Datenschutzbeauftragter des Kantons Zug
Tätigkeitsbericht 2010 [Nr. 12]

Kanton Zug

Tätigkeitsbericht 2010 [Nr. 12]
Der Datenschutzbeauftragte hat dem Kantonsrat und dem Regierungsrat jährlich einen Bericht über seine Tätigkeit zu erstatten. Der Bericht ist zu veröffentlichen.[1]

Der vorliegende Tätigkeitsbericht Nr. 12 deckt den Zeitraum zwischen 1. Januar 2010 und 31. Dezember 2010 ab.

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

Zug, 15. Januar 2011

Datenschutzbeauftragter des Kantons Zug
Dr. iur. René Huber

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

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

ISSN 1424-4756

Ein paar häufig verwendete Abkürzungen:

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

1 § 19 Abs. 1 Bst. h Datenschutzgesetz des Kantons Zug.

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

Datenschutzstelle des Kantons Zug
Regierungsgebäude, Seestrasse 2
Postfach 156, 6301 Zug
Tel. 041 728 31 47, Fax 041 728 37 01
www.datenschutz-zug.ch

Inhaltsverzeichnis

Hilfe! – Der Kanton stellt meine Personendaten ins Internet!

Liebe Leserin
Lieber Leser

Viele Beanstandungen im Jahr 2010 betrafen die Veröffentlichungen privater Daten von Zuger Einwohnerinnen und Einwohnern im Internet durch gemeindliche oder kantonale Stellen – insbesondere zu den folgenden Themen:

Automobilisten:	Warum sind meine Fahrzeughalterdaten für jedermann im Internet einsehbar?![3]
Grundeigentümer:	Fotos, Grundbuchdaten und viele weitere Daten zu meinem Haus und Grundstück gehören nicht ins Internet![4]
Eltern:	Fotos meiner Kinder gehören nicht auf die Schulwebseite![5]
Eingebürgerte Schweizer:	Die Daten zu meiner Einbürgerung haben im Web nichts zu suchen!

Das Internet stellt nicht nur nützliche Informationen speditiv zur Verfügung. Es ist auch nicht nur der Hort des Guten und Schönen. Denn Daten werden unbemerkt genutzt, allenfalls auch zu unserem Nachteil. Ohne unser Wissen kopiert, ausgewertet, auf ewige Zeiten gespeichert und verknüpft mit weiteren Daten über uns. Zu Zwecken, mit denen wir nie gerechnet, von denen wir keine Kenntnis haben.

Jedermann kann sich ein Bild über uns machen, das wir nicht mehr beeinflussen können, zu dem wir nichts zu sagen haben. All dies kann für uns Folgen haben, die wir nie gewollt haben. Unser Privates gehört daher nicht ins Internet. Wenn wir selbst diese Informationen über uns freigeben, haben wir nur uns selbst an der Nase zu nehmen, falls uns Schaden entsteht.

Dritten aber ist es in aller Regel nicht erlaubt, Privates über uns ins Internet zu stellen. Und schon gar nicht darf der Kanton oder die Gemeinde unsere privaten Daten ins Internet stellen. Daten, die wir der Verwaltung aufgrund von Gesetzen für ganz bestimmte Zwecke zwingend geben mussten.

Die persönlichen Daten der Zugerinnen und Zuger gehören nicht ins Internet. Alle derartigen Veröffentlichungen durch den Staat müssen unzulässig sein. Der Staat hat eine besondere Verantwortung, er hat hier Vorbild zu sein. Dafür setzen wir uns ein.

Dr. iur. René Huber
Datenschutzbeauftragter des Kantons Zug

3 Was Sie dagegen unternehmen können, zeigen wir Ihnen auf S. 30.

4 S. dazu hinten Fall Nr. 2 S. 10.

5 S. dazu hinten Fall Nr. 9 S. 15.

Sind Sie in Eile? – Das Wichtigste des Jahres 2010

Was ist Datenschutz? – 19 Fälle aus unserer Praxis
Wir stellen Ihnen 19 konkrete Beispiele aus unserer Beratungspraxis vor. Damit sehen Sie, worum es beim Datenschutz konkret geht. Alle Fälle auf einen Blick – in der Übersichtstabelle am Anfang.
Näheres S. 9

1496 Zuger Datensammlungen!
Wer bearbeitet welche Daten wozu und über wen? Das zeigt Ihnen das Register über alle Datensammlungen, die bei der kantonalen und gemeindlichen Verwaltung vorhanden sind. Wir führen dieses Register. Zurzeit sind 1496 Datensammlungen bei uns registriert. Das Register steht Ihnen im Internet zur Verfügung.
Näheres S. 26

Aktuelles zur Datensicherheit
Dokumente mit einem Passwort schützen und dann mailen – ist das denn sicher? Wir haben es überprüfen lassen. Daneben haben wir uns auch mit der IT-Strategie des Kantons für die Jahre 2011 bis 2017 befasst.
Näheres S. 6

Kümmern Sie sich um Ihre Daten!
Was können Sie selber für den Schutz Ihrer eigenen Daten tun? Hier finden Sie praktische Tipps dazu: Sperren Sie ihre Daten bei Gemeinde und Strassenverkehrsamt. Seien Sie bei Internet, Facebook und Twitter vorsichtig. Und hier erfahren Sie auch, was die Verwaltung alles über Sie weiss. Schliesslich – halten Sie sich bezüglich Datenschutz einfach und kostenlos auf dem Laufenden.
Näheres S. 30

Wichtiges aus der Gesetzgebung
Neben vielen anderen Gesetzgebungsprojekten haben wir vertieft bei Änderungen des Polizeigesetzes und des Datenschutzgesetzes sowie bei der neuen Verordnung über das Krebsregister mitgearbeitet.
Näheres S. 24

Elektronischer Newsletter der Datenschutzstelle
Über Aktuelles aus Datenschutz und Datensicherheit informieren wir Sie in Kurzform kostenlos per E-Mail. Im Berichtsjahr haben wir über 30 Nachrichten verschickt. Der Newsletter stösst auf viel Interesse – wir haben 2010 über 70 Neuabonnierte gewinnen können.
Näheres S. 20

I. Grundlegende Themen und Projekte

1. Schengen-Kontrolle bei der Zuger Polizei

Ausgangslage

Aufgrund der Abkommen von Schengen fallen die Personenkontrollen an der Grenze praktisch weg, dafür findet ein intensiver Datenaustausch zwischen den Polizeibehörden auf europäischer Ebene statt. Auch die Polizei in Zug hat nun [indirekten] Zugang zum Schengen-Datenpool SIS.[6] Gemäss einen Bericht der EU-Kommission[7] umfasste das SIS im Januar 2010 bereits über 31 Millionen Einträge gesuchter Personen und Gegenstände. Gemäss diesem Bericht ist beim Wechsel auf das neue System SIS II im Jahr 2013 geplant, dass dieses bis zu 100 Millionen Einträge verarbeiten wird.

Wo derartige Datensammlungen vorhanden sind, sind Fehlmanipulationen, Verwechslungen, Irrtümer, Fehler, veraltete Daten und auch Missbräuche aufgrund von menschlichem Verhalten oder der hochkomplexen Technik nie auszuschliessen. Für davon betroffene Personen kann dies gravierende Folgen haben – eine Verhaftung dürfte die Regel sein.

Die EU sieht deshalb eine ganze Reihe verschiedener Kontrollen an unterschiedlichen Stellen vor. Unter anderem müssen die polizeilichen Zugriffe auf das Schengener Informationssystem SIS durch die Datenschutzbehörden mindestens einmal jährlich überprüft werden – ausdrücklich auch auf kantonaler Ebene.

Datenschutzbeauftragter macht eine Kontrolle bei der Zuger Polizei

Der DSB verfügte grundsätzlich nicht über genügendes Know-how und insbesondere auch nicht über die erforderlichen zeitlichen Ressourcen, um einen SIS-Audit innert der vorgegebenen Fristen durchzuführen. Er beauftragte daher für eine solche erstmalige Kontrolle bei der Zuger Polizei ein externes Unternehmen, das über erfahrene Spezialisten im Audit-Bereich verfügt.

Das Ziel war die Beurteilung der Nutzung des SIS durch die Zuger Polizei. Im Zentrum standen dabei die Umsetzung der allgemeinen rechtlichen Vorgaben, des Datenschutzes und der organisatorischen Informationssicherheit. Nicht geprüft wurde hingegen die technische Informationssicherheit. Es erfolgten somit *keine* technischen Überprüfungen von IT-Systemen, Netzwerken oder Geräten.

Die Überprüfung kam erfreulicherweise zum Schluss, dass die Umsetzung der rechtlichen Vorgaben bezüglich Informationssicherheit und Datenschutz *sehr gut* erfüllt wurden. Gewisse kleinere Mängel wurden festgestellt. Diese sind gemäss den Verbesserungsvorschlägen mit tiefer bis mittlerer Priorität in Ordnung zu bringen.

Ausblick

Nach dieser eher grundlegenden erstmaligen Überprüfung bei der Polizei ist nun vorgesehen, dass der DSB ein- oder allenfalls zweimal jährlich Zugriffe der Polizei auf das SIS anhand von Stichproben zusammen mit den Verantwortlichen der Polizei überprüft. Da jede einzelne Abfrage der Polizei zentral auf den entsprechenden Systemen des Bundes aufgezeichnet wird, kann anhand der Liste der Zugriffe überprüft werden, ob eine erfolgte SIS-Abfrage des Polizeimitarbeitenden aufgrund eines entsprechenden polizeilichen Auftrages erfolgte oder nicht. Diese Kontrollen sind gemäss den EU-Vorgaben mindestens einmal jährlich vorzunehmen. Diese Überprüfung wird der Datenschutzbeauftragte selber durchführen.

6 Genauer: «SISone4all» – so wird das aktuell noch in Betrieb stehende System bezeichnet.

7 European Commission/ «SEC(2010) 1138 final» vom 21. September 2010.

2. Schalter von 00.00 bis 24.00 Uhr geöffnet – E-Government

Ausgangslage

Ein Gang zur Behörde in die Kantonshauptstadt zwischen 08.30 und 11.45 Uhr sowie 14.00 und 17.00 Uhr, am Freitag jeweils bis 16.00 Uhr? Nur wenn es denn anders nicht geht. In der heutigen Zeit möchten sich viele diesen Gang an den Schalter bei der öffentlichen Verwaltung ersparen und das Geschäft lieber via Internet am Computer erledigen, am Abend oder am Wochenende.

Was ganz einfach aussieht, ist es aber bei genauerer Betrachtung nicht: Vorweg müssen die Behörden absolut sicher sein, dass die Person, die ein Geschäft erledigen will, auch wirklich diejenige ist, die sie vorgibt zu sein. Dazu veröffentlichte der «New Yorker» bereits 1993 den berühmten Cartoon mit den beiden Hunden am Computer und der Aussage des einen Hundes «On the internet, nobody knows you're a dog!».

Beim E-Government[8] sind Datenschutz und Datensicherheit somit wichtige Voraussetzungen. Darauf hat denn auch der Regierungsrat in seiner «E-Government-Strategie Zug» vom 8. April 2008 hingewiesen. Der Datenschutzbeauftragte ist daher bei entsprechenden Projekten involviert.

Datensicherheit

Eine ganze Palette von Fragen muss technisch sauber gelöst werden, so etwa: Die Website der Behörden muss zertifiziert und fälschungssicher sein, damit nicht Betrüger aufgrund gefälschter Seiten an Bürgerdaten herankommen. Die Bürgerin muss sich fälschungssicher identifizieren, damit nicht Daten an falsche Personen gehen. Die Behörden müssen somit sicher sein, mit wem sie kommunizieren. Die Übertragung der Daten muss in beiden Richtungen stark verschlüsselt sein, damit Daten auf dem Weg von und zum Bürger nicht abgefangen, kopiert, gelöscht oder verändert werden können. Die Infrastruktur der Verwaltung muss gegen Angriffe und Schadprogramm wirkungsvoll geschützt sein. Sie muss stabil, störungsfrei und auch im Falle von Hochbetrieb, ja selbst bei böswilliger Datenüberschwemmung sauber funktionieren. Bei gewissen Eingaben müssen nämlich gesetzliche Fristen eingehalten werden, so etwa bei Eingaben von Anwälten an Gerichts- und Justizbehörden. Hier werden verspätete Eingaben nicht berücksichtigt. Bestimmte Dokumente müssen gegen Veränderungen wirkungsvoll gesichert werden, damit sie durch Bürger oder Behörde nachträglich nicht abgeändert werden können.

