werden. Dadurch sind diese Beiträge im Archiv der Mailing-Liste stets greifbar.

3.3 Medienarbeit

Es gab diverse Gelegenheiten, das Thema Datenschutz einer breiteren Öffentlichkeit näher zu bringen. Die Zuger Printmedien sowie Radiostationen berichteten u. a. über den Gesetzgebungsprozess des Datenschutzgesetzes [im Vorfeld der kantonsrätlichen Beratungen, anlässlich der beiden Lesungen im Kantonsrat, bei Inkrafttreten Anfang Dezember 2000], über den DSB-Internetauftritt, über die «DSB-Mailing-Liste» und über die Veröffentlichung des DSB-Tätigkeitsberichts 1999. Verschiedentlich berichteten die Medien auch aus aktuellem Anlass. Es ist darauf hinzuweisen, dass es erfreulicherweise keinen Anlass gab, über gravierende datenschutzrechtliche Vorfälle oder gar Skandale zu berichten. Im Zusammenhang mit der Revision des Steuergesetzes verfasste der DSB einen Beitrag zum Thema «Öffentliches Steuerregister und Datenschutz/ Einkommen und Vermögen – Privatsache?».¹³⁹

3.4 Datenschutz im Weiterbildungsangebot der kantonalen Verwaltung

Kurs Datenschutz

Am 17. November 2000 führte der DSB erstmals für Führungskräfte einen halbtägigen verwaltungsinternen Einführungskurs ins Datenschutzrecht durch [«Datenschutz – eine Kurzeinführung»]. Der Kurs stiess nur auf ein geringes Interesse [6 Personen] – jedoch waren die Kursteilnehmenden mit dem Gebotenen durchwegs zufrieden. Für diese hatte die geringe Beteiligung sein Gutes, bestand doch die Möglichkeit, auf konkrete Anliegen aus dem eigenen Arbeitsbereich vertieft eingehen zu können. Diese Erfahrung hat gezeigt, dass sich ein Weiterbildungsangebot zukünftig auf ein klar definiertes Publikum ausrichten muss, das zum geplanten Weiterbildungsanlass gezielt einzuladen ist [z. B. «Datenschutz in der Sozialarbeit», «Datenschutz im polizeilichen Bereich» oder «Datenschutz und Schule»]. Daneben müssten gewisse Grundlagen flächendeckend geschult werden. Insbesondere die Grundlagen der sicheren Arbeit mit dem PC, korrekte Nutzung von E-Mail und Internet sowie die Grundsätze des Datenschutzrechts. Diese Aufgaben kann der DSB nicht selber durchführen. Er kann nur Anstösse und inhaltliche Vorgaben für entsprechende Ausbildungsprojekte liefern.

Tätigkeitsbericht 1999

Um die Verwaltungsmitarbeitenden für das Thema

Datenschutz/Datensicherheit zu sensibilisieren wurde ein ausführlicher Tätigkeitsbericht 1999 verfasst, der mit der Personalzeitschrift an sämtliche kantonale Mitarbeitenden, an die Gemeinden sowie an weitere interessierte Stellen verschickt wurde. Die Auflage betrug 2200 Exemplare – Ende 2000 war die Auflage restlos vergriffen. Wer diese Publikation zu Rate ziehen möchte, kann sich auf der DSB-Web-Site eine layoutgetreue Kopie ausdrucken.

Der Tätigkeitsbericht ist ein Forum, das die Themen Datenschutz und Datensicherheit breit vermittelt.

3.5 DSB-Vortragstätigkeit

Es gab zahlreiche Gelegenheiten im Rahmen von Referaten, Kurz-Präsentationen oder Sitzungen über datenschutzrechtliche Anliegen zu informieren. Diese Veranstaltungen sind wichtig, ermöglichen sie doch die direkte Information, vertiefte Diskussionen und nicht zuletzt – eine kritische Auseinandersetzung.

4. Mitarbeit bei der Gesetzgebung

Im Rahmen verschiedener Gesetzgebungsarbeiten hat der DSB mitgearbeitet oder Stellung bezogen. Zum Teil eher punktuell, zum Teil in grösserem Ausmass. Grundsätzlich ist die Arbeit im Rahmen der Gesetzgebung wichtig, können durch frühzeitiges Einbringen der datenschutzrechtlichen Anliegen auf der generell-abstrakten Ebene spätere Datenschutz-Konflikte verhindert werden.

4.1 Datenschutzgesetz des Kantons Zug

S. dazu die Ausführungen vorne S. 5 ff.

4.2 Archivgesetzgebung

Gemäss dem Bundesgesetz über die Archivierung¹⁴⁰ leistet die Archivierung einen Beitrag zur Rechtssicherheit sowie zur kontinuierlichen und rationalen Verwaltungsführung. Sie schafft insbesondere die Voraussetzungen für die historische und sozialwissenschaftliche Forschung. Archiviert werden rechtlich, politisch, wirtschaftlich, historisch, sozial oder kulturell wertvolle Unterlagen des Bundes.

Das Zuger Archivwesen wird zurzeit in einer Verordnung aus dem Jahre 1982 nur sehr lückenhaft geregelt.¹⁴¹ Es besteht Handlungsbedarf, rechtlich sauber zu definieren, was mit den Daten zu geschehen hat, die von der Verwaltung nicht mehr benötigt werden.¹⁴²

¹³⁹ Vgl. Zuger Steuer Praxis, Oktober 2000/Nr. 14, S. 11–18. Dieser Artikel ist im Archiv der «Mailing-Liste» unter «www.datenschutz-zug.ch» zugänglich.

¹⁴⁰ Art. 2 BG über die Archivierung (ISR 152.11).

¹⁴¹ Verordnung über das Staatsarchiv (BGS 152.4).

¹⁴² Es ist darauf hinzuweisen, dass § 11 DSGVO vorschreibt, dass Daten, die nicht mehr benötigt werden, zu archivieren sind. Falls sie nicht archivwürdig sind, sind sie zu anonymisieren oder zu vernichten.

Der Regierungsrat hat deshalb am 28. März 2000 die Staatskanzlei beauftragt, eine Gesetzesvorlage auszuarbeiten. Es wurde eine Arbeitsgruppe der Staatskanzlei gebildet¹⁴³, die an insgesamt 10 Sitzungen einen Gesetzesentwurf erarbeitete. Dieser ging im Januar 2001 in ein verwaltungsinternes Mitberichtsverfahren.

4.3 Revision des Steuergesetzes

Im Zusammenhang mit dem neuen Zuger Steuergesetz hat der DSB die Nichtöffentlichkeit des Steuerregisters [§ 108 StG] aus datenschutzrechtlicher Sicht ausdrücklich begrüsst. Er hat in diesem Zusammenhang einen Beitrag in der «Zuger Steuerpraxis»¹⁴⁴ veröffentlicht. Darüber wurde auch in der Tagespresse und im Radio berichtet. Aufgrund des seit dem 1. Januar 2001 in Kraft stehenden Steuergesetzes erhalten Private keine Auskünfte mehr aus dem Steuerregister über Einkommens- und Vermögensverhältnisse von Steuerpflichtigen.

4.4 Vernehmlassungen

Bundesrecht

Bundesrecht spielt auch für den Kanton eine zentrale Rolle, wird es doch in der Regel durch kantonale Behörden vollzogen. Es ist deshalb wichtig, sich schon bei der Schaffung von Rechtserlassen zu beteiligen. Aus Kapazitätsgründen können Vernehmlassungen durch den DSB jedoch nur sehr beschränkt erarbeitet werden. Es ist aber darauf hinzuweisen, dass in der Regel der Eidg. DSB den datenschutzrechtlichen Aspekt einbringen kann. Im Übrigen darf die Bedeutung einer Zuger Stellungnahme auch nicht überschätzt werden.