Bezüglich der sehr komplexen Anforderungen beim Abstimmen und Wählen muss der Hinweis genügen, dass die Systeme in der Lage sein müssen, überprüfen zu können, ob jemand berechtigt ist abzustimmen oder zu wählen und ob bereits eine Wahl auf konventionellem oder elektronischem Weg vorgenommen wurde. Es muss somit alles nachvollziehbar sein – aber trotzdem muss das Stimm- und Wahlgeheimnis gewahrt sein, damit keinesfalls eruierbar ist, wie die einzelnen Bürger gestimmt haben.

Datenschutz

Amtsgeheimnis und Datenschutz schützen die Bürger vor dem allwissenden und allmächtigen Staat: Daten werden daher nicht zentral und für alle Mitarbeitenden der Verwaltungen von Gemeinden, Kanton und Bund einsehbar gespeichert.

Vielmehr darf jede Stelle nur diejenigen Daten sehen und bearbeiten, die sie für die Erfüllung ihrer gesetzlichen Aufgaben zwingend benötigt – mehr nicht.

Diese Rechtslage muss auch beim E-Government gelten. Somit dürfen Online-Geschäfte nicht zentral verwaltet und bearbeitet werden und der Bürger darf weder mit einer einheitlichen Nummer[9] identifiziert werden noch darf ihm ein einheitliches Benutzerkonto für alle Geschäfte zugewiesen werden. Die Geschäfte müssen – wie bei der bisherigen Bearbeitung auch – bereichsspezifisch und grundsätzlich de-

8 E-Government Umschreibung beim Bund: «Die Unterstützung der Beziehungen, Prozesse und politischen Partizipation innerhalb der staatlichen Stellen sowie zwischen den staatlichen Stellen und der Bevölkerung, Unternehmen und Institutionen durch die Bereitstellung von Informationen und Interaktionsmöglichkeiten mittels elektronischer Medien.»

9 Es darf daher grundsätzlich weder die neue AHV-Versichertennummer [«AHV-N13»] noch eine neu zu vergebende «Bürgernummer» genutzt werden.

zentral bearbeitet und gespeichert werden: so bleiben die Steuergeschäfte bei der Steuerverwaltung, die Polizeidaten bei der Polizei und die Schuldaten bei der Schule.

E-Government in Österreich beruht auf solchen bereichsspezifischen Personenkennungen, die einerseits in eindeutiger Weise gewährleisten, dass die Daten einer ganz bestimmten Person bearbeitet werden, dabei es aber nicht möglich ist, dass ein Bezug über einen bestimmten Bereich hinaus gemacht werden kann.[10]

Aufschlussreich ist die Rechtslage in Portugal: Dort steht das Verbot, allen Bürgern eine einheitlich zu nutzende Bürgernummer zu geben, sogar ausdrücklich in der Verfassung.[11]

Ausblick

Die einstige Euphorie bezüglich E-Government hat sich unterdessen etwas gelegt, zudem lässt sich auch nicht jedes Geschäft zwischen Privaten und Staat via Internet lösen. Trotzdem: Es ist klar, dass in den kommenden Jahren eine Verschiebung auf den elektronischen Weg kommen wird. Viele komplexe Fragen sind dabei allerdings noch zu lösen. Der Datenschutzbeauftragte wird dabei Input leisten.

10 Ausgangspunkt ist die durch das Meldewesen jeder Person zentral zugeordnete «Zentrale Melderegister-Zahl». Diese Zahl wird durch die österreichische Datenschutzkommission mit einem geheimen Schlüssel verschlüsselt. Die so entstandene Zahl heisst Stammzahl. Die Stammzahl wird ausschliesslich auf der Bürgerkarte gespeichert und darf nur als Ausgangsbasis für die Errechnung des bereichsspezifischen Personenkennzeichens verwendet werden.
Das bereichsspezifische Personenkennzeichen [kurz: bPK] wird mit Hilfe der Stammzahl und der Benennung des Bereiches berechnet. Das Wesen der bPK ist es, dass für unterschiedliche Bereiche unterschiedliche bPK generiert werden. Das bedeutet, dass die bPK für den Bereich Steuern und Abgaben verschieden von der bPK für den Bereich Bauen und Wohnen ist. Die Berechnungsvorgänge sind alle nicht umkehrbar. Von der bPK kann daher nicht auf die Stammzahl geschlossen werden.

11 Art. 35 Ziff. 5 der Verfassung von Portugal [1974/revidiert 2005].

12 § 7 Abs. 1 Datenschutzgesetz.

13 Datensicherheitsverordnung vom 16. Januar 2007 [BGS 157.12].

14 Gemäss § 7 Datensicherheitsverordnung.

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

3. Wichtiges zur Datensicherheit

Schulung der Mitarbeitenden

Das Datenschutzgesetz sieht vor, dass Daten durch angemessene technische und organisatorische Massnahmen vor Verlust, Fälschung und Entwendung, aber auch vor Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte zu sichern sind.[12] Damit die kantonalen und gemeindlichen Organe wissen, was hier genau zu tun ist, hat der Regierungsrat die Datensicherheitsverordnung[13] und darauf gestützt eine *Weisung* erlassen. Der Datenschutzbeauftragte seinerseits hat *Merkblätter*[14] für die Instruktion der Mitarbeitenden erarbeitet.[15]

Alle Organe müssen ihre Mitarbeitenden bezüglich Datensicherheit ausbilden. 2009 hat die Finanzdirektion ein webbasiertes E-Learning-Modul zur Datensicherheit zur Verfügung gestellt, das durch eine externe Firma entwickelt worden war und zu dem der DSB Hinweise gegeben hat.

Das ist eine erfreuliche Erweiterung der Palette an Ausbildungsinstrumenten. Der Lerninhalt dieses Tools entspricht den Merkblättern des Datenschutzbeauftragten. Damit haben die Mitarbeitenden die Möglichkeit, den Kurs individuell an ihrem Arbeitsplatz zu absolvieren. Es wird dabei mit einem Arbeitsaufwand von etwas mehr als einer Stunde gerechnet. Der Kurs kann mit einer Abschlussprüfung abgeschlossen werden. Wird diese bestanden, kann eine Kurs-Bestätigung ausgedruckt werden. Bis Ende Jahr haben über 1400 Mitarbeitende aus der Verwaltung von Kanton und Gemeinden diesen Kurs absolviert.

Sichere E-Mail? – Datenschutzbeauftragter lässt «hacken»

Auch die Verwaltung verschickt immer mehr Nachrichten und Dokumente per E-Mail. Solange dies im verwaltungseigenen Netzwerk geschieht, wird dieser Datenverkehr als sicher beurteilt. Die E-Mails und angehängten Dokumente müssen daher in aller Regel nicht speziell gesichert werden.

Sobald jedoch E-Mails das Verwaltungsnetz verlassen, somit via Internet transportiert werden, ist die Übertragung nicht mehr sicher. Bekanntlich ist der Versand einer E-Mail via Internet weniger vertraulich als eine Postkarte. Denn E-Mails werden an vielen Punkten gespeichert, sie können auf ihrer Reise zum Adressaten eingesehen, kopiert, verändert oder gelöscht werden. Deshalb schreibt das Zuger Recht den Verwaltungsmitarbeitenden vor: «Personendaten und vertrauliche Sachdaten dürfen unverschlüsselt *nur im kantonseigenen Netzwerk* übertragen werden.»[16] Sobald E-Mails, die Personendaten enthalten – was praktisch immer der Fall ist –, an Adressaten ausserhalb des Verwaltungsnetzes gehen, muss der Inhalt zwingend verschlüsselt werden.

Als Anwender würden wir eigentlich erwarten, dass jede E-Mail, die wir versenden, automatisch verschlüsselt wird, und somit sicher zum Adressaten gelangt. Allenfalls wäre uns auch geholfen, wenn wir im E-Mail-Programm den Knopf «Nachricht verschlüsseln» hätten. Leider ist die Technik jedoch noch nicht so weit. Ohne besonderen Aufwand kann einem beliebigen Adressaten keine verschlüsselte E-Mail gesendet werden.

Wie können die Mitarbeitenden nun aber die vorstehend zitierte Vorschrift einhalten? Eine einfache Möglichkeit besteht darin,[17] die zu versendenden Personendaten oder vertraulichen Sachdaten in einer MS-Office-Datei abzuspeichern – somit etwa in einer Word- oder Excel-Datei – und diese mit einem sicheren Passwort zu schützen. Als Alternative können Dokumente auch in einen ZIP-Ordner gestellt werden, der mit einem sicheren Passwort geschützt wird. Dieses Vorgehen wird denn auch in den Zuger Merkblättern zur Datensicherheit seit Jahren empfohlen.[18]

Im Berichtsjahr liessen wir nun die Sicherheit dieses Vorgehens durch eine spezialisierte IT-Firma überprüfen. Die Fragestellung lautete: Ist dieses Vorgehen beim heutigen Stand der Technik noch sicher? Kann das passwortgeschützte Dokument allenfalls «gehackt» werden? Gibt es nicht Tools auf dem Markt, die den Inhalt der Datei zugänglich machen können? Was sind die Anforderungen an das Passwort?

Wir übergaben der IT-Firma 15 MS-Dokumente und ZIP-Ordner, die mit ganz unterschiedlich guten Passwörtern gesichert waren, mit dem Auftrag, diese mit marktgängigen Tools oder Web-Diensten zu öffnen beziehungsweise zu «hacken». Aufgrund der daraus gewonnenen Erkenntnisse waren unsere Empfehlungen in den Merkblättern zur Datensicherheit aus dem Jahr 2008 kritisch zu überprüfen.

Das Resultat: Dokumente, die mit einem 40-Bit-Verschlüsselungs-Algorithmus gesichert waren, konnten innerhalb von wenigen Sekunden mit Tools, die kostenlos im Internet zur Verfügung stehen, geöffnet werden. Diese Verschlüsselungsqualität garantiert somit keinerlei Schutz. Wählt der Anwender hingegen mindestens eine 128-Bit-Verschlüsselung und ist zudem das Passwort genügend stark, ist die Datei im Rahmen normaler Verwaltungstätigkeit genügend geschützt. Das Passwort muss aufgrund des Tests somit mindestens die folgenden Eigenschaften haben:

- Länge von mindestens 8 Zeichen
- mindestens 1 Grossbuchstabe
- mindestens 1 Kleinbuchstabe
- mindestens 1 Zahl
- mindestens 1 Sonderzeichen
- es darf sich nicht um ein Wort aus irgend einer Sprache handeln

Wichtig ist zudem, dass das Passwort dem Adressaten nicht per E-Mail, sondern auf einem anderen Versandkanal zugestellt wird, somit telefonisch oder allenfalls per Fax.

Informatik wohin?

Der Regierungsrat hat am 28. September 2010 die neue Informatikstrategie 2011 bis 2017 beschlossen. Zu diesem wichtigen Projekt hat auch der Datenschutzbeauftragte Stellung genommen. Dabei machte er auf die folgenden Punkte aufmerksam:

- Dass die IT-Dienstleistungen für die kantonale Verwaltung auch längerfristig grundsätzlich

16 § 3 Verordnung über die Benutzung von elektronischen Geräten und elektronischen Kommunikationsmitteln im Arbeitsverhältnis [BGS 154.28].

17 Müssen regelmässig mit Externen Dokumente ausgetauscht werden, gibt es Tools, die einen verschlüsselten Datenverkehr zwischen bekannten Adressaten ermöglichen. Voraussetzung ist dabei, dass Sender und Empfänger diese Tools installiert haben. Für Mitarbeitende der Zuger Verwaltung besteht zudem die Möglichkeit, Externe in geschützte Arbeitsräume von «iZug» einzubeziehen. Diesfalls sind Zugriff und Übertragung gesichert.

18 Das Vorgehen wird in den «Merkblättern zur Datensicherheit» auf S. 6 beschrieben. Die Merkblätter sind auf unserer Website «www.datenschutz-zug.ch» im Bereich «Kanton Zug/ Datensicherheit» veröffentlicht.

durch das Amt für Informatik und Organisation und somit *verwaltungsintern* erbracht werden, begrüsste er ausdrücklich.

- Die Gefahren von aussen nehmen ständig zu, interne Risiken dürfen auch nicht übersehen werden, Geräte werden immer öfters auch mobil eingesetzt und der Ausbau von E-Government und der Einbezug von Externen erhöhen Gefahren und Risiken für Systeme und Datenbestände. Deshalb muss Datensicherheit ein *zentrales Anliegen jeder Datenverarbeitung* sein.
- Offenbar ist ein «erleichterter Datenaustausch» unter Verwaltungsstellen aller Stufen geplant. Diesbezüglich ist zu beachten, dass der Datenaustausch keinesfalls durch die Technik gesteuert oder gar vorgegeben werden darf. Das sind Entscheide, die *vorgängig und abschliessend durch den Gesetzgeber* zu fällen sind.
- Die Komplexität der heutigen IT-Instrumente nimmt ständig zu. Damit die Mitarbeitenden Geräte und Systeme korrekt und sicher beherrschen, sind sie regelmässig zu schulen. Aus- und Weiterbildungsangebote dürfen nicht einzig auf Freiwilligkeit beruhen. Vielmehr muss der Arbeitgeber hier das Erforderliche anordnen.

Der Regierungsrat hat in der IT-Strategie die Bedeutung der Datensicherheit ebenfalls hervorgehoben. Diesbezüglich sollen noch zusätzliche Anpassungen und Weiterentwicklungen von Schutzmassnahmen vorgenommen sowie ein systematisches Risikomanagement implementiert werden. Die Informatikstrategie soll den Datenschutz und die IT-Sicherheit im Denken und Handeln aller an der Weiterentwicklung der Informatik beteiligten Personen und Instanzen verankern. Der IT-Dienstleister wird für die Schulung der Verantwortlichen für Informatiksicherheit im gesamten Kanton zuständig sein. Die Richtlinien im Bereich der Informatiksicherheit sind laufend zu analysieren und zu verbessern. Ergänzend sind regelmässig Informatiksicherheitsaudits vorzunehmen. Für die Informatiksicherheit wurde beim Amt für Informatik und Organisation eine 50%-Stelle geschaffen.

19 § 3 der Verordnung über das Bewilligungsverfahren für den elektronischen Datenaustausch [Online-Verordnung, BGS 157.22].

4. Online-Zugriffe

Online-Gesuche 2010

Im Berichtsjahr hat der Datenschutzbeauftragte zu zwei Gesuchen Stellung genommen. Das Strassenverkehrsamt und der Rettungsdienst des Kantons Zug wünschten den Zugriff im Abrufverfahren auf Daten der gemeindlichen Einwohnerkontrolle. Dem Gesuch des Rettungsdienstes konnte im gewünschten Umfang zugestimmt werden. Beim Gesuch des Strassenverkehrsamtes zeigte es sich, dass die Angaben über den Zivilstand für die Arbeitserfüllung offenbar nur in seltenen Ausnahmefällen erforderlich ist. Diesfalls kann aber die betroffene Person selber den entsprechenden Nachweis erbringen. Der Online-Zugriff auf den Zivilstand war deshalb nicht zu genehmigen, im Übrigen konnte der Zugriff bewilligt werden.

Wird Online-Zugriff auf zusätzliche Daten gewünscht – was ist zu tun?

Es stellte sich die Frage, was zu tun ist, wenn eine Verwaltungsstelle, die über einen bewilligten Online-Zugriff verfügt, Zugriff auf *zusätzliche Daten* wünscht.

Aufgrund der Online-Verordnung ist klar, dass diesfalls ein *neues* Online-Gesuch zu stellen ist. Denn nur so ist gewährleistet, dass alle involvierten und anzuhörenden Stellen Gelegenheit haben, ihre diesbezügliche Beurteilung gemäss Online-Verordnung abgeben zu können.[19] Ein «kleiner Dienstweg» ist in der Verordnung *nicht* vorgesehen.

II. Berichterstattung 2010

1. Fälle aus unserer Beratungspraxis

Falls Sie im Folgenden wichtige Themen vermissen, konsultieren Sie bitte die früheren Tätigkeitsberichte. Sie finden dort über 370 weitere Fallbeispiele. Die Tätigkeitsberichte 1999 – 2010 können Sie übrigens beim DSB kostenlos bestellen [041 728 31 47]. Sie finden sie zudem auch layoutgetreu im Internet unter: «www.datenschutz-zug.ch», Rubrik «Kanton Zug/Tätigkeiten».

Im Bereich «Suche» können Sie übrigens Abfragen machen, die sich ausschliesslich auf die Tätigkeitsberichte beziehen.

1.1 Übersicht

Stichwort	Fragestellung	Fall Nr.	Seite
AHV-Nummer	Wozu braucht die Schule die AHV-Nummer der Kinder?	10	16
Akteneinsicht	Zur Einsicht in Akten abgeschlossener Strafverfahren	16	17
Amtsblatt	Amtsblatt im Internet muss amtliche Mitteilungen regelmässig löschen	4	12
Arbeitsrecht	Wann ist eine Videoüberwachung eines Büros der Verwaltung zulässig?	7	13
Arbeitsrecht	Wenn Mitarbeitende ausfallen – wer hat Zugriff auf deren E-Mails?	8	14
Bibliothek	Bibliotheksoftware muss regelmässig Kundendaten löschen	3	11
Datensicherheit	Wie viel Datensicherheit für ein Datenbankprogramm über die SchülerInnen	6	13
Datenvernichtung	Private verlangen von der Verwaltung die Löschung all ihrer Daten	1	10
E-Mail	Wenn Mitarbeitende ausfallen – wer hat Zugriff auf deren E-Mails?	8	14
E-Mail	Wie hat die Verwaltung mit E-Mails von anfragenden BürgerInnen umzugehen?	19	19
Fahrtauglichkeit	An wen geht der Arztbericht bei der Abklärung der Fahrtauglichkeit?	15	17
Geoinformationen	Private verlangen die Löschung von Daten über ihre Grundstücke im Internet	2	10
Grundbuchdaten	Private verlangen die Löschung von Daten über ihre Grundstücke im Internet	2	10
Internet	Keine Fotos von Kindergartenschüler auf der Schulwebsite	9	15
Internet	Private verlangen die Löschung von Daten über ihre Grundstücke im Internet	2	10
Krankengeschichten	Wie revisionssicher muss die Software sein?	14	16
Löschen von Daten	Private verlangen von der Verwaltung die Löschung all ihrer Daten	1	10
Personalrecht	s. Arbeitsrecht		
politische Partei	Sind einer politischen Partei die Adressen aller Stimmberechtigten herauszugeben?	18	19
Sammelauskunft	Sind einer politischen Partei die Adressen aller Stimmberechtigten herauszugeben?	18	19
Schule	Keine Fotos von Kindergartenschüler auf der Schulwebsite	9	15
Schule	Wozu braucht die Schule die AHV-Nummer der Kinder?	10	16
Schule	Informationen an SchülerInnen nur noch per E-Mail?	11	16
Schule	Wie viel Transparenz über Gewaltvorfälle?	12	16
Schule	Datenschutzbeauftragter unterstützt Arbeiten von SchülerInnen und Studierender	13	16
Schulsoftware	Wie viel Datensicherheit für ein Datenbankprogramm über die SchülerInnen	6	13
Software	Bibliotheksoftware muss regelmässig Kundendaten löschen	3	11
Software	Wie revisionssicher muss Software Gesundheits- bzw. Sozialbereich sein?	14	16
Stimmregister	Sind einer politischen Partei die Adressen aller Stimmberechtigten herauszugeben?	18	19
Strafanstalt	Welche Auskünfte über Strafgefangene an eine ausländische Botschaft?	17	17
Strafverfahren	Zur Einsicht in Akten abgeschlossener Strafverfahren	16	17
Strassenverkehr	Wenn die Fahrtauglichkeit überprüft wird – an wen geht der Arztbericht?	15	17
Videoüberwachung	Anfragen, Grundsätzliches und Hinweise zum Gesetzesprojekt	5	12
Videoüberwachung	Wann ist eine Videoüberwachung eines Büros der Verwaltung zulässig?	7	13
Wahlen/Abstimmungen	Sind einer politischen Partei die Adressen aller Stimmberechtigten herauszugeben?	18	19
Weitergabe von E-Mails	Wie hat die Verwaltung mit E-Mails von anfragenden BürgerInnen umzugehen?	19	19

Wo wir helfen können – und wo nicht
Bei vielen Anfragen, die bei uns eingehen, geht es um die Datenbearbeitung von *Zuger Unternehmen oder Zuger Privatpersonen.*[20]

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

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

Für Zuger Anfragende ist es ohnehin oft nicht leicht nachvollziehbar, weshalb für die Datenbearbeitungen durch Zuger Unternehmen nicht auch der Zuger Datenschutzbeauftragte zuständig ist, sondern sie sich «in Bundesbern» erkundigen müssen.

1.2 Kanton

Fall 1 Löschen Sie bitte alle meine Daten!
Auch dieses Jahr erhielten wir wieder verschiedene Anfragen zum Thema Vernichten von Daten. So verlangten Privatpersonen von der Verwaltung oder der Datenschutzstelle: «Löschen Sie bitte alle meine Daten!»

Im Vorjahr gingen wir in allgemeiner Weise bereits auf dieses Thema ein und stellten abschliessend fest: «Die Akten eines öffentlichen Organs dürfen daher grundsätzlich nicht vernichtet werden.»[21]

Ergänzend kann festgehalten werden, dass die Verwaltung das fragliche Dossier bereinigen und dem Privaten zur Einsicht geben kann, damit klar ist, über welche Daten die Verwaltung noch verfügt. Je nach Situation kann das Dossier anschliessend unter besonderem Verschluss aufbewahrt werden, damit sichergestellt ist, dass bei der Verwaltung nur noch wenige Personen Einsicht nehmen können.

Fall 2 Kanton veröffentlicht die Grundbuchdaten meiner Liegenschaft im Internet – das will ich nicht!
Mehrere Private verlangten beim Datenschutzbeauftragten, dass die Grundbuchdaten ihrer Liegenschaft, eine ganze Reihe weiterer grundstücksbezogener Daten und die detailgetreue Luftaufnahmen ihrer Liegenschaft, die der Kanton im Internet[22] veröffentlicht, zu löschen seien. Welche Daten zu Zuger Grundstücken sind im Internet, somit weltweit durch jedermann frei zugänglich, kopierbar und ausdruckbar?

Es geht insbesondere um die folgenden Daten über alle Zuger Grundeigentümer: Vorname und Familienname des Grundeigentümers, Adresse, nähere Bezeichnung des Grundstücks, Grundstückbeschreibung, Grundstücksfläche, Nutzung des Grundstücks nach Zonen, Landwert nach Landwertzone, Assekuranznummer des Gebäudes, Gebäudebezeichnung, Baujahr des Gebäudes, Eigentumsform, Adresse des Gebäudeverwalters, Angaben der amtlichen Vermessung, Rohrleitungssysteme, fotografisches Luftbild mit sämtlichen Details der Liegenschaft, des Umschwungs und der Bepflanzung [etc.].

Zudem können pro Liegenschaft verschiedene Berichte mit allen Daten generiert und ausgedruckt werden.

Die Grundstückseigentümer wollten nicht, dass weltweit jedermann all diese Daten über sie einsehen und auswerten kann. Sie machten insbesondere geltend, dass sie mehrmals monatlich von Kaufinteressenten aus dem In- und Ausland kontaktiert beziehungsweise belästigt wurden, dass sie regelmässig durch diverse Unternehmen im Zusammenhang mit ihrer Liegenschaft

20 Hausarzt, Vermieter, Arbeitgeber, Nachbar etc.

21 DSB TB 2009 Fall Nr. 2 S. 10/11.

22 Unter «www.zugmap.ch».

angegangen wurden, dass jedermann ihre landwirtschaftlichen Beiträge eruieren kann, dass die detaillierte Foto ihres Hauses ihre persönliche Sicherheit tangiert, dass ihre Daten offenbar verfolgt und ausgewertet werden – all dies verletze ihr Interesse auf Schutz ihrer Privatsphäre und Achtung ihrer Persönlichkeitsrechte. Es sei keinerlei Grund erkennbar, wieso irgend welchen privaten Dritten weltweit all diese Daten über sie zur Verfügung gestellt werden [völlig unbestritten war übrigens, dass öffentliche Stellen und Beauftragte, die für ihre Aufgabenerfüllung auf solche Daten angewiesen sind, diese auch erhalten können; dafür stehen aber besondere Systeme und Tools in geschlossenen IT-Umgebungen zur Verfügung].