Trotzdem – bei wichtigen Vorlagen wurde versucht, ein paar Gedanken in die Berner Gesetzesmaschinerie einzuspeisen. Sehr hilfreich sind dabei die Grundlagenpapiere, die vom schweizerischen Verband der Datenschutzbeauftragten¹⁴⁵ erarbeitet werden.

– Verordnung über das automatisierte Administrativmassnahmen-Register [ADMAS-Verordnung]

– Bundesgesetz über die Öffentlichkeit der Verwaltung [Öffentlichkeitsgesetz, BGÖ]

– Bundesgesetz für Ausländerinnen und Ausländer [Ausländergesetz, AuG]

– Strafbare Handlungen gegen den Geheim- und Privatbereich: Nicht strafbare Handlungen gemäss Art. 179^{quinquies} Strafgesetzbuch.

Kantonales Recht

Auf zwei Arten leistete der DSB im Berichtsjahr hier Input: einerseits durch direkte Mitarbeit bei Gesetzesprojekten¹⁴⁶, andererseits wurde er punktuell um Stellungnahmen bei konkreten Fragen zu laufenden Gesetzesvorhaben angegangen. Datenschutzrelevante Mitberichtsverfahren fanden jedoch keine statt. Oder – die betreffenden Projekte gelangten nicht bis zum Datenschutzbeauftragten ...

5. Register der Datensammlungen

Das DSG verpflichtet die kantonale und die gemeindlichen Verwaltungen dazu, bis Ende 2002 ein Register grundsätzlich aller¹⁴⁷ durch sie geführten Datensammlungen zu erstellen. Dies hat in erster Linie den Zweck, der Bevölkerung zu ermöglichen, die sie betreffenden Daten einsehen zu können. Daneben ist eine solche Bestandesaufnahme aber auch ein günstiger Zeitpunkt für die Verwaltung, kritisch zu hinterfragen, ob die vorhandenen Datensammlungen zu Recht geführt sind, inhaltlich in Ordnung – bzw. sachlich überhaupt notwendig sind.

Die Zuger Einwohnergemeinden haben dies erkannt und die Aufgabe nicht als lästige Pflichtübung verstanden. Vielmehr haben sie sich zu einem gemeinsamen und professionellen Projekt zusammengeschlossen. Für dieses mustergültige Vorgehen verdienen die Einwohnergemeinden uneingeschränktes Lob.

[Ausblick auf 2001: in den beiden Pilotgemeinden Baar und Hünenberg werden in Zusammenarbeit mit einer externen Beratungsfirma, dem DSB sowie der Direktion des Innern die vorhandenen Datensammlungen erhoben, anschliessend wird ein «Musterordner» erarbeitet. Darauf gestützt können die übrigen neun Gemeinden das Register selbständig erarbeiten. Der DSB stellt den Gemeinden kostenlos eine EDV-Lösung zur Verfügung, die es erlaubt, das Register im Internet zu veröffentlichen. Die kantonale Verwaltung sowie die übrigen Gemeindearten werden in einem nächsten Schritt die gleiche Aufgabe zu bewältigen haben.]

6. Kontrolle

Grundsätzliches

Der DSB führte im Berichtsjahr keine systemati-

143 Zusammensetzung:
Dr. Peter Hoppe/Staatsarchivar,
lic. iur. Bruno Zimmermann und
Dr. René Huber/DSB.

144 Oktober 2000/Nr. 14 S. 11–18.

145 S. dazu hinten S. 31/Kapitel II.
Ziff. 7.

146 S. dazu vorne S. 29/Kapitel II.
Ziff. 4.

147 Ausnahmen gemäss § 12 Abs. 2
DSG: Hilfsdatensammlungen
(gemäss Umschreibung in § 2
Bst. e DSG) und Datensammlungen,
die nur bis maximal sechs Monate
geführt werden.

sehen Inspektionen durch. Nachdem die Rechtsgrundlage des Datenschutzes erst gegen Ende Jahr in Kraft getreten ist, ist das Vorgehen: Instruktion, Hilfestellung und erst dann Kontrolle. Selbstverständlich wurde bei der Behandlung von Problemen auf festgestellte Sicherheitslücken [etc.] hingewiesen.

Volkszählung 2000

S. dazu vorne Fall Nr. 23 S. 21.

7. Zusammenarbeit mit dem Eidg. und den kantonalen Datenschutzbeauftragten

Seit 1994 besteht ein lockerer Zusammenschluss der kantonalen Datenschutzbeauftragten und dem Eidg. Datenschutzbeauftragten. Um Zusammenarbeit und Aussenwirkung zu stärken, wurde am 28. März 2000 der Verein «DSB+CPD.CH»¹⁴⁸ gegründet. Er umfasste Ende 2000 die DSB von 25 Kantonen sowie den Eidg. DSB. Zur Struktur: Das «Büro» [=Vorstand] erledigt alle laufenden Geschäfte und die Medienarbeit, verfasst bei wichtigen Vernehmlassungen¹⁴⁹ Eingaben zu Handen der kantonalen DSB und organisiert Weiterbildungsveranstaltungen. Daneben findet die Zusammenarbeit in Arbeitsgruppen¹⁵⁰, in Plenumsveranstaltungen und in Rundschreiben statt. Der Schreibende betreut eine vereinsinterne Web-Site als Informationsplattform. Durch die Gründung des Vereins konnte die frühere lockere und unverbindlichere Zusammenarbeit in eine besser organisierte Struktur überführt werden.

Kooperation mit dem Datenschutzbeauftragten der Stadt Zürich

Am 20. Dezember 2000 wurde der Schreibende vom Gemeinderat der Stadt Zürich zum Stellvertreter des DSB der Stadt Zürich gewählt. Es handelt sich dabei um ein Nebenamt, das etwa einem 5%-Pensum entspricht. Durch diese Zusammenarbeit werden sich wertvolle Synergien für den Datenschutz im Kanton Zug ergeben.

8. Näheres zur Datenschutzstelle

Allgemeines

Die Datenschutzstelle besteht nur aus dem Datenschutzbeauftragten. Dessen Arbeitspensum betrug im Berichtsjahr 65%. Das DSB-Sekretariat wird von

Hildegard Steiner von der Staatskanzlei betreut. Für die weitere administrative Unterstützung konnte auf die Staatskanzlei zurückgegriffen werden.

Stellvertretung

Im Berichtsjahr musste die Frage der Stellvertretung in grundsätzlicher Hinsicht geregelt werden. Eine diesbezügliche gesetzliche Vorschrift ist nicht vorhanden. Der DSB kann die Frage deshalb in eigener Kompetenz lösen.

Freundlicherweise hat sich der Landschreiber Dr. Tino Jorio bereit erklärt, die Stellvertretung zu übernehmen. Es hat sich jedoch gezeigt, dass die ferienbedingten Abwesenheiten des DSB und seines Stellvertreters sehr oft zusammenfallen. Den Ratsuchenden sollte jedoch grundsätzlich stets eine Ansprechperson in Sachen Datenschutz zur Verfügung stehen.

In der Person von Dr. iur. Rolf Bründler, Rechtsanwalt in Luzern, konnte ein externer Fachmann gefunden werden. Rolf Bründler war von 1990 bis Anfang 2000 der Datenschutzbeauftragte des Kantons Luzern. Nun ist er als selbständiger Rechtsanwalt in Luzern tätig.