Der Datenschutzbeauftragte teilte die Auffassung der Zuger Grundeigentümer in seiner Stellungnahme gegenüber dem Regierungsrat vollumfänglich. Es ist kein Grund und kein Interesse ersichtlich, wieso x-beliebige Private weltweit alle diese oben aufgeführten Daten einsehen und zu beliebigen Zwecken verwenden dürfen. Diese Publikation befriedigt ausschliesslich die Neugierde Dritter. Dies ist in keiner Art und Weise durch den Staat zu fördern. Zu bedenken ist bei Veröffentlichungen im Internet auch, dass die Daten weltweit, somit auch in Staaten ohne Datenschutzbestimmungen zugänglich sind, die Betroffenen mit der Veröffentlichung jegliche Kontrolle über ihre Daten verlieren, sich Bedrohungen und Sicherheitsprobleme aller Art ergeben können und dass die veröffentlichten Daten faktisch nicht mehr gelöscht oder korrigiert werden können, da im Internet Publiziertes nicht mehr zurückgeholt oder geändert werden kann. Der Regierungsrat verweigerte gegenüber einem Privaten die Sperrung seiner Daten jedoch.[23] Er beschloss aber, die Frage der Publikation von grundstücksbezogenen Daten im Internet im Rahmen einer Verordnung zu regeln und dabei zu prüfen, ob und unter welchen Voraussetzungen ein Sperrrecht vorzusehen sei.

Sofern und soweit nicht übergeordnetes Bundesrecht zwingend die Veröffentlichung dieser Daten verlangt – was gemäss unserer Rechtsauffassung nicht beziehungsweise allenfalls höchstens teilweise der Fall ist –, dürfen solche Daten Privater durch den Staat *nicht ins Internet* gestellt werden. Zumindest muss ein *voraussetzungsloses Sperrrecht* vorgesehen werden. Etwas anderes wäre umso unverständlicher, nachdem sogar Google Street View in Deutschland jedem Hauseigentümer und selbst jedem Mieter das Recht gibt, seine Daten – somit die Fotos von Gebäude und Umgebung – in Google Street View voraussetzungslos mit wenigen Klicks zu löschen.[24]

Der Datenschutzbeauftragte wird sich auch 2011 intensiv mit dieser Angelegenheit befassen und im nächsten Tätigkeitsbericht über den aktuellen Stand informieren.

Fall 3 Datenschutz – auch in der Bibliothek

Eine ganze Reihe kantonaler Bibliotheken befasste sich mit der Ablösung der bisherigen Bibliotheksverwaltungssoftware. Die neue Lösung sah vor, dass Medien-, Benutzer- und Kundendaten extern bei einer privaten Firma gehostet und betreut werden sollten. Der Datenschutzbeauftragte wurde um eine Beurteilung dieses Projekts gebeten.

Grundsätzlich wäre eine verwaltungsinterne Lösung, somit Hosting und Betreuung durch den kantonalen IT-Dienstleister vorzuziehen gewesen, sind doch Daten, die das eigene Netz nicht verlassen, grundsätzlich besser geschützt. Zudem unterstehen alle Beteiligten aufgrund des Personalrechts dem Amtsgeheimnis und die Gefahr der Nutzung der Kundendaten für andere Zwecke ist verwaltungsintern gering. Im weiteren ist dem DSB auch jederzeit möglich, allfällige Kontrollen vorzunehmen.

Ein Outsourcing ist rechtlich aber zulässig, sofern entsprechende zusätzliche technische und organisatorische Massnahmen implementiert werden. Beim vorliegenden Projekt ist eine verschlüsselte Übertragung vorgesehen, das Rechenzentrum entspricht offenbar mindestens den aktuellen Sicherheitsstandards, die externen Mitarbeitenden sollten vertraglich zur Geheimhaltung und das Unternehmen zum Verbot einer Nutzung der Daten für andere Zwecke ver-

23 Rechtskräftiger Entscheid des Regierungsrates vom 28. September 2010.

24 «https://streetview-deutschland.appspot.com/submission».

pflichtet werden. Die technischen Anforderungen waren – soweit ersichtlich – erfüllt.

Ein heikler Punkt im Bibliothekswesen ist die Bearbeitung und Speicherung der Kundendaten. Zum Schutze der Privatsphäre der Kundschaft muss es ausgeschlossen sein, dass die Angaben über die ausgeliehenen Werke über lange Zeit, allenfalls Jahre, gespeichert bleiben und so ein eigentliches Persönlichkeitsprofil über jede Kundin angelegt wird. Vielmehr müssen bei den Kundendaten die Angaben zu den ausgeliehenen Werken sobald als möglich und automatisch durch das Bibliotheksprogramm gelöscht werden. Diese Löschfrist kann im Bereiche von 30 bis 60 Tagen liegen.

Die vorliegende Bibliothekssoftware war zwar in der Lage, diese automatische Löschung vorzunehmen, dies hätte jedoch Einfluss auf statistische Erhebungen der Bibliotheken gehabt, was die Bibliotheksleitenden nicht wollten.

Bekanntlich ist technisch fast alles machbar und so konnte erfreulicherweise auch hier eine technische Lösung gefunden werden, die durch die Löschung der «Kunden-History» die Privatsphäre der BibliothekskundInnen achtet, die es den Bibliotheksleitungen aber trotzdem ermöglicht, eine Statistik über die ausgeliehenen Werke zu generieren.

Fall 4 Das Amtsblatt im Internet – und das Recht auf Vergessen?

Gemäss Gesetz[25] ist die Publikation des Amtsblattes im Internet zulässig. Davon ausgenommen sind im Amtlichen Teil besonders schützenswerte Daten. Die Veröffentlichung des Amtlichen Teils ist nach einer bestimmten Frist, die der Regierungsrat festsetzt, [26] zu löschen.

Eine Überprüfung des Datenschutzbeauftragten ergab, dass diese gesetzlichen Vorgaben nicht eingehalten waren: Ab 2007/Nr. 1 waren sämtliche Ausgaben mit dem Amtlichen Teil im Internet zugänglich. Zudem fanden sich viele besonders schützenswerte Daten zu Privatpersonen. Die für das Amtsblatt zuständige Staatskanzlei veranlasste umgehend, dass zukünftig keine besonders schützenswerten Personendaten mehr im Internet zu veröffentlich sind und dass immer nur noch die aktuelle Ausgabe des Amtsblatts im Internet ist. Damit ist den gesetzlichen Vorgaben diesbezüglich vorbildlich nachgelebt.

Fall 5 Videoüberwachung – bald gesetzlich geregelt?

Die Videoüberwachung beschäftigt Privatpersonen, Medien und Gemeinden. Regelmässig erhalten wir denn auch Anfragen von Privaten, die wissen wollen, wo sie in der Öffentlichkeit von Videoüberwachungsanlagen erfasst werden. Gemeinden erkundigen sich, ob sie an bestimmten neuralgischen Stellen – etwa im Umfeld von Schulen oder Entsorgungsanlagen – Kameras installieren dürfen.

Bei der Videoüberwachung handelt es sich grundsätzlich um einen schweren Eingriff in die Privatsphäre. In einer freiheitlichen Gesellschaft haben wir das Recht, uns in der Öffentlichkeit frei, unbeobachtet und unkontrolliert zu bewegen. Ausnahmsweise kann Videoüberwachung das richtige Instrument sein, um ein ganz bestimmtes Rechtsgut zu schützen. Der Einsatz benötigt grundsätzlich eine ausdrückliche gesetzliche Grundlage. Zurzeit gibt es im Zuger Recht *keine* diesbezügliche Regelung. Aufgrund eines politischen Vorstosses[27] aus dem Jahr 2007 ist die Sicherheitsdirektion zurzeit jedoch an der Ausarbeitung eines Gesetzes. Der Datenschutzbeauftragte wird dazu beigezogen werden. Voraussichtlich kommt die Vorlage des Regierungsrates Ende 2011 in den Kantonsrat, wird im Jahr 2012 im Kantonsrat beraten und sollte auf den 1. Januar 2013 in Kraft treten.

Videoüberwachung wird in ihrer Wirkung von vielen oft überschätzt, obwohl die meisten wissenschaftliche Studien belegen, dass der Sicherheitsgewinn in aller Regel gering ist.[28] Auch wenn Videoüberwachung nicht das Wundermittel gegen alles und jedes ist, unter gewissen Umständen kann der Einsatz sinnvoll sein. Wir begrüssen daher aus grundsätzlichen Überlegungen die ausdrückliche Regelung in einem formellen Gesetz. Wichtig ist dabei, dass das Verhältnismässigkeitsprinzip eingehalten ist und

25 § 6 Abs. 3 Publikationsgesetz [BGS 152.3].

26 Der Regierungsrat hat diese Frist bis anhin noch nicht festgesetzt.

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

28 Vgl. dazu ganz aktuell: Carmen Lingg S. 92 in: «3. Zürcher Präventionsforum – Videoüberwachung als Prävention», Christian Schwarzenegger/Rolf Nägeli [Hrsg.], Zürich Schulthess 2010.

eine Lösung gefunden wird, die eines freiheitlichen Rechtsstaates würdig ist.
Wir haben in den letzten Jahren viele konkrete Hinweise zur Videoüberwachung veröffentlicht. Eine Liste der besprochenen Fälle aus der Praxis finden Sie in unserem Tätigkeitsbericht aus dem Jahre 2007.[29]

1.3 Datensicherheit

Fall 6 Web-Zugriff auf LehrerOffice – wie viel Datensicherheit?
LehrerOffice ist eine Software, die im Kanton Zug durch Schulen und Lehrpersonen zur Verwaltung der Schülerdaten eingesetzt wird. Geplant ist die Ablösung der bisher dezentralen Datenhaltung durch eine zentral betreute Weblösung. Die Entwickler erkundigen sich, wie stark der Zugang via Internet auf das System zu sichern sei.

LehrerOffice verwaltet nicht nur die Noten der SchülerInnen, sondern kann auch persönliche Beurteilungen, Bemerkungen und Informationen zur Person des Schülers, seiner Familie und seines Umfeldes enthalten. Mit der Zeit entsteht über die einzelne Schülerin ein eigentliches Persönlichkeitsprofil. Die Risiken, dass Schüler versuchen, dieses System anzugreifen, sind hoch, da es sich um ein höchst interessantes Angriffsobjekt handelt.

Es ist deshalb in technischer und organisatorischer Hinsicht grundsätzlich ein *starker* Schutz der LehrerOffice-Daten vorzusehen.

Wir haben deshalb empfohlen, jedenfalls die folgenden *technischen* Massnahmen vorzusehen:
- verschlüsselte Verbindung zur Applikation [SSL-Verschlüsselung];
- der Gebrauch eines starken Passwortes wird erzwungen und durch das System kontrolliert [min. 8 Zeichen, Buchstaben, Zahlen und Sonderzeichen obligatorisch];
- der Passwort-Wechsel wird mindestens alle sechs Monate erzwungen und kontrolliert;
- das Benutzerlogin wird nach fünf fehlerhaften Anmeldeversuchen für 24 Std. gesperrt;
- für gewisse User, die umfassenden Zugang zum System beziehungsweise zu den Daten haben – wie etwa Schulverwaltungen – ist der Einsatz eines dritten Sicherheitselements [wie RSA-Token] zu begrüssen.

In organisatorischer Hinsicht ist folgendes vorzusehen:
- der Zugriff auf Programm und Daten durch die Mitarbeitenden der Schule erfolgt gemäss detailliertem Rollen- und Berechtigungskonzept;
- die Berechtigungen werden durch die Schulverwaltung regelmässig überprüft [Eintritt, Mutationen, Austritt];
- die wichtigsten Daten [z.B. Noten] werden regelmässig auf Korrektheit, jedenfalls Plausibilität überprüft;
- die Lehrpersonen dürfen ihre Zugangsberechtigung nicht weitergeben;
- ein korrektes Rollen- und Berechtigungskonzept weist im Rechenzentrum nur den Berechtigten den Zugriff auf die Personendaten zu;
- die Serverumgebung entspricht den Vorgaben der Zuger Datensicherheitsverordnung;
- sollte das Passwort durch die Lehrperson aufgeschrieben oder elektronisch gespeichert werden, darf dies nicht im Bereich der Schule sein.

Sind diese Anforderungen eingehalten und sind die Webapplikation und das zentrale System gemäss den heutigen üblichen Standards geschützt, erfüllt LehrerOffice zurzeit die Vorgaben der Zuger Datensicherheitsverordnung. Ohne Zweifel wäre die Sicherheit wesentlich höher, wenn jeder User für den Zugang zu LehrerOffice – wie beim Internet-Banking – eine SmartCard oder einen Token benützen müsste. Allerdings wären Betreuungsaufwand und Kosten dafür erheblich.

1.4 Personalrecht

Fall 7 Bei Vorfällen – Videoüberwachung eines Büros?
In einem Büro eines Mitarbeiters einer Verwaltungsstelle wurden durch eine unbekannte Drittperson regelmässig Manipulationen von allenfalls strafrechtlicher Relevanz vorgenommen. Es stand aber eine strafbare Handlung von

29 DSB TB 2007 Nr. 2 S. 8.

nur geringfügiger Bedeutung zur Diskussion. Die Voraussetzungen, dass die Polizei eine Videoüberwachung vornimmt, waren hier deshalb nicht gegeben.

Der Datenschutzbeauftragte wurde angefragt, ob er eine Überwachung des Büros durch die Verwaltung mit einer Videoanlage bewilligen könne, damit die Täterschaft allenfalls überführt werden könnte.

Im Gegensatz zu anderen Kantonen[30] liegt es grundsätzlich nicht am Zuger Datenschutzbeauftragten, Videoüberwachungen zu bewilligen oder zu verweigern; er gibt dazu Hinweise.

Beweismittel müssen rechtmässig erhoben werden, ansonsten sie in einem Gerichtsverfahren nicht zugelassen werden, somit unbeachtlich sind und der Aufwand vergebens war. Die heimliche Überwachung eines Arbeitsplatzes ist grundsätzlich heikel. Das Bundesgericht hat in einem Urteil im Jahr 2009 entschieden, dass die heimliche Überwachung eines Arbeitnehmers nicht zum Vornherein beziehungsweise in jedem Fall unzulässig ist.[31] Die heimliche Überwachung des Kassaraums einer Bijouterie, in dem sich Mitarbeitende nur ganz kurz aufhalten, erachtete es – im Gegensatz zur Vorinstanz – als zulässig.

Fazit: Unter Berücksichtigung dieses Urteils geht der Datenschutzbeauftragte davon aus, dass der Arbeitgeber das Verhalten des Mitarbeiters im vorliegenden Fall ausnahmsweise überwachen darf, wenn dieser der Überwachungsanlage nicht dauernd ausgesetzt ist, sondern lediglich sporadisch und nur für eine kurze Zeit.

Ob der Einsatz einer heimlichen Videoüberwachung im Rahmen einer privaten Beweiserhebung rechtmässig ist, hat der Arbeitgeber nach sorgfältiger Prüfung des konkreten Sachverhalts und aller zu berücksichtigenden Umstände und unter Beachtung des Verhältnismässigkeitsprinzips zu entscheiden. In einem allfälligen Strafverfahren wird abschliessend zu entscheiden sein, ob die Aufzeichnung als Beweismittel zugelassen wird.

30 Vgl. dagegen etwa Basel-Stadt: § 6a Gesetz über den Schutz von Personendaten [Datenschutzgesetz, 153.260].

31 Entscheid des Bundesgerichts vom 12. November 2009/6B_536/2009.

32 § 2 Abs. 1 Verordnung über die Benutzung von elektronischen Geräten und elektronischen Kommunikationsmitteln im Arbeitsverhältnis [BGS 154.28].

Fall 8 Was passiert mit E-Mails, wenn Mitarbeitende ausfallen?

E-Mail ist auch in der kantonalen Verwaltung die Kommunikationsform par excellence. Technische Pannen oder Nichterreichbarkeit von Mitarbeitenden werden bei bestimmten Stellen daher nur höchst ungern hingenommen. Was ist deshalb zu tun, wenn E-Mails eingehen, die Mitarbeitenden aber nicht reagieren, weil sie erkrankt, in den Ferien verunfallt, freigestellt oder verstorben sind?

Im Berichtsjahr wurde die Regelung der vorliegenden Materie neu geregelt. Dabei war auch der Datenschutzbeauftragte intensiv mitbeteiligt.

In der Zuger Verwaltung ist der Zugang zum Datenbereich und zum E-Mail-Konto des Mitarbeitenden mit einem Passwort geschützt. Gemäss ausdrücklicher Vorschrift ist das Passwort persönlich und darf nicht weitergegeben werden.[32] Vorgesetzte dürfen somit von ihren Mitarbeitenden nicht verlangen, ihr Passwort bekanntzugeben. Was ist nun bei unerwarteten längeren Abwesenheiten zu tun? Zwei Dinge sind hier zu unterscheiden: Für die meisten Stellen ist es in erster Linie wichtig, dass möglichst schnell eine *Abwesenheitsmeldung* eingerichtet wird, damit allfällige E-Mail-Sender über die Abwesenheit des Mitarbeitenden und über dessen Stellvertretung im Bild sind. In einem zweiten Schritt kann es erforderlich sein, dass auf die bereits eingegangenen E-Mails zugegriffen werden kann. Was ist in diesen beiden Fällen zu tun?

Zur Abwesenheitsmeldung

Unter dem bei der kantonalen Verwaltung bis ins Jahr 2009 im Einsatz stehenden Mail-System war es möglich, dass bestimmte Aussenstehende, etwa Vorgesetzte oder Sekretariate, eine Abwesenheitsregel im E-Mail-Konto eines Mitarbeitenden placieren konnten, ohne dass sie das Passwort des Betroffenen benötigten und ohne dass sie Einsicht in das E-Mail-Konto oder auf Daten erhielten. Bei der Umstellung auf MS-Outlook entfiel diese Möglichkeit leider, und nun war es Dritten ohne Kenntnis des Passwortes nicht mehr möglich, eine Abwesenheitsmitteilung einzugeben.

Damit der Arbeitsbereich des ausgefallenen Mitarbeitenden – auf dem sich ja zulässigerweise auch private E-Mails oder private Dateien befinden können[33] – nicht sofort dem Vorgesetzten zugänglich wird, kann der Vorgesetzte nun neuerdings den kantonalen IT-Dienstleister anweisen, auf dem E-Mail-Konto des ausgefallenen Mitarbeitenden eine bestimmte Abwesenheitsmeldung einzurichten.[34] Der IT-Dienstleister verfügt über ein Tool, solche Meldungen auf den E-Mail-Konten eingeben zu können, ohne dass das Passwort benötigt oder zurückgesetzt wird und ohne Einsicht in E-Mails oder Daten zu erhalten. Wird die Abwesenheitsregel auf diese Art möglichst umgehend eingerichtet, ist es meist nicht nötig, dass Vorgesetzte auch Einsicht in E-Mails oder Daten der ausgefallenen Person haben müssen, da die externen Stellen nun darüber im Bild sind, an wen sie sich wenden müssen. Diesfalls sind die Interessen des Arbeitgebers an einem einwandfreien Geschäftsgang gewahrt und der abwesende Mitarbeitende ist seinerseits davor geschützt, dass Vorgesetzte oder Sekretariate vorschnell auf seine Daten zugreifen.

Die hier beschriebene Lösung steht seit Juli 2010 zur Verfügung. Bis Ende des Berichtsjahres hat der IT-Dienstleister in insgesamt zehn Fällen Abwesenheitsmeldungen eingerichtet.

Zum Zugriff auf das E-Mail-Konto und auf Daten
Bei langer Abwesenheit, bei Freistellung und im Todesfall muss es aber auch die Möglichkeit geben, dass auf E-Mail-Konto und Daten des Betroffenen zugegriffen wird. Bis anhin wurde in diesen Fällen der Datenschutzbeauftragte beigezogen.[35] Ihm wurde – als unabhängiger Stelle – der Zugriff auf das Konto des ausgefallenen Mitarbeitenden eingerichtet und er nahm die Triage zwischen Geschäftlichem und Privatem vor.

Aufgrund der Revision der diesbezüglichen Verordnung ist nun neu die vorgesetzte Stelle berechtigt, bei länger dauernder Abwesenheit eines Mitarbeitenden auf dessen geschäftliche Daten zuzugreifen. Folglich hat der Vorgesetzte auf das E-Mail-Konto und auch auf die Daten des Betroffenen Einsicht. Befinden sich private E-Mails oder private Dateien auf dem Konto, sind diese vor der Einsicht des Vorgesetzten – im Gegensatz zu früher – nun *nicht mehr geschützt*. Der Datenschutzbeauftragte muss zukünftig somit nicht zwingend beigezogen werden, um diese Triage zwischen Geschäftlichem und Privatem vorzunehmen – aber er darf dazu beigezogen werden. Da der Zugriff des Vorgesetzten auf Privates heikel ist und allenfalls das Arbeitsverhältnis belasten kann, dürfte es sinnvoll sein, auch zukünftig, wenn immer möglich und nötig, den Datenschutzbeauftragten mit der Triage zu beauftragen.

Fazit: Seit Juli 2010 können die Vertraulichkeit und der Schutz allenfalls vorhandener privater Daten bei der privaten Nutzung von E-Mail, Computer oder anderer Kommunikationsmittel durch die Mitarbeitenden nicht mehr gewährleistet werden, da Vorgesetzte allenfalls Zugriff auf diese Daten erhalten. Die Regelung ist aber rechtmässig, da die Interessen des Arbeitgebers an einem einwandfreien Geschäftsgang den Interessen der Mitarbeitenden klar vorgehen. Über diese wichtige Änderung wurden übrigens sämtliche Mitarbeitende per E-Mail informiert.

1.5 Schule

Fall 9 Fotos der Kindergartenschüler auf der Schulwebsite

Verschiedene Eltern beschwerten sich, weil Fotos ihrer Kinder – zum Teil Primarschüler, zum Teil Kindergartenschüler – prominent auf der Website der Schule veröffentlicht waren. Sie erkundigten sich nach der Rechtslage und nach allfälligen Interventionsmöglichkeiten.

Ohne Zustimmung der Eltern ist die Publikation von Fotos ihrer Kinder nicht erlaubt. Die Eltern können daher die Löschung der Bilder verlangen. Wir haben verschiedentlich darauf hingewiesen, dass im Internet keine Fotos von Schülerinnen und Schülern zu publizieren sind,[36] wenn diese erkennbar sind – selbst mit Zustimmung der Eltern nicht.

Die Eltern haben in der Folge die Löschung der entsprechenden Fotos verlangt.

33 § 8 der vorstehenden Verordnung lässt eine zeitlich geringfügige private Nutzung ausdrücklich zu.

34 § 5 Abs. 1 der vorstehenden Verordnung.

35 Gestützt auf den entsprechenden Regierungsratsbeschluss vom 24. August 2004.

36 DSB TB 2007 Fall Nr. 3 S. 9/10; DSB TB 2005 Fall Nr. 9 S. 11/12.

Fall 10 Wozu braucht die Schule die AHV-Nummer meiner Kinder?
«Wozu, um Himmels willen, braucht die Schule die AHV-Nummer von unserem Kindergärtler?!» Das wollten Eltern von uns wissen, nachdem die Schule sich bei ihnen nach der AHV-Nummer der Kinder erkundigt hatte.

Das Bundesamt für Statistik [BFS] ist zurzeit daran, das Projekt «Modernisierung der Erhebungen im Bildungsbereich/MEB» umzusetzen. Es handelt sich um eine grossangelegte gesamtschweizerische Erhebung im Bildungs- und Schulbereich. Dabei werden eine ganze Reihe von Daten über Lehrpersonen und SchülerInnen erhoben, darunter auch die neue AHV-Versichertennummer [«AHV-N13»]. Das BFS verfügt über die entsprechenden Rechtsgrundlagen, die Datenerhebung durch die Schule war somit korrekt.

Zusätzliche Hinweise zum Projekt «MEB» finden Sie in unserem Tätigkeitsbericht 2009.[37]

Fall 11 Mittelschule: Infos an Schüler nur noch per E-Mail?
Für die Verbreitung von Informationen ist E-Mail ein praktisches Instrument. Es stellte sich in diesem Zusammenhang die Frage, ob Mittelschüler verpflichtet werden können, der Schulleitung eine E-Mail-Adresse bekannt zu geben, um so eine einfache Kommunikation zwischen Schule und Schülerin zu ermöglichen.

Es gibt keine Rechtsgrundlage, die SchülerInnen verpflichtet, zu Schulzwecken ein E-Mail-Konto zu haben und es auch regelmässig auf eingegangene Nachrichten zu kontrollieren.[38]

Vermutlich würde dieser Kommunikationsweg aus praktischen Gründen auch gar nicht zuverlässig funktionieren, da viele Schüler ihre E-Mail-Adresse häufig wechseln, andere kaum mailen, sondern nur SMS versenden und Dritte ihre E-Mails nur sehr unregelmässig abrufen.