Die Stellvertretung konnte somit mit zwei bestens qualifizierten Fachleuten besetzt werden. Da die beiden Stellvertreter pro Jahr nur je etwa während zwei Wochen «einsatzbereit» sein müssen, zudem über den Geschäftsgang der Datenschutzstelle nicht im Bild sind, handelt es sich um eine Anlaufstelle für datenschutzrechtliche «Notfälle». Die Stellvertretung ist nicht befugt, in folgenden Fällen aktiv zu werden: in nicht dringlichen Angelegenheiten, bei laufenden Projekten, sich gegenüber den Medien zu äussern und in heiklen oder umstrittenen Materien eine Stellungnahme abzugeben.

Weiterbildung

Der Zuger Datenschutz findet nicht im luftleeren Raum statt. Die Einbettung in den überregionalen, nationalen und auch internationalen Kontext ist wichtig. Es muss versucht werden, rechtzeitig wichtige Tendenzen, Strömungen und Neuerungen zu erkennen – nicht nur im Bereich des Datenschutzes, sondern darüber hinaus auch bezüglich Verwaltungsmanagement und insbesondere auch bezüglich der Informatik. Der DSB hält sich [u. a.] durch den Besuch entsprechender Weiterbildungsveranstaltungen auf dem Laufenden.

148 «Die schweizerischen Datenschutzbeauftragten – Les Commissaires suisses à la protection des données».

149 Revision von Art. 179^{quater} Strafgesetzbuch [Geheim-/Privatsphäre, nicht strafbare Handlungen], Entwurf eines Ausweisgesetzes, Entwurf eines Öffentlichkeitsgesetzes des Bundes, Ausländergesetz.

150 Folgende Arbeitsgruppen sind tätig: «AG Informationstechnologie», «AG Innere Sicherheit», «AG Gesundheit» sowie «AG Statistik/VZ2000».

III. Ein paar Tipps für Sie als ...

1. Bürgerin/Bürger

Lassen Sie Ihre Daten sperren

Auch wenn Sie kein Verbrecher sind – schützen Sie Ihre Privatsphäre und lassen Sie Ihre Daten sperren, wo es möglich ist. Die Folge: Ihre Daten werden grundsätzlich nicht mehr an Private weitergegeben. Das Datenschutzgesetz stellt Ihnen dieses Instrument im DSG ausdrücklich zur Verfügung.¹⁵¹

Wie vorne dargelegt¹⁵², ist die Sperre bei der gemeindlichen Einwohnerkontrolle und dem Strassenverkehrsamt sinnvoll. Die übrigen Verwaltungsstellen dürfen grundsätzlich keine Daten an Private weitergeben, deshalb sind die Daten auch nicht zu sperren. So sperren Sie Ihre Daten: Bei der entsprechenden Stelle ist die Sperrung schriftlich, jedoch voraussetzungslos – somit ohne Begründung –, zu verlangen. Die Sperrung ist kostenlos.

Zurückhaltung ...

sollten Sie überall dort üben, wo von Ihnen persönliche Daten verlangt werden. Das gilt gegenüber dem Datenhunger der Wirtschaft – aber auch der öffentlichen Verwaltung. Oft können wir Sinn und Zweck einer Datenerhebung gar nicht richtig durchschauen. Erinnern Sie sich noch an frühere Puzzle-Spiele? So ist es hier: Das Zusammensetzen auch vieler sehr kleiner Teile ergibt ein schönes Bild – über Sie. Seien Sie deshalb kritisch!

Wollen Sie auf dem Laufenden bleiben?

Wenn Sie auf dem Gebiet des Datenschutzes und der Datensicherheit regelmässig über Aktuelles per E-Mail informiert sein möchten, schreiben Sie sich in die DSB-Mailing-Liste ein. Alles Nähere dazu finden Sie vorne auf S. 28.

Haben Sie Fragen? Ist Ihnen etwas unklar? Wenden Sie sich an den Datenschutzbeauftragten.

¹⁵¹ § 9 Abs. 1 DSG.

¹⁵² S. S. 6 f.

¹⁵³ § 29 Gesetz über das Arbeitsverhältnis des Staatspersonals (Personalgesetz, BGS 154.211) sowie § 11 Personalverordnung (BGS 154.211).

¹⁵⁴ Bezüglich E-Mail, Internet, Fax, Telefon und Korrespondenz; s. dazu vorne S. 14 ff. sowie den DSB-Tätigkeitsbericht 1999 S. 12–16.

2. Mitarbeiterin/Mitarbeiter der Verwaltung

Amtsgeheimnis und Datenbekanntgabe

Grundsätzlich stehen alle Informationen, die im Zusammenhang mit der Ausübung der Arbeit stehen, unter dem Amtsgeheimnis¹⁵³. Es kann nicht oft genug wiederholt werden: Das Amtsgeheimnis gilt auch innerhalb der Verwaltung! Die Daten der Verwaltung befinden sich nicht in einem grossen Suppentopf – wobei jede und jeder nach Lust und Laune daraus schöpfen darf. Vielmehr gilt: Man arbeitet nur mit denjenigen Daten, die für die Erfüllung der eigenen Aufgabe zwingend notwendig sind. Alles andere geht einen nichts an. Somit gilt der Grundsatz: Diejenigen Informationen, zu denen man Zugang hat, werden nicht weitergegeben.

Datensicherheit an Ihrem Arbeitsplatz

Sie bearbeiten Daten von Bürgerinnen und Bürgern. Darunter viele heikle, besonders schützenswerte. Seien Sie sich dieser besonderen Verantwortung bewusst. Halten Sie sich an die Sicherheitsvorschriften und Sicherheitsgrundsätze wie sie hier dargestellt werden.¹⁵⁴

Denken Sie daran: Personendaten dürfen nicht unverschlüsselt via Internet-E-Mail verschickt werden.

Lassen Sie an Ihrem Arbeitsplatz keine Akten offen herumliegen. Beim Verlassen ist das Pult leer, die Akten sind sicher verschlossen – das «clean desk»-Prinzip ist wichtig. Schliessen Sie Ihr Büro auch bei nur kurzer Abwesenheit ab.

Die Sicherheitsanforderungen der IT-Infrastruktur können Sie nicht selber bestimmen, sie wird Ihnen vorgegeben. Jedoch sind Sie für die Einhaltung aller Sicherheitsbestimmungen verantwortlich, die Ihren Arbeitsbereich betreffen. Stellen Sie Mängel fest, so sind Sie verpflichtet, die verantwortlichen Stellen zu informieren [Vorgesetzte, IT-Verantwortliche].

Wollen Sie auf dem Laufenden bleiben?

Wenn Sie auf dem Gebiet des Datenschutzes und der Datensicherheit regelmässig über Aktuelles per E-Mail informiert sein möchten, schreiben Sie sich in die DSB-Mailing-Liste ein. Alles Nähere dazu finden Sie vorne auf S. 28.

Haben Sie Fragen? Ist Ihnen etwas unklar? Wenden Sie sich an den Datenschutzbeauftragten.

1. Zur Arbeit des Datenschutzbeauftragten

Auf dem vorliegenden Gebiet ist für das Jahr 2001 nicht mit massiven Umwälzungen zu rechnen. E-Government oder etwa die Schaffung eines zentralen Datenpools sind keine Themen; ebenso wenig das Outsourcen der kantonalen Informatik. Zu Letzterem: Der DSB geht entschieden davon aus, dass das Datenhandling zum Kerngeschäft des Kantons gehört und IT-Dienstleistungen deshalb durch verwaltungseigene Stellen zu erbringen sind. Auch Überlegungen bezüglich der Datensicherheit, des Vertrauens durch Bürgerinnen und Bürger in das staatliche Datenhandling, die Zuordnung der obersten Verantwortung beim Regierungsrat, aber insbesondere auch Gründe der Kontinuität¹⁵⁵ führen zu diesem Schluss.