Ergänzend ist darauf hinzuweisen, dass es der Schule übrigens nicht gestattet ist, Personendaten oder besonders schützenswerte Daten unverschlüsselt über das öffentlich Netz zu versenden.

Die Information über Aktuelles via Lehrperson, «Schwarzes Brett», Schul-Website oder Telefonalarm dürfte deshalb nach wie vor zuverlässiger sein.

Fall 12 Gewalt in der Schule – wie viel Transparenz?
Schulsozialarbeiter werden regelmässig mit Fällen von Gewalt an der Schule konfrontiert. Neuere Ansätze in der Prävention von Gewalt an Schulen sehen vor, solche Vorfälle nicht zu verschweigen, sondern Eltern und SchülerInnen über die Vorfälle und auch die getroffenen Massnahmen oder Sanktionen offen zu informieren. Geplant ist, solche Informationen in der Schule am «Schwarzen Brett» bekannt zu machen. Die Eltern sollten im Rahmen eines Mitteilungsblattes oder Briefes informiert werden. Ist dies zulässig?

Sofern die Information vollständig anonym erfolgt, Beteiligte somit weder namentlich genannt, noch aufgrund der Schilderung erkennbar sind, ist eine solche Information zulässig. Sind Täter oder Opfer aber erkennbar, ist dies grundsätzlich nicht zulässig. Anders verhält es sich nur dann, wenn alle Beteiligten einer solchen Information freiwillig und ausdrücklich zustimmen.

Fall 13 DSB unterstützt Arbeiten von Schülern und Studierenden
Im Berichtsjahr hat der Datenschutzbeauftragte verschiedene Arbeiten – insbesondere Vorträge oder Semesterarbeiten – von Studierenden sowie Schülerinnen und Schülern zum Thema Datenschutz und Datensicherheit unterstützt: Durch Beratung, Hinweise und Tipps oder kostenlose Abgabe von weiterführenden Unterlagen.

1.6 Gesundheitswesen

Fall 14 Krankengeschichte – revisionssicher?
Software zur Erfassung elektronischer Krankengeschichten sieht aus Gründen der Beweisbarkeit in aller Regel vor, dass erfasste Einträge nicht mehr verändert werden können. Eine Stelle erkundigte sich, ob man nicht dem Vorgesetzten die Kompetenz geben dürfe, Änderungen

37 DSB TB 2009 Fall Nr. 24 S. 19/20.

38 Anders ist die Rechtslage diesbezüglich hingegen für die Verwaltungsangestellten, die dazu ausdrücklich verpflichtet sind [§ 5 der Verordnung über die Benutzung von elektronischen Geräten; BGS 154.28].

vorzunehmen, damit Tippfehler und Ungenauigkeiten in den Einträgen nachträglich korrigiert werden könnten.

Wir rieten davon ab. Dass bei solchen Einträgen Schreibfehler und Ungenauigkeiten vorkommen, ist normal, handelt es sich teilweise doch um einen elektronischen «Notizblock». Dagegen ist zu Beweiszwecken wichtiger, dass die Einträge nicht mehr verändert werden können. Dies schützt in erster Linie auch die Mitarbeitenden, können sie sich doch darauf verlassen, dass das System ihre Einträge korrekt führt.

Nachträgliche Änderungen dürfen nur dann zugelassen sein, wenn diese ihrerseits sauber protokolliert werden, damit stets ersichtlich ist, wer, was, wann, wie abgeändert hat.

Fall 15 Fahrtauglichkeit: An wen geht der Arztbericht?

Um die Fahrtauglichkeit von Autofahrenden zu überprüfen, sieht das Strassenverkehrsrecht für bestimmte Personen vertrauensärztliche Kontrolluntersuchungen vor. Ältere Betroffene wollten wissen, wer Einsicht in diese Daten erhält.

Über 70-jährige Ausweisinhaber müssen sich alle zwei Jahre einer vertrauensärztlichen Kontrolluntersuchung unterziehen.[39] Im Kanton Zug wird diese Untersuchung in aller Regel durch den Hausarzt durchgeführt. Was zu untersuchen ist, gibt der Bund in seinen Formularen[40] vor. Der Hausarzt hat somit diejenigen Untersuchungen vorzunehmen, die es ihm ermöglichen, die Fahrtauglichkeit zu beurteilen. Ist der betroffenen Person nicht klar, warum der Hausarzt eine bestimmte Untersuchung vornimmt, muss dieser um nähere Angaben gebeten werden.

Welche Daten gehen nun an das Strassenverkehrsamt? Der Hausarzt behält die medizinischen Daten der Untersuchung bei sich und äussert sich gegenüber dem Strassenverkehrsamt nur über die Fahrtauglichkeit. Wie dem Formular entnommen werden kann, lautet seine Antwort diesbezüglich somit nur: «ja», «nein» oder «bedingt»[41].

Fazit: Alle medizinischen Daten bleiben beim Hausarzt, das Strassenverkehrsamt erfährt nur, ob die Fahrtauglichkeit gegeben ist oder nicht. Das Arztgeheimnis bleibt gewahrt.

1.7 Justiz

Fall 16 Einsicht in Akten abgeschlossener Strafverfahren

Auf hängige Strafverfahren kommt das Datenschutzgesetz nicht zur Anwendung.[42] Ein Organ der Justiz erkundigte sich, wie die Rechtslage nach rechtskräftigem Abschluss des Verfahrens ist, wenn ein Beteiligter Einsicht in seine Akten verlangt.

Nach Abschluss des Verfahrens ist das Datenschutzgesetz anwendbar, und die dort vorgesehene Auskunft und Einsicht erlaubt dem Betroffenen, Einsicht in seine *eigenen Daten* zu nehmen. Bei gewissen Akten kann sich die Frage stellen, ob es sich dabei um eigene Daten oder aber um solche einer *anderen Person* handelt. Sofern diese Person der Einsicht nicht zustimmt, müssten diese Daten geschwärzt werden.

Fall 17 Botschaft: Wie viele unserer Staatsangehörigen sind im Gefängnis?

Die Botschaft eines europäischen Staates wollte wissen, wie viele Personen mit der entsprechenden Nationalität sich zurzeit in Zuger Gefängnissen aufhielten. Die zuständige Direktion verweigerte diese Auskunft. Die Botschaft wandte sich anschliessend an den Datenschutzbeauftragten. Wir kamen zum Schluss, dass die Bekanntgabe nur der Zahl – ohne irgendwelche weiteren Angaben – allfälliger Personen mit der entsprechenden Staatsangehörigkeit in Zuger Gefängnissen aus datenschutzrechtlicher Sicht mitgeteilt werden kann. Denn im vorliegenden Fall war keinerlei Bezug zu einzelnen Personen möglich;[43] es handelte sich somit um eine rein statistische Angabe. Diese unterliegt nicht dem Datenschutzrecht. Unter speziellen Umständen können die Daten dem Amtsgeheimnis unterliegen, was die zuständige Direktion zu beurteilen hatte.

39 Art. 27 Abs. 1 Bst. b Verordnung über die Zulassung von Personen und Fahrzeugen zum Strassenverkehr [Verkehrszulassungsverordnung, VZV; SR 741.51].

40 Anhang 3 zur VZV [«www.admin.ch/ch/d/sr/741_51/app3.html»].

41 Zu den medizinisch bedingten Auflagen gehört etwa die Pflicht, Kontaktlinsen oder eine Brille zu tragen.

42 § 3 Abs. 2 Bst. a Datenschutzgesetz.

43 Unter gewissen Umständen kann allenfalls ein Bezug zu einer bestimmten Person gemacht werden: Wenn es sich um eine prominente Person mit einer Staatsangehörigkeit handelt, die sonst nicht in Zuger Gefängnissen vertreten ist. Diesfalls wäre die Auskunft nicht zu erteilen.

1.8 Gemeinde

Fall 18 Stimmregister – copy/paste?
Eine politische Partei möchte von der Einwohnergemeinde die Adressen sämtlicher Stimmberechtigten in elektronischer Form für einen einmaligen Briefversand im Zusammenhang mit den Wahlen 2010. Die Gemeinde erkundigt sich beim Datenschutzbeauftragten, ob sie diese – tausende – Adressen herausgeben darf.

Das Wahl- und Abstimmungsgesetz sieht vor «Das Stimmregister steht den Stimmberechtigten zur Einsicht offen»[44] und die Verordnung dazu: «Parteien und andere politische Gruppierungen erhalten auf Gesuch hin Auszüge aus dem Stimmregister»[45]. Was bedeuten diese beiden Bestimmungen für unsere Fragestellung?

Die Bestimmung des Gesetzes
Sinn und Zweck dieser Bestimmung liegen darin, dass die Stimmberechtigten vor Ort überprüfen können, ob sie selber im Stimmregister eingetragen sind, und zudem, ob bestimmte andere Personen eingetragen oder nicht eingetragen sind. Die Bestimmung kann wohl nur historisch erklärt werden, da früher Register allenfalls nicht derart akkurat geführt wurden wie heute, zudem den Betroffenen früher keine allgemeine Einsicht in ihre eigenen Daten gewährt wurde. Diese Bestimmung könnte heutzutage wohl gestrichen werden. Dass Bürger überprüfen können, ob die Verwaltung *andere Bürger* korrekt erfasst hat, ist – soweit ersichtlich – völlig einzigartig. Man stelle sich die analoge Situation etwa bei der Steuerverwaltung oder der Polizei vor …

Die Bestimmung dient somit einzig der Kontrolle des Registers durch die Stimmberechtigten der jeweiligen Gemeinde. Eine andere Funktion ist nicht ersichtlich. Insbesondere kann es hier nicht darum gehen, das Stimmregister als Quelle für den Bezug von Daten über die Stimmberechtigten zu erhalten [etwa: Adressen, Geburtsdaten, Konfession etc.]. Wer Einsicht in das Stimmregister nimmt, erhält deshalb keine Auszüge und darf auch keine Abschriften von Daten anderer Stimmberechtigter machen. Auf Verlangen erhält man nur eine Kopie des eigenen Eintrages. Dieses Recht ergibt sich aber bereits aufgrund des Datenschutzgesetzes.

Die Bestimmung der Verordnung
Das Gesetz regelt die Einsicht abschliessend. Im Gesetz sind *keine Auszüge* vorgesehen. Die Verordnung geht daher über den Regelungsbereich des Gesetzes hinaus, wenn sie Auszüge zulässt. Sie ist daher diesbezüglich *nicht rechtmässig* und § 6 darf daher nicht angewendet werden. Zu diesem Schluss bezüglich § 6 ist der Datenschutzbeauftragte übrigens bereits in seiner Stellungnahme zum Entwurf dieser Verordnung im Jahr 2007 gekommen, was der Regierungsrat jedoch nicht berücksichtigt hat.

Zwischenergebnis: Aufgrund der Vorschriften des Wahlrechts kann die Datenbekanntgabe unseres Erachtens *nicht bewilligt* werden.

Handelt es sich um eine «Sammelauskunft»?
Das Datenschutzgesetz[46] sieht vor, dass Private von der Gemeinde über die EinwohnerInnen die folgenden Daten erhalten, sofern die Daten für einen schützenswerten ideellen Zweck verwendet werden: Name, Vorname, Geschlecht, Geburtsdatum, aktuelle Adresse und die in einem bestimmten Zeitraum Zugezogenen.

Die Aufzählung der Daten, die bekannt gegeben werden dürfen, ist *abschliessend*. Obwohl die Gemeinde noch über sehr viele weitere Angaben zu den EinwohnerInnen verfügt, darf sie diese somit *nicht* bekannt geben. Im Rahmen einer Sammelauskunft dürfen daher etwa Zivilstand, Staatsangehörigkeit, Kinderzahl, Konfession, Haushaltsgrösse etc. *nicht* bekannt gegeben werden. Auch die Frage, ob jemand in der Gemeinde stimm- und wahlberechtigt ist, kann somit *nicht* Gegenstand einer Sammelauskunft sein.

Fazit: Im Rahmen einer Sammelauskunft kann die Partei somit nicht [nur] die Adressen aller Stimmberechtigten erhalten. Hingegen kann sie die Adressen sämtlicher Einwohnerinnen und Einwohner der Gemeinde gestützt auf das Datenschutzgesetz erhalten.

44 § 4 Abs. 5 Gesetz über die Wahlen und Abstimmungen [WAG, BGS 131.1].