Ein wirkungsvoller Datenschutz kann nicht in einem Tag etabliert werden. Auch nicht in einem Jahr. Der Datenschutzbeauftragte muss sich aus Gründen der ungenügenden personellen Ressourcen strenge Prioritäten setzen und sich auf zentrale Themen beschränken. Folgendes ist für 2001 vorgesehen:

– IT-Security: Mitarbeit bei der Schaffung der Verordnung über Informationssicherheit¹⁵⁶ sowie der Weisung zur Nutzung von E-Mail und Internet in der Verwaltung; Begleitung der Implementierung von IT-Security-Massnahmen.

– Umsetzung des DSG: Die Verwaltung muss wissen, welche Anforderungen das Zuger DSG an sie stellt – dazu wird der DSB Unterstützung anbieten.

– Register der Datensammlungen: Es ist das Konzept sowie ein Muster für die Einwohnergemeinden zu erarbeiten und die Umsetzung in den Einwohnergemeinden zu realisieren. Der DSB wird eine internettaugliche EDV-Lösung bereitstellen, die es Kanton und Gemeinden erlauben wird, ihre Register im Internet zu veröffentlichen. Der Zuger Bevölkerung wird damit eine zentrale, öffentlich zugängliche Anlaufstelle zur Verfügung gestellt.

– Schulung: Es ist ein Konzept zu erarbeiten, wie die Themen Datenschutz und Datensicherheit sämtlichen Mitarbeitenden in der öffentlichen Verwaltung vermittelt werden können.

– Archivgesetz: Der DSB ist an der Ausarbeitung der neuen Archivgesetzgebung mitbeteiligt. Mitte 2002 sollte diese in Kraft gesetzt werden können.

– Daily business: ist im bisherigen Rahmen zu erledigen.

2. Zur Lage im Kanton Zug

Bitte kein Rosinenpicken!

Im Rahmen der Revision des Steuergesetzes stellte sich die Frage, ob die Einkommens- und Vermögensverhältnisse wie bis anhin durch jedermann einsehbar sein sollen. Die Stellungnahme des DSB lautete in dieser Frage klar: Einkommens- und Vermögensverhältnisse sind Privatsache und somit nicht für jedermann einsehbar.¹⁵⁷

Reaktionen darauf zeigten: Jene Seite, die den Schutz der Privatsphäre generell als wichtig erachtet, reagierte mit Unverständnis – umgekehrt kam positiver Feedback von Personen, bei denen das Thema Datenschutz nicht zuoberst auf der Prioritätenliste steht.

Für beide gilt: Datenschutz ist kein Selbstbedienungsladen, in dem man nimmt, was gerade gut ins eigene Konzept, zu den eigenen Interessen passt.

Der Schutz der Privatsphäre der Bürgerinnen und Bürger ist vielmehr ein verfassungsmässig verankertes Grundrecht, das konsequent und unabhängig vom politischen Tagesgeschäft zu beachten und zu schützen ist.

Bitte nicht immer gleich die Gesetzgebungsmaschine anwerfen!

Das DSG ist als Querschnittsmaterie grundsätzlich auf sämtliche Bereiche der öffentlichen Verwaltung anwendbar und regelt nur die grossen Linien.

Das DSG verlangt in § 5 für jede Datenbearbeitung eine gesetzliche Grundlage. Durch die Schaffung einer gesetzlichen Grundlage kann grundsätzlich mehr oder weniger jede Datenbearbeitung – darunter fallen insbesondere auch die Datenbekanntgabe oder der Datenaustausch – als zulässig erklärt werden. Im Berichtsjahr zeigte es sich, dass die Zuger Verwaltung¹⁵⁸ sehr schnell bereit ist, die Gesetzgebungsmaschine anzuwerfen, um Datenbekanntgabe und Datenaustausch durch Schaffung von gesetzlichen Grundlagen als zulässig zu erklären.

Hier ist Zurückhaltung zu fordern. Der Schutz der Privatsphäre darf nicht in kleinen Schritten, somit fast unbemerkt, Stück für Stück demontiert werden – bis wir nur noch eine inhaltslose Hülle vor uns haben.

Das Grundrecht auf Datenschutz darf nicht leichtfertig auf dem Altar der Effizienz geopfert werden.

155 Die IT-Branche ist sehr instabil: Unternehmen jeglicher Grösse können übernommen werden, sich zusammenschliessen – oder aber auch untergehen. Solchen Risiken darf die öffentliche Verwaltung das Datenhandling, aber auch die Daten von Bürgerinnen und Bürgern, nicht aussetzen.

156 Aufgrund von § 7 Abs. 2 DSG muss der Regierungsrat bis am 8. Dezember 2001 eine diesbezügliche Verordnung erlassen.

157 Näheres dazu s. vorne S. 25.

158 Betr. «gewöhnlich» schützenswerten Daten. Bezüglich besonders schützenswerten Daten ist ein formelles Gesetz notwendig, somit ist neben der Verwaltung auch der Kantonsrat einbezogen.

«Datenschutz ist gar nicht so langweilig wie ich dachte ...»

Anlässlich von Referaten, Diskussionen und in vielen Gesprächen wird immer wieder deutlich, dass viele Verwaltungsmitarbeitende nicht genau über Datenschutz und Datensicherheit im Bild sind. Sobald jedoch die abstrakte Materie mit Leben gefüllt wird, konkret wird, ist durchaus ein grosses Interesse am vorliegenden Thema festzustellen. Damit sind gute Voraussetzungen für Schulung vorhanden. Flächendeckende Ausbildung in Datenschutz und insbesondere auch Datensicherheit ist ein «Muss» für jede kompetente öffentliche Verwaltung.

3. Sind bald andere Dimensionen angesagt?

An dieser Stelle stand im letztjährigen Bericht: «Das Thema Datenschutz – insbesondere auch der Aspekt der Datensicherheit – wird in den nächsten Jahren massiv an Bedeutung gewinnen. Die Möglichkeiten der Datenbearbeitung werden durch die ständige Weiterentwicklung der Technologie ungeahnte Masse annehmen. Damit nimmt auch die Bedrohung der Privatsphäre und der Grundrechte des Einzelnen zu.»

Diese Tendenz hat auch im Berichtsjahr weiter zugenommen: Der Einsatz von DNA-Analysen im polizeilichen Bereich wird forciert, täglich werden neue Video-Überwachungsanlagen installiert, neue Möglichkeiten der Überwachung der Mitarbeitenden im papierlosen Büro stehen vor der Tür,¹⁵⁹ zudem geht die Durchdringung von Arbeitswelt und Freizeit durch die Technik ungebremst weiter; ebenso die zunehmende Verknüpfung aller über uns vorhandenen Daten.

Zwei Hauptmotoren der Bedrohung des Privaten sind auszumachen. Von staatlicher Seite sind es Sicherheitsaspekte und Kostenersparnis – auf privater Seite kommerzielle Interessen.

Zu beachten ist jedoch: Wir sind nicht alle Verbrecher. Es dürfen deshalb nicht Privatsphäre und Freiheit von uns allen eingeschränkt werden, weil gewisse Personen gegen Regeln verstossen. Ebenso wenig dürfen Effizienzsteigerungen mit einem geringeren Schutzniveau bezahlt werden.

Der Datenhunger von Wirtschaft und Staat nimmt auf allen Gebieten ständig zu.

Es wird zunehmend wichtiger, hier klare Schranken

zu definieren. Andernfalls steht die Freiheit des Individuums auf dem Spiel.