45 § 6 Abs. 1 Verordnung zum Wahl- und Abstimmungsgesetz [WAV, BGS 131.21].

46 § 8 Abs. 2 Bst. c Datenschutzgesetz.

Ergänzend ist auf die geltenden Rahmenbedingungen hinzuweisen: Haben Einwohner ihre Daten gesperrt, dürfen sie im Rahmen einer Sammelauskunft nicht bekannt gegeben werden. Der Anfragende hat sich schriftlich zu verpflichten, dass die Daten nur einmal für den angegebenen Zweck genutzt werden und nicht an Dritte weitergegeben werden. Da es um die Daten der gesamten Wohnbevölkerung geht, somit um Abertausende von Adressen, hat die Gemeinde die erforderlichen Kontrollmassnahmen vorzusehen. Üblicherweise werden den Adressen ein paar Kontrolladressen beigegeben, die es der Gemeinde erlauben, zu überprüfen, ob die Adressen nicht weitergegeben oder mehrfach genutzt werden.

Fall 19 Wenn die Gemeinde Bürgeranfragen per E-Mail erhält …

Mehrere Personen haben sich beim Datenschutzbeauftragten beschwert, weil E-Mails von ihnen, die sie an eine ganz bestimmte Person in der Gemeinde gerichtet haben, an viele weitere Stellen in der Gemeinde weitergeleitet wurden. Was ist hier zu beachten?

Es ist vorweg auf das Amtsgeheimnis hinzuweisen.[47] Dieses sieht vor, dass es den Mitarbeitenden untersagt ist, Drittpersonen oder *anderen Amtsstellen* Tatsachen mitzuteilen, die sie bei der Ausübung ihres Amtes erfahren und an denen ein öffentliches Geheimhaltungsinteresse oder ein Persönlichkeitsschutzinteresse besteht oder die gemäss besonderer Vorschrift geheim zu halten sind. Immer wieder wird von der Verwaltung übersehen, dass das Amtsgeheimnis auch zwischen den verschiedenen Stellen innerhalb der Gemeinde gilt. Die Verwaltung ist somit nicht eine einzige grosse Familie, die untereinander alle Daten austauschen darf. Vielmehr gilt: Die Daten bleiben grundsätzlich bei der Stelle, die sie für ihre Aufgabenerfüllung benötigt. Dass eine Verletzung des Amtsgeheimnis strafbar ist, ist bekannt.[48]

Wenn eine Privatperson ein Anliegen per E-Mail bei einer bestimmten Verwaltungsstelle vorbringt, die nicht oder nur teilweise zuständig und die sich allenfalls bei einer anderen Stelle informieren muss, so ist die E-Mail der Privatperson – falls überhaupt – nur *anonymisiert* weiterzuleiten. Es ist nicht erforderlich, dass jedermann in der Gemeinde weiss, wer warum wann welches Anliegen vorgebracht hat. Erst recht nicht, wenn die E-Mail Vertrauliches enthält, Kritik vorbringt oder einen unerfreulichen Inhalt hat.

Die angeschriebene Verwaltungsstelle kann den Anfragenden – ohne dass weitere Stellen im «cc» aufgeführt sind – auch direkt darüber informieren, wer für sein Anliegen zuständig ist.

Anders ist die Rechtslage nur dann, wenn der Anfragende ausdrücklich wünscht, dass seine E-Mail an andere Stellen weitergeleitet wird.

Diese Hinweise beziehen sich nicht nur auf Bürgeranliegen, die per E-Mail bei der Verwaltung eingehen, sondern vielmehr auch auf telefonische oder briefliche Eingaben. Bei der elektronischen Post stellt sich das Problem jedoch besonders akut, weil mit einem Klick Informationen ohne jeglichen Aufwand innert Sekunden an x-beliebig viele Stellen weitergeleitet werden können.

47 § 29 Personalgesetz. Dieses ist nicht nur für den Kanton anwendbar, sondern gilt in dieser oder einer ähnlichen Form auch in den meisten Gemeinden.

48 Art. 320 Strafgesetzbuch.

2. Unsere Öffentlichkeitsarbeit

2.1 Website

Unter «www.datenschutz-zug.ch» finden Sie viele wichtige Informationen und weiterführende Links zu Datenschutz und Datensicherheit in Zug, der Schweiz und Europa. Der Inhalt wird etwa alle zwei Wochen überprüft und allenfalls aktualisiert.

Wie wird unser Web-Angebot genutzt?
Durchschnittlich besuchen täglich 50 bis 110 einzelne Personen aus der Schweiz die DSB-Website während 3 bis 8 Minuten. Im Vergleich zum letzten Jahr hat die Nutzung erfreulicherweise *weiter zugenommen* – insgesamt um rund 20 %.[49]

Viele wichtige Dokumente stehen auf der DSB-Website zur Verfügung. Die zehn meistverlangten Dokumente wurden im Berichtsjahr zwischen 350 und 1100 Mal heruntergeladen.

Fazit: Unser Internetangebot wird rege genutzt. Nicht unbedeutend ist insbesondere das Herunterladen unserer Publikationen. Informiert sich die Öffentlichkeit im Internet, reduziert sich in aller Regel für den DSB der Beratungsaufwand.

2.2 Newsletter

Unser Konzept des Internet-Auftritts hat sich bewährt: Die *grundlegenden* Informationen werden auf der Website veröffentlicht.[50] *Aktuelles* aus den Bereichen Datenschutz und Datensicherheit wird hingegen *per E-Mail* in Form von Kurzhinweisen – versehen mit Links auf Fundstellen, wo sich ausführliche Informationen finden – verschickt.[51] Diese Dienstleistung kann auf einfachste Weise in Anspruch genommen werden: Es genügt, wenn man auf der entsprechenden Seite der DSB-Website[52] seine eigene E-Mail-Adresse bekannt gibt. Wer übrigens keine Nachrichten mehr erhalten möchte, kann sich ebenso einfach selber wieder aus der Versandliste austragen.

Hier das Wichtigste in Kürze:

Häufigkeit des Nachrichtenversandes
Monatlich werden per E-Mail 2 bis 4 Kurznachrichten verschickt.

Archiv der verschickten Nachrichten
Sämtliche verschickten Nachrichten sind in einer Archiv-Datenbank gespeichert [z. T. mit zusätzlichen Dokumenten versehen]. Diese Datenbank ist via Website auch für nicht eingeschriebene Personen zugänglich. Das Archiv verfügt über eine effiziente Suchmaschine.
Ende 2010 befanden sich insgesamt 875 Nachrichten im Archiv.

Besucherstatistik 2010
Pro Monat besuchen zwischen 300 und 600 Personen das Archiv. Das entspricht einer leichten Zunahme im Vergleich zum Vorjahr. Dabei werden pro Monat zwischen 50 und 190 PDF-Dokumente heruntergeladen. Die Statistik zeigt klar, dass die einzelnen Nachrichten gelesen und in der Folge die in der Nachricht gemeldeten Dokumente im Archiv oft auch gleich heruntergeladen werden.

Zuwachs der Abonnenten 2010
+ 72 Neuabonnierte!

Verschickte Nachrichten 2010
30 per E-Mail verschickte Nachrichten

Abo-Kosten
keine

Fazit
Schreiben auch Sie sich ein – es lohnt sich!

2.3 Tätigkeitsbericht 2009

Mit dem Tätigkeitsbericht sollen die Themen Datenschutz und Datensicherheit einem *breiten Publikum* vorgestellt werden. Im Zentrum steht dabei die Präsentation von konkreten Fällen aus unserer Beratungspraxis des Berichtsjahrs. Dabei versuchen wir, die Fälle möglichst kurz, verständlich und praxisnah zu präsentieren.

Neben der Öffentlichkeit sollen aber insbesondere auch die Mitarbeitenden der Verwaltung

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

50 Insbesondere Gesetze, Literatur, Adressen und Links.

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

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

bezüglich Datenschutz und Datensicherheit sensibilisiert und ein stückweit ausgebildet werden. Sehr erfreulich ist, dass die meisten Zuger Gemeinden unser kostenloses Angebot nutzen, und unseren Tätigkeitsbericht jeweils für einen Teil – einige auch für alle – ihrer Verwaltungsmitarbeitenden bestellen. Eine kostengünstigere und effizientere Sensibilisierungsmassnahme gibt es vermutlich nicht.

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

Ein Hinweis zur Print-Ausgabe: Es hat sich erneut klar gezeigt, dass sehr viele Personen den gedruckten Tätigkeitsbericht für ihre Arbeit benützen und diesen dafür als geeigneter und ansprechender erachten als das Herunterladen des Berichts aus dem Internet. Wer die Papierversion dem PDF vorzieht, handelt insgesamt übrigens ökologischer, wenn er das PDF nicht auf seinem Drucker ausdruckt, sondern die in hoher Auflage auf umweltfreundlichem Papier mit optimierter Technik gedruckte Ausgabe bei uns bestellt.

Die beiden Angebote ergänzen sich und stellen – je nach Zielgruppe – beide eine nützliche Arbeitshilfe dar.

Wer die letztjährigen Tätigkeitsberichte zu Rate ziehen möchte, kann sie beim DSB kostenlos bestellen oder sie auf der DSB-Website[53] als PDF beziehen.

2.4 «Gerichts- und Verwaltungspraxis des Kantons Zug»

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

Der DSB publiziert in der GVP wichtige Stellungnahmen aus seiner Beratungspraxis. In GVP 2009[54] veröffentlichte er die folgenden sieben Fälle:

- Zur Einsicht eines Betroffenen in die eigenen Daten im Polizei-Journal
- Rechtsfolgen unzulässiger Datenbekanntgabe durch Verwaltungsmitarbeitende
- Lässt das geltende Recht verdeckte Überwachung von Sozialhilfebezügern zu?
- Pandemievorbereitungen: Dürfen Verwaltungsmitarbeitende Daten bei sich zu Hause bearbeiten?
- Datenerhebung zur Wohnsituation der Bevölkerung
- Einbürgerung: Worüber ist die Bürgergemeindeversammlung zu informieren?
- Zur Rechtslage bezüglich Videoüberwachung des öffentlichen Raums

Die Beiträge des DSB in der GVP der Jahre 2000 – 2009 können layoutgetreu und kostenlos von der DSB-Website[55] heruntergeladen werden.

2.5 «Schulinfo Zug»

Die Direktion für Bildung und Kultur informiert Lehrpersonen aller Stufen, Schulbehörden und weitere interessierte Stellen und Personen über alles Aktuelle aus der Schule mit der Publikation «Schulinfo Zug». Dieses sehr nützliche und sehr attraktive Schulmagazin erscheint dreimal pro Jahr in einer Auflage von 3400 Exemplaren.

Da wir sehr viele Anfragen aus dem Schulbereich erhalten, stellen die Herausgeber dem Datenschutzbeauftragten freundlicherweise jeweils pro Ausgabe eine Seite zur Verfügung, um die Leserschaft kurz über Aktuelles aus dem Bereich Datenschutz und Schule zu informieren. In diesem Jahr hat der DSB die folgenden drei Beiträge verfasst: «Cyber-Mobbing in der Schule»,[56] «Daten über Lehrpersonen und Schülerschaft»[57] und «Sprechen – aber mit wem worüber?».[58]

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

54 GVP 2009 S. 370 – 390.

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

56 Schulinfo Zug 2009-10/Nr. 3 S. 51.

57 Schulinfo Zug 2010-11/Nr. 1 S. 42 [betr. das Statistikprojekt «Modernisierung der Erhebungen im Bildungsbereich/MEB» des Bundesamtes für Statistik].

58 Schulinfo Zug 2010-11/Nr. 2 S. 51.

Erfreulicherweise erhalten wir aus der Leserschaft regelmässig Rückmeldungen oder Fragen zu unserer Kolumne, was zeigt, dass «Schulinfo Zug» gelesen wird.

Die Beiträge des DSB in der «Schulinfo Zug» der Jahre 2004 – 2010 können layoutgetreu von der DSB-Website heruntergeladen werden.

2.6 «Personalziitig»

Die Personalzeitung der Zuger Verwaltung heisst «Personalziitig», erscheint viermal pro Jahr in einer Auflage von 2750 Exemplaren und wird allen aktiven und pensionierten Mitarbeitenden der Zuger Verwaltung sowie weiteren Kreisen kostenlos zugestellt.

Der Regierungsrat hat im Jahr 2008 erfreulicherweise beschlossen, dass der Datenschutzbeauftragte zwei bis drei Beiträge pro Jahr für die «Personalziitig» verfassen soll, um die Mitarbeitenden auf diesem Weg für die Themen Datenschutz und Datensicherheit zu sensibilisieren.