Besteht Grund zur Hoffnung, dass die Waagschale nicht auf die falsche Seite kippt? Vielleicht – nicht zuletzt dank der Hilfe und Unterstützung durch die Technik. Sie hat einerseits erst ermöglicht, dass alles und jedes gespeichert und analysiert werden kann. Die Technik bietet aber auf der anderen Seite vermehrt auch Instrumente an, die den Schutz der Privatsphäre fördern. Etwa durch Verschlüsselung, durch die Möglichkeit des anonymen Surfen oder durch die Entwicklung von «E-Money»¹⁶⁰. Diese «datenschutzfreundlichen Techniken»¹⁶¹ sind sehr zu begrüssen. Sie alleine genügen jedoch nicht. Die Gesellschaft, somit wir alle, sind bei der Frage nach dem Stellenwert, den das Private haben soll, gefordert. Es ist dabei zu bedenken, dass nur der Schutz der Privatsphäre die Freiheit des Menschen garantieren kann.

Denn – könnte es nicht sein, dass die Privatsphäre wie Sauerstoff ist, man ihre Bedeutung erst richtig würdigt und schätzt, wenn sie nicht mehr da ist?¹⁶²

¹⁵⁹ Wird nur noch am PC gearbeitet, fallen Rand-Daten an, die mit entsprechender Software die Arbeitstätigkeiten, die Arbeitsgeschwindigkeit, Arbeitsrhythmus etc. des Mitarbeitenden exakt analysieren und auswerten können. Damit ist es für den Arbeitgeber ein Leichtes, den ganzen Arbeitstag des Mitarbeitenden zu kontrollieren. Solche Tools sind bereits im Einsatz.

¹⁶⁰ Dieses soll das anonyme Bezahlen im Internet ermöglichen – analog zur Barzahlung im täglichen Leben.

¹⁶¹ Bzw. «Privacy enhancing technologies/PET».

¹⁶² Vgl. dazu «Privatheit – Sauerstoff der Freiheit», in NZZ, 14.04.01, S. 21 [dieser grundlegende Beitrag ist auf der DSB-Web-Site/Archiv Mailing-Liste zugänglich].

Nicht der Datenschutzbeauftragte setzt den Datenschutz um – dies machen die Mitarbeitenden der Verwaltungen bei ihrer täglichen Arbeit. Der Datenschutzbeauftragte bietet Dienstleistungen an, damit der Datenschutz durch die Mitarbeitenden korrekt umgesetzt wird.

Bei konkreten Problemstellungen muss oft gemeinsam nach einer Lösung gesucht werden. Dies ist nicht immer einfach. Werden für die Mitarbeitenden der Verwaltung durch die Vorgaben des Datenschutzes gewisse Arbeitsabläufe erschwert, so darf nicht vergessen werden, dass die Verwaltung die Daten von der Zuger Bevölkerung nur zu treuhänderischer Verwaltung übertragen erhält. Die Datenherrschaft bleibt jedoch bei der Bevölkerung. Mit den Daten in jeder Beziehung rechtmässig umzugehen und den Schutz der Privatsphäre zu gewährleisten, muss deshalb für die Verwaltung ein zentrales Anliegen sein.

Die Arbeit als Datenschutzbeauftragter wäre ohne die offene, angenehme und kooperative Zusammenarbeit kantonaler und gemeindlicher Stellen nicht möglich. Allen Personen sei dafür, nicht minder aber auch für kritischen Input, sehr herzlich gedankt.

Mein Dank geht auch an alle Mitarbeitenden der Staatskanzlei, wo ich quasi «Kost und Logis» habe, für die in jeder Beziehung äusserst angenehme und kollegiale Zusammenarbeit. Insbesondere natürlich geht mein Dank an Hildegard Steiner, welche das DSB-Sekretariat auch im Jahr 2000 kompetent betreute.

Last but not least gebührt ein doppelter Dank dem Landschreiber Dr. Tino Jorio: Er hat sich bereit erklärt, die Stellvertretung des Datenschutzbeauftragten zu übernehmen. Daneben sei aber auch sein Interesse und seine Bereitschaft verdankt, datenschutzrechtliche Fragen mit grossem Engagement, viel Verve und nicht zuletzt auch kritisch zu diskutieren.

Sachregister

Seite		Seite	
20	Aktenübergabe an NachfolgerIn	5	Geburtsdatum [Bekanntgabe]
32	Amtsgeheimnis	22	Grundbuch: Online-Zugriff
32	Arbeitsplatz Datensicherheit	23	Handelsregister [Umfang Datenbekanntgabe]
29	Archivgesetzgebung		Internet
8	Audit	14	Grundsätzliches
14	Briefpost: in neutralem Umschlag?	15	Nutzung durch Mitarbeitende
10	Datensicherheit: Grundsätze	14	Internet-Auftritt: Schule
2	DNA-Analyse	24	Kantonsarzt [Datenbekanntgabe]
26	Dokumentenverwaltung [zur Archivierung]	5	Kirchgemeinden [Datenbekanntgabe]
	DSB	27	Korporationsgemeinde: Sammelauskunft
29	Datenschutz-Kurs	7	Meldepflicht betr. Datensammlungen
7	fehlende Befugnisse	26	Mütter- und Väterberatungsstelle [Datenbekanntgabe]
28	Internet-Auftritt	25	Outsourcing des Postversands
30	Kontrolle	19	Personaldossier: Einsicht
28	Mailing-Liste	25	Postversand [Outsourcing]
29	Medienarbeit	20	Referendum: Bekanntgabe von Unterzeichnenden?
31	Stellvertretung	30	Register der Datensammlungen
30	Vernehmlassungen	26	Sammelauskunft: Einwohnerkontrolle
9	zur Unabhängigkeit	22	Schule: Web-Auftritt von Schülern
4	DSB Highlights 2000	26	Schule [Angaben auf Klassenliste]
31	DSB+CPD.CH	10	Sicherheitsüberprüfung: kantonale Informatik
	DSG	19	Sicherheitsüberprüfung [von externen Personen]
5	allgemeine Strafbestimmung?	19	Sicherheitsüberprüfung [von Mitarbeitenden]
6	Allgemeines	28	Sperrn [bei Datenbearbeitung durch Private]
5	Erste Lesung im Kantonsrat	6	Sperrrecht: Allgemeines
7	fehlende Regelungen	24	Spital: Herausgabe der KG
6	Zweite Lesung im Kantonsrat	24	Spital [Finanzkontrolle]
15	E-Government	21	Staatskalender
22	Einbürgerung: Kantonsrat	18	Statistik [Datenbekanntgabe]
27	Einbürgerung und Datenschutz	30	Steuergesetz-Revision
18	Einsicht in eigene Akten	25	Steuerregister [zur Öffentlichkeit]
26	Einwohnerkontrolle: Sammelauskunft	23	Strafanzeige: Bekanntgabe des Anzeigenden?
	E-Mail	7	Strafbestimmung [allg. im DSG]
15	Chiffrierung	23	Strassenverkehrsamt: Datensperre
16	RRats-Weisung	8	Verbandsbeschwerderecht
15	via Internet	23	Verkehrsplanung: Adressbezug von Zivilschutz?
17	via Intranet	16	Verschlüsselung betr. E-Mail
5	EU-Grundrechtscharta	20	Video-/Tonaufnahmen [Zulässigkeit?]
14	Fax	17	Videoüberwachung
24	Finanzkontrolle [Spitalwesen]	21	Volkszählung 2000
18	Forschung [Datenbekanntgabe]	15	Web-Camera: Internet
20	Fotos: Publikation?	6	Zweckbindung [Grundsatz]
23	Gebäudeversicherung: Datenbekanntgabe		

Der Kantonsrat des Kantons Zug, in Vollziehung des Art. 37 des Bundesgesetzes über den Datenschutz vom 19. Juni 1992²⁾ und gestützt auf § 41 Buchstabe b der Kantonsverfassung³⁾, beschliesst:

I. Allgemeine Bestimmungen

§ 1 Zweck

Dieses Gesetz bezweckt, Grundrechte von Personen zu schützen, über die Organe Daten bearbeiten.

§ 2 Begriffe

- a) Personendaten (im folgenden «Daten») sind alle Angaben, die sich auf eine bestimmte oder bestimmbar natürliche oder juristische Person oder auf eine Personengesellschaft des Handelsrechts beziehen.
- b) Besonders schützenswerte Daten sind alle Angaben über die religiösen, weltanschaulichen, politischen, berufspolitischen Ansichten oder Tätigkeiten, die Intimsphäre, die Gesundheit, die ethnische Zugehörigkeit, Massnahmen der sozialen Hilfe, administrative und strafrechtliche Verfolgungen und Sanktionen. Dasselbe gilt für eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der natürlichen Person (Persönlichkeitsprofil) erlaubt.
- c) Das Bearbeiten von Daten ist jeder Umgang mit Daten, namentlich solche zu erheben, zu beschaffen, aufzuzeichnen, zu sammeln, aufzubewahren, zu verwenden, umzuarbeiten, bekanntzugeben, auszutauschen, zusammenzuführen, zu archivieren und zu vernichten.
- d) Mit der Bekanntgabe werden Daten zugänglich gemacht, namentlich wird in solche Einsicht gewährt, werden solche weitergegeben und veröffentlicht.
- e) Eine Datensammlung ist ein Bestand von Daten, der so aufgebaut ist, dass die Daten nach den betroffenen Personen erschliessbar sind. Eine Hilfsdatensammlung liegt vor, sofern die Daten offensichtliche Hilfsfunktionen haben, selber aber keine Aussagen über Personen enthalten.
- f) Betroffene Personen sind natürliche oder juristische Personen oder Personengesellschaften des Handelsrechts, über die Daten bearbeitet werden.
- g) Der Begriff «Kanton» wird als Sammelbegriff für die Staatsverwaltung, die kantonalen Körperschaften und Anstalten, die Gerichte sowie die kantonalen Schulen verwendet.
- h) Gemeinden sind die Einwohner-, Bürger-, römisch-katholischen und evangelisch-reformierte Kirchgemeinden sowie Korporationsgemeinden.
- i) Organe sind Behörden und Dienststellen, die für den Kanton oder die Gemeinden handeln, und natürliche oder juristische Personen oder Personengesellschaften des Handelsrechts, soweit ihnen öffentliche Aufgaben übertragen sind.
- k) Dritte sind alle diejenigen, die weder betroffene Personen noch Organe sind.
- l) Als gesetzliche Grundlagen gelten die Verfassung, ein Konkordat, ein Gesetz, ein Kantonsratsbeschluss, eine Verordnung, ein publizierter Regierungsratsbeschluss oder ein publizierter gemeindlicher Erlass.

§ 3 Geltungsbereich

¹⁾Das Gesetz gilt für das Bearbeiten von Daten durch Organe.

²⁾Es wird nicht angewendet auf

- a) hängige Verfahren der Zivil-, Verwaltungs- und Strafrechtspflege;
 - b) Geschäfte, über welche die Stimmberechtigten, der Kantonsrat oder Gemeindeparlamente beschliessen;
 - c) öffentliche Register des Privatrechtsverkehrs;
 - d) Daten, die eine natürliche Person als Arbeitsinstrument ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Dritte oder Organe weitergibt.
- ³⁾Abweichende Regelungen in formellen Gesetzen bleiben vorbehalten.

II. Grundsätze beim Bearbeiten von Daten

§ 4 Richtigkeit, Datenbeschaffung, Zweckbestimmung, Anonymisierung

Daten

- a) müssen aktuell, richtig und vollständig sein, soweit es der Bearbeitungszweck verlangt;
- b) sind in der Regel bei der betroffenen Person zu beschaffen;
- c) dürfen nur für Zwecke bearbeitet werden, die bei der Beschaffung angegeben worden, aus den Umständen ersichtlich oder gesetzlich vorgesehen sind;
- d) dürfen für Forschung, Planung und Statistik bearbeitet werden, wenn sie anonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt, wenn sie nicht weitergegeben werden und wenn die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

§ 5 Voraussetzungen für das Bearbeiten von Daten

¹⁾Die Organe dürfen Daten bearbeiten, sofern

- a) eine gesetzliche Grundlage dafür besteht oder
 - b) es für eine in einer gesetzlichen Grundlage umschriebene Aufgabe unentbehrlich ist oder
 - c) die betroffene Person im Einzelfall ausdrücklich eingewilligt hat oder ihre Einwilligung nach den Umständen offensichtlich vorausgesetzt werden kann.
- ²⁾Die Organe dürfen besonders schützenswerte Daten bearbeiten, sofern
- a) ein formelles Gesetz es ausdrücklich vorsieht oder
 - b) es für eine in einem formellen Gesetz umschriebene Aufgabe offensichtlich unentbehrlich ist oder
 - c) die betroffene Person im Einzelfall ausdrücklich eingewilligt oder ihre Daten allgemein zugänglich gemacht hat.

§ 6 Ausgelagertes Bearbeiten von Daten

¹⁾Das Bearbeiten von Daten kann ausgelagert werden, wenn

- a) die Auftraggeberin oder der Auftraggeber dafür sorgt, dass die Daten nur so bearbeitet werden, wie sie oder er es selbst tun dürfte und
 - b) keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.
- ²⁾Die Einhaltung des Datenschutzes wird durch Auflagen, Vereinbarungen oder in anderer Weise sichergestellt.

§ 7 Datensicherung

¹⁾Daten sind insbesondere vor Verlust, Fälschung, Entwendung,

Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte zu sichern.

²Der Regierungsrat erlässt innerhalb eines Jahres nach Inkrafttreten dieses Gesetzes diesbezüglich Vorschriften, insbesondere über die Sicherheitsgrundsätze und das Bewilligungsverfahren im Bereich des elektronischen Datenaustausches.

§ 8 Bekanntgabe von Daten

¹Bekanntgabe an Dritte erfolgt schriftlich und nur auf schriftliches Gesuch hin.

²Die Einwohnerkontrolle erteilt Organen für die Erfüllung ihrer Aufgaben voraussetzungslos Einzel- oder Sammelauskünfte betreffend Name, Vorname, Geschlecht, Geburtsdatum, Zivilstand, aktuelle Adresse, Ort und Datum des Zu- und Wegzugs, Heimatort, Staatsangehörigkeit und Todestag. Gesuch und Auskunft können schriftlich oder mündlich erfolgen.

³Die Einwohnerkontrolle erteilt Dritten folgende Auskünfte:

- a) Einzelauskünfte betreffend Name, Vorname, Geschlecht, aktuelle Adresse (bei Wegzug mit Wegzugsdatum und Wegzugsort) und Todestag werden voraussetzungslos erteilt. Gesuch und Auskunft können schriftlich oder mündlich erfolgen.
- b) Wird ein Interesse glaubhaft gemacht, werden bei Einzelauskünften aufgrund eines schriftlichen Gesuchs die folgenden erweiterten Personalien bekannt gegeben: Geburtsdatum, Zivilstand, Heimatort, Staatsangehörigkeit und Zuzugsort. Die Auskunft erfolgt schriftlich.
- c) Wird ein Interesse glaubhaft gemacht, werden Sammelauskünfte aufgrund eines schriftlichen Gesuchs erteilt, sofern schützenswerte ideelle Zwecke vorliegen. Sammelauskünfte sind auf die einfachen Personalien beschränkt (gemäss Bst. a dieses Absatzes). Die Auskunft erfolgt schriftlich.
⁴Die Absätze 2 und 3 sind sinngemäss auch auf das Amt für Ausländerfragen sowie Bürger- und Korporationsgemeinden anwendbar.
⁵Auskünfte gemäss Abs. 3 können verweigert werden, sofern schutzwürdige Interessen Betroffener beeinträchtigt werden.

§ 9 Sperrung der Bekanntgabe

¹Eine betroffene Person kann voraussetzungslos vom Organ verlangen, dass Daten nur an Organe bekanntgegeben werden dürfen.

²Die 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.

³Das Organ verweigert die Sperrung oder hebt sie auf, wenn

- a) eine Rechtspflicht zur Bekanntgabe besteht oder
- b) die oder der Dritte glaubhaft macht, dass sie oder er dadurch behindert wird, schutzwürdige Ansprüche gegenüber der betroffenen Person geltend zu machen. Der betroffenen Person ist vorher wenn möglich Gelegenheit zur Stellungnahme zu geben.

§ 10 Einschränkung der Bekanntgabe an Organe

Das Organ lehnt die Bekanntgabe von Daten an ein anderes Organ ab, schränkt sie ein oder verbindet sie mit Auflagen, wenn dem nicht

- a) wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen einer betroffenen Person entgegenstehen oder

- b) gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften entgegenstehen.

§ 11 Anonymisieren und Vernichten von Daten

Organe müssen Daten, die sie nicht mehr benötigen, anonymisieren oder vernichten, soweit die Daten nicht unmittelbaren Beweis-zwecken dienen oder dem zuständigen Archiv abzuliefern sind.

III. Kontrollrechte der betroffenen Personen

§ 12 Anmeldung und Register

¹Der Kanton und die Gemeinden führen über ihre Datensammlungen je öffentliche Register. Sie veröffentlichen diese alle zwei Jahre in geeigneter Form.

²Nicht in das Register aufgenommen werden Datensammlungen, die

- a) nur bis maximal sechs Monate geführt werden;
- b) Hilfsdatensammlungen darstellen.

³Das Register enthält für jede Datensammlung deren Bezeichnung, Angaben über die Rechtsgrundlage, den Zweck, die Mittel und Verfahren des Bearbeitens, die Art und Herkunft der Daten, deren regelmässige Empfängerinnen oder Empfänger, das Organ, das die Datensammlung führt, andere an der Datensammlung beteiligte Organe und den allfälligen Aufbewahrungsort von Kopien.

⁴Neue Datensammlungen und Änderungen bestehender Datensammlungen sind sofort der Datenschutzstelle zu melden.

⁵Die kantonale Datenschutzstelle führt für den Kanton das Register. Die Gemeinden beauftragen ihrerseits eine Person mit der Registerführung.

§ 13 Auskunft und Einsicht

¹Jede betroffene Person kann mündlich oder schriftlich Auskunft verlangen

- a) bei der Registerführerin oder beim Registerführer über den Inhalt des Registers;
- b) beim Organ, ob über sie Daten bearbeitet werden und gegebenenfalls über ihre Daten.
- c) beim Organ über diejenigen Dritten, die Daten gemäss § 8 Abs. 3 Bst. b über sie erhalten haben.

²Soweit Mittel und Verfahren des Bearbeitens es zulassen, wird Einsicht in die Daten beim Organ, das die Datensammlung führt, gewährt.

³Daten über die Gesundheit kann die Inhaberin oder der Inhaber der Datensammlung aus wichtigen Gründen der betroffenen Person durch eine von ihr bezeichnete Ärztin oder einen von ihr bezeichneten Arzt mitteilen lassen.

§ 14 Einschränkung der Bekanntgabe an die betroffenen Personen

¹Ein Organ darf die Auskunft und Einsicht über Daten aus überwiegenden Interessen der Öffentlichkeit oder Dritter begründet einschränken, mit Auflagen versehen, aufschieben oder verweigern.

²Bei ausgelagerter Datenbearbeitung ist das Organ zuständig, das die Datenbearbeitung ausgelagert hat.

§ 15 Ansprüche bei widerrechtlichem Bearbeiten von Daten

¹Wer ein schützenswertes Interesse hat, kann vom Organ verlangen, dass es

- a) die Widerrechtlichkeit des Bearbeitens feststellt;
- b) das widerrechtliche Bearbeiten unterlässt;
- c) die Folgen eines widerrechtlichen Bearbeitens beseitigt.
²Die betroffene Person kann insbesondere vom Organ verlangen, dass es
 - a) Daten berichtigt oder vernichtet;
 - b) den Entscheid oder die Berichtigung Dritten mitteilt oder veröffentlicht.
³Bestreitet das Organ die Unrichtigkeit von Daten, obliegt ihm der Beweis für die Richtigkeit. Die betroffene Person hat bei der Abklärung mitzuwirken.

§ 16 Ablehnung von Gesuchen

Entspricht ein Organ einem Gesuch aufgrund dieses Gesetzes nicht, erlässt es einen begründeten, mit einer Rechtsmittelbelehrung versehenen Entscheid.

§ 17 Kosten

¹Auskunft und Einsicht durch die betroffenen Personen sind kostenlos.

²Jede Person kann von den sie betreffenden Daten Kopien verlangen. In der Regel werden dafür keine Kosten erhoben.

³Für schriftlich erteilte Auskünfte an Dritte gemäss § 8 Abs. 3 Bst. c kann eine Gebühr gemäss Kantonsratsbeschluss über die Gebühren in Verwaltungs- und Zivilsachen vom 11. März 1974⁴) erhoben werden.

IV. Aufsicht

§ 18 Datenschutzstellen

¹Der Kanton schafft eine Datenschutzstelle.

²Sie ist fachlich unabhängig. Administrativ ist sie der Staatskanzlei zugeordnet.

³Gemeinden und kantonale Direktionen können für ihren Aufgabenbereich eigene Datenschutzstellen schaffen. Die kantonale Datenschutzstelle übt in diesen Fällen die Aufsicht aus. Betroffene Personen können sich auch direkt an die kantonale Datenschutzstelle wenden.

⁴Ist keine eigene Datenschutzstelle vorhanden, ist für den Datenschutz die kantonale Datenschutzstelle zuständig.

§ 19 Aufgaben

¹Die kantonale Datenschutzstelle

- a) überwacht die Anwendung der Vorschriften über den Datenschutz;
- b) berät die Organe in Fragen des Datenschutzes;
- c) erteilt den betroffenen Personen Auskunft über ihre Rechte;
- d) vermittelt zwischen den Organen und betroffenen Personen bei allen Streitigkeiten über den Datenschutz;
- e) nimmt zu rechtsetzenden Erlassen aus datenschutzrechtlicher Sicht Stellung;
- f) orientiert die Organe und die Öffentlichkeit über wesentliche Anliegen des Datenschutzes;
- g) beaufsichtigt die Datenschutzstellen der Gemeinden und der kantonalen Direktionen und kann Weisungen erteilen;
- h) erstattet dem Regierungsrat jährlich Bericht über ihre Tätigkeit. Diese Berichte werden veröffentlicht;

- i) führt für den Kanton das Register;
- k) arbeitet mit dem Eidgenössischen Datenschutzbeauftragten und den Datenschutzbehörden anderer Kantone zusammen.
²Die Datenschutzstellen der Gemeinden oder der kantonalen Direktionen üben sinngemäss dieselben Aufgaben aus.

§ 20 Befugnisse

¹Die Datenschutzstelle kann ungeachtet allfälliger Geheimhaltungsvorschriften bei den Organen Auskünfte über das Bearbeiten von Daten einholen und Einsicht in die Datensammlungen nehmen.

²Ergibt die Abklärung, dass Datenschutzvorschriften verletzt werden, fordert sie das Organ auf, die erforderlichen Massnahmen zu ergreifen. Die zuständige vorgesetzte Behörde ist zu orientieren.

³Wird die Aufforderung nicht befolgt oder abgelehnt, unterbreitet sie die Angelegenheit dem zuständigen Gemeinderat (gemeindliche Angelegenheiten) bzw. dem Regierungsrat (kantonale Angelegenheiten) zum Entscheid. Der Entscheid wird der betroffenen Person und der Datenschutzstelle mitgeteilt.

§ 21 Unterstützung durch die Organe

Die Organe unterstützen die Datenschutzstelle bei der Erfüllung ihrer Aufgaben.

V. Rechtspflege und Strafbestimmung

§ 22 Grundsatz

Die Rechtspflege richtet sich nach dem Gesetz über den Rechtsschutz in Verwaltungssachen vom 1. April 1976⁵).

§ 23 Einsprache

Gegen Entscheide der Organe kann Einsprache erhoben werden.

§ 24 Strafbestimmung

Wer als beauftragte Person für das Bearbeiten von Daten ohne anderslautende ausdrückliche Ermächtigung des auftraggebenden Organs Daten für sich oder andere verwendet oder anderen bekannt gibt, wird mit Haft oder Busse bestraft.

§ 25 Verfahren bei Haftungsansprüchen

¹Wird die betroffene Person durch eine natürliche oder juristische Person geschädigt, die Datenbearbeitung im Auftrag eines Organs ausführt, so haftet das auftragserteilende Organ aufgrund des Verantwortlichkeitsgesetzes⁶).

²Im Verfahren um Feststellung der Widerrechtlichkeit des Bearbeitens von Daten ist gleichzeitig über die geltend gemachten Schadenersatz- und Genugtuungsansprüche zu entscheiden.

³Im Übrigen kommt das Verantwortlichkeitsgesetz⁶) zur Anwendung.

VI. Übergangs- und Schlussbestimmungen

§ 26 Anpassung an das neue Recht

¹Die Organe passen ihre Datensammlungen innert zwei Jahren nach Inkrafttreten dieses Gesetzes dem neuen Recht an. Kanton und Gemeinden erstellen in derselben Frist das Register.

²Folgende Gesetze werden wie folgt geändert: ...

a) Gesetz über die Kantonspolizei vom 31. Oktober 1966¹⁾:

X. Datenschutz

§ 14^{bis} Grundsatz

Soweit dieses Gesetz nichts anderes regelt, gelten die Bestimmungen des Datenschutzgesetzes.

§ 14^{ter} Beschränkung der Auskunft und Einsicht der betroffenen Person

¹Der Regierungsrat bezeichnet die von der Polizei geführten Datensammlungen, für die nur ein beschränktes Auskunfts- und Einsichtsrecht besteht.

²Gesuche um Auskunft über und Einsicht in solche Datensammlungen sind an die Datenschutzstelle zu richten.

³Diese prüft, ob die Polizei über die betroffene Person rechtmässig Daten bearbeitet.

⁴In einer stets gleichlautenden Antwort teilt die Datenschutzstelle der betroffenen Person mit, dass in Bezug auf sie entweder keine Daten unrechtmässig bearbeitet werden oder dass die Datenschutzstelle bei Vorhandensein allfälliger Fehler in der Datenbearbeitung an die Polizei eine Empfehlung zu deren Behebung gerichtet habe.

⁵Ein Rechtsmittel gegen diese Mitteilung ist ausgeschlossen.

b) Gesetz über die Veröffentlichung der Gesetze und das Amtsblatt des Kantons Zug vom 29. Januar 1981⁸⁾:

§ 6 Zweck, Gestaltung und Erscheinen

(...)

³(...) wöchentlich einmal. Die Veröffentlichung im Internet oder durch andere elektronische Kommunikationsmittel sind für beide Teile zulässig. Davon ausgenommen sind im Amtlichen Teil besonders schützenswerte Daten. Die Veröffentlichung des Amtlichen Teils ist nach einer bestimmten Frist, die der Regierungsrat festsetzt, zu löschen.

§ 27 Inkrafttreten

Dieses Gesetz tritt nach unbenützter Referendumsfrist (§ 34 der Kantonsverfassung) oder nach der Annahme durch das Volk am Tage nach der Veröffentlichung im Amtsblatt in Kraft⁹⁾.

1) GS 26, 867

2) SR 235

3) BGS 111.1

4) BGS 641.1

5) BGS 162.1

6) BGS 154.11

7) GS 19, 233 (BGS 512.1)

8) GS 22, 19 (BGS 152.3)

9) Inkrafttreten am 9. Dezember 2000

**Datenschutzbeauftragter
des Kantons Zug**

Dr. René Huber
Regierungsgebäude
Postfach 156
6301 Zug
Tel. 728 31 87 (direkt)
Tel. 728 31 47
(Sekretariat)
Fax 728 37 01
www.datenschutz-zug.ch

**Eidg. Datenschutz-
beauftragter**

Feldegweg 1
Postfach
3003 Bern
Tel. 031-322 43 95
www.edsb.ch

Kantonale Verwaltung

Tel. 728 33 11 (Zentrale)

Gemeindeverwaltungen

Baar
Rathausstrasse 1
6340 Baar
Tel. 769 01 11
Fax 769 01 90

Cham
Mandelhof
6330 Cham
Tel. 784 47 47
Fax 784 47 74

Hünenberg
Chamerstrasse 11
6331 Hünenberg
Tel. 784 44 44
Fax 784 44 99

Menzingen
Rathaus
6313 Menzingen
Tel. 755 13 12
Fax 755 32 49

Neuheim
Dorfplatz 5
6345 Neuheim
Tel. 757 21 30
Fax 757 21 40

Oberägeri
Alosenstrasse 2
Postfach 159
6315 Oberägeri
Tel. 754 70 20
Fax 754 70 21

Risch
Zentrum
Dorfmatte
6343 Rotkreuz
Tel. 798 18 18
Fax 798 18 88

Steinhausen
Bahnhofstrasse 3
6312 Steinhausen
Tel. 748 11 11
Fax 741 31 81

Unterägeri
Postfach 79
6314 Unterägeri
Tel. 754 55 00
Fax 754 55 55

Walchwil
Postfach 93
6318 Walchwil
Tel. 759 80 10
Fax 758 24 68

Zug
Stadthaus am Kolinplatz
Postfach 1258
6301 Zug
Tel. 728 15 15
Fax 728 23 71

Bitte dieses Formular ausdrucken, ausfüllen und retournieren an:

Datenschutzbeauftragter des Kantons Zug – René Huber – Postfach 156 – 6301 Zug

Liebe Leserin, lieber Leser

Sie haben den Tätigkeitsbericht 2000 des Zuger Datenschutzbeauftragten gelesen. Damit Ihre Bedürfnisse im nächsten Bericht noch besser abgedeckt werden können, bin ich auf Ihre Rückmeldung angewiesen. Nehmen Sie sich für die Beantwortung folgender Fragen kurz Zeit – für Ihren Input danke ich Ihnen im Voraus sehr herzlich.

Datenschutzbeauftragter des Kantons Zug
René Huber

Bitte Zutreffendes ankreuzen

Nutzen für Ihre Arbeit?	gering	mittel	gross
Nutzen im Privatbereich?	gering	mittel	gross
Verständlichkeit?	zu fachtechnisch	gut	zu simpel
Ausführlichkeit der einzelnen Berichte?	zu ausführlich	gerade richtig	zu knapp
Umfang des Berichts insgesamt?	zu umfangreich	gerade richtig	zu knapp
Präsentation/Layout?	schlecht	i.O.	gut

Was haben Sie vermisst? _____

Anregungen/Wünsche/Kritik _____

Weiteres? _____

Hinweis: Die folgenden Angaben dienen der Verbesserung und Weiterentwicklung des nächsten Tätigkeitsberichts. Ihre Angaben werden bei Eintreffen anonymisiert, das Formular umgehend vernichtet.

Absender [freiwillig]

Firma/Amtsstelle _____

Funktion _____