Im Berichtsjahr veröffentlichte die «Personalziitig» ein zweiseitiges Interview mit dem Datenschutzbeauftragten zur aktuellen Lage bezüglich Datenschutz und Datensicherheit.[59] In einem weiteren Beitrag[60] konnte der DSB zudem den Verwaltungsmitarbeitenden ein paar Fälle aus der Praxis vorstellen, die einen ganz direkten Bezug zu ihrer Arbeit haben: Wer sieht eigentlich in Ihr Personaldossier? Was sieht der Pöstler beim Versand Ihres Lohnausweises? Was müssen Sie bedenken, wenn Sie zu Hause arbeiten? Was müssen Sie beim Versenden von E-Mails beachten? Wie schützen Sie die Privatsphäre der Kunden am Schalter?

2.7 In der Zeitung – Kolumne «Ratgeber Datenschutz»

Für die Zuger Presse betreute der Datenschutzbeauftragte im Berichtsjahr die Kolumne «Ratgeber Datenschutz». Er verfasste die folgenden sechs Beiträge:
- Datenklau – bald überall?
- 1507 Datensammlungen in Zug
- Dürfen Mitarbeitende der Verwaltung eigentlich zu Hause arbeiten?
- Fichenaffäre 2010: Mehr als 200 000 Fichierte!
- Ihr Verein und Ihre Daten
- Umfrage zum Datenschutz in Deutschland

Dies ist eine gute Plattform, um eine breitere Öffentlichkeit für Datenschutz und Datensicherheit zu sensibilisieren und gleichzeitig der Leserschaft auch nützliche Tipps für den Umgang mit ihren eigenen Daten zu geben.

2.8 Zuger Datenschutz in den Medien

Aufgrund unserer Medienmitteilungen berichteten die Zuger Printmedien und Lokalradios verschiedentlich über Datenschutz oder die Datenschutzstelle. Im Zentrum stand die Veröffentlichung unseres Tätigkeitsberichts. Aber auch im Zusammenhang mit Gesetzgebung, Politik oder weiteren datenschutzrechtlichen Aktualitäten – beispielsweise zur Videoüberwachung – erhielten wir Anfragen von Medien.

Die Frage der Veröffentlichung von Grundbuchdaten im Internet interessierte nicht nur die Zeitungen, sondern führte auch zu einem Interview mit dem Datenschutzbeauftragten im Rahmen der Radiosendung «Espresso» bei DRS 1.[61]

Verschiedene deutsche Medien nahmen die Veröffentlichung unseres Tätigkeitsberichts zum Anlass, über den Zuger Datenschutz zu berichten.[62]

59 Personalziitig Nr. 52/2010 S. 24 f.

60 Personalziitig Nr. 52/2010 S. 26 f.

61 DRS 1, «Espresso» vom 29. Oktober 2010: «Internet: Das Eigenheim wird zum Glashaus».

62 Datenschutz und Datensicherheit/DuD 2010/7 S. 502 f. und Medienmitteilung des «Virtuellen Datenschutzbüros» vom 22. April 2010.

3. Mitarbeit bei der Gesetzgebung

Der Datenschutzbeauftragte ist von Gesetzes wegen ausdrücklich verpflichtet, bei der Gesetzgebung Input zu geben.[63] Dies zu recht. Werden neue Rechtserlasse geschaffen, werden grundlegende und weitreichende Weichenstellungen für die Zukunft getroffen. Dabei muss der verfassungsmässige Schutz der Privatsphäre der Bürgerinnen und Bürger beachtet werden. Die Mitarbeit bei der Gesetzgebung ist für den Datenschutzbeauftragten daher von *grosser* Bedeutung.

Die Verwaltung ihrerseits ist verpflichtet, den DSB über geplante Rechtsetzungserlasse *unaufgefordert, frühzeitig und vollständig* zu informieren. Dabei bedeutet «frühzeitig» – sobald ein Projekt in Angriff genommen wird. Das ist wichtig, weil dann noch Varianten, Alternativen und Verbesserungen gesucht und implementiert werden können.

Der Einbezug des DSB bei der Gesetzgebung ist weitgehend eine Selbstverständlichkeit. Übersieht eine vorbereitende Stelle ausnahmsweise die Datenschutzrelevanz eines Gesetzesprojektes, was im Berichtsjahr vorgekommen ist, schreitet erfahrungsgemäss spätestens der Regierungsrat entsprechend ein.

3.1 Vernehmlassungen

Falls Sie sich für eine der folgenden Stellungnahmen des Datenschutzbeauftragten interessieren – in aller Regel können wir sie Ihnen gerne kostenlos zusenden. Eine E-Mail an uns genügt.

Bundesrecht
Der Bund gibt den Kantonen jeweils die Möglichkeit, sich zu den bundesrechtlichen Gesetzgebungsvorhaben zu äussern. Tangiert eine Vorlage Datenschutz/Datensicherheit, so lädt der Regierungsrat den DSB zu einer Stellungnahme ein. Diese übernimmt der Regierungsrat in aller Regel in seiner Vernehmlassungsantwort gegenüber dem Bund. Im Berichtsjahr hat der Datenschutzbeauftragte insbesondere zu den folgenden Vorlagen Stellung genommen:

- Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs [BÜPF]
- Bundesgesetz über Erwerb und Verlust des Schweizer Bürgerrechts [BüG]
- Verordnung betreffend das Grundbuch [GBV]
- Verordnung über die elektronische öffentliche Beurkundung [E VeöB]
- Bundesbeschluss über die Genehmigung und die Umsetzung des Übereinkommens über den Zugang zu Informationen, die Öffentlichkeitsbeteiligung an Entscheidungsverfahren und den Zugang zu Gerichten in Umweltangelegenheiten [Aarhus-Konvention]

Rechtserlasse im Zusammenhang mit Schengen
Die EU entwickelt das Schengen-Recht laufend weiter. Die Schweiz hat die entsprechenden Neuerungen zu übernehmen und umzusetzen. Sind die Kantone in ihrer Gesetzgebungshoheit betroffen, so können auch sie sich – grundsätzlich – zu diesen EU-Vorgaben äussern. Warum die Kantone im Schengen-Bereich tatsächlich aber keine Möglichkeiten zu einer Beeinflussung der Gesetzgebung haben, kann dem letzten Tätigkeitsbericht entnommen werden.[64]

Der DSB nahm zum folgenden Schengen-Projekt Stellung:

- Entwurf eines EJPD-Aussprachepapiers betreffend weiteres Vorgehen i. S. Prüm und PCSC [Inhalt: Vertiefung der internationalen Polizeizusammenarbeit, insbesondere durch den erleichterten Austausch von DNA-Profilen, Fingerabdrücken sowie Fahrzeugdaten und Fahrzeughalterdaten (Prümer Zusammenarbeit mit der EU und Agreement on Cooperation in preventing and combating serious crime/PCSC-Abkommen mit den USA)]

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

- Konkordat über private Sicherheitsdienstleistungen [Konkordatsentwurf vom 29. September 2009]

63 § 19 Abs. 1 Bst. e Datenschutzgesetz.

64 Vgl. dazu ausführlich DSB TB 2009 S. 24/25.

- Interkantonale Vereinbarung über die computergestützte Zusammenarbeit der Kantone bei der Aufklärung von Gewaltdelikten [ViCLAS-Konkordat]
- Änderung des Gesetzes betreffend die Einführung des ZGB [EG ZGB, BGS 211.1; betr. Sachenrecht]
- Gesetz über Geoinformation im Kanton Zug [Geoinformationsgesetz, GeoIG]
- Änderung des Gesetzes betreffend die Einführung des ZGB [EG ZGB, BGS 211.1; betr. Umsetzung des neuen Kindes- und Erwachsenenschutzrechts]
- gesetzliche Regelung der Zentralisierung der Verlustscheinbewirtschaftung
- Integrationsgesetz
- Gesetz über die Organisation und die Verwaltung der Gemeinden [Gemeindegesetz, BGS 171.1]
- Gesetzliche Regelung der Übernahme von Forderungen aus der obligatorischen Krankenpflegeversicherung
- Sozialhilfegesetz [SEG, BGS 861.4]
- Gesetz über die Organisation der Zivil- und Strafrechtspflege [Gerichtsorganisationsgesetz, GOG, BGS 161.1]
- Verordnung zum Einführungsgesetz zum Bundesgesetz über den Bevölkerungsschutz und den Zivilschutz [VO zum EG BZG]
- Verordnung über die Benutzung von elektronischen Geräten und elektronischen Kommunikationsmitteln im Arbeitsverhältnis [BGS 154.28]
- Informatikstrategie und Änderung der Informatikverordnung [ITV, BGS 153.53]
- Reglement über die Nutzung von Telefongeräten in der kantonalen Verwaltung [BGS 154.29]
- Statistikkonzept des Kantons Zug
- Weisung zur Überprüfung der Datensicherheit vom 16. Januar 2007 [betr. Bildschirmsperre]

3.2 Unsere Mitarbeit bei ausgewählten Rechtserlassen

Revision Datenschutzgesetz

Aufgrund der Vorgaben von Schengen sowie des Zusatzprotokolls zum Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[65] müssen die Datenschutzbeauftragten *vollständig unabhängig* organisiert sein. Im Kanton Zug ist dies nach wie vor nicht der Fall.

Der Regierungsrat hat deshalb bereits im Jahr 2009 beschlossen, dass das Datenschutzgesetz zu revidieren und vorzusehen sei, dass der Datenschutzbeauftragte neu durch den Kantonsrat auf eine Amtszeit von vier Jahren zu wählen sei.

Im Berichtsjahr hat die zuständige Sicherheitsdirektion – in enger Zusammenarbeit mit dem Datenschutzbeauftragten – eine Vorlage ausgearbeitet. Aufgrund der parallel dazu laufenden Arbeiten am Polizeigesetz ergaben sich gewisse Verzögerungen, sodass die DSG-Revision dem Regierungsrat im Berichtsjahr noch nicht vorgelegt werden konnte.

Die geplante Revision ist sehr zu begrüssen. Da der Datenschutzbeauftragte eine ganze Reihe von Kontrollaufgaben gegenüber der Verwaltung wahrzunehmen hat, gewährleistet die geltende Rechtslage – Anstellung des DSB durch den Regierungsrat mit einem jederzeit kündbaren Arbeitsvertrag – keine genügende *institutionelle Unabhängigkeit* gegenüber der Verwaltung.

Revision Polizeigesetz

Zwei Schengen-Vorgaben verlangen nach einer Revision des geltenden Zuger Polizeigesetzes[66] bezüglich der Bestimmungen, welche die polizeiliche Datenbearbeitung definieren.[67] Im Zentrum steht die Regelung der Erteilung von Information, Auskunft und Einsicht seitens der Polizei an Betroffene. Daneben ist der Datenaustausch mit Behörden von Schengen-Staaten näher zu regeln.

Die Sicherheitsdirektion arbeitet bei dieser Revision eng mit der Zuger Polizei und dem Datenschutzbeauftragten zusammen. Es ist davon auszugehen, dass die erste Lesung im Regierungsrat – zusammen mit der DSG-Revision – im ersten Quartal 2011 statt finden wird.

Verordnung über das Krebsregister

Der Regierungsrat erachtet es für die Krebsprävention und für die Überprüfung der Wirksamkeit von Behandlungsmassnahmen als

65 Das Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung [SR 0.235.11] ist für die Schweiz am 1. April 2008 in Kraft getreten.

66 Polizeigesetz vom 30. November 2007 [BGS 512.1].

67 Rahmenbeschluss 2006/960/JI über die Vereinfachung des Informationsaustauschs zwischen Strafverfolgungsbehörden und Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.

wichtig, systematisch Krankendaten von Zuger Krebspatienten zentral zu sammeln und auszuwerten. Er entschied deshalb im Vorjahr, neu ein Zuger Krebsregister aufzubauen. Dieses sollte aber nicht auf der grünen Wiese in Zug angelegt werden, sondern vielmehr im Auftrag durch das bereits bestehende Krebsregister des Kantons Zürich[68] betrieben werden.

Für alle Beteiligten war klar, dass diese Materie durch einen speziellen Rechtserlass näher zu regeln war, geht es doch um äusserst heikle Personen- bzw. Krankheitsdaten[69]. Hier muss deshalb allen Beteiligten klar sein, wer diese Daten, wann, wozu, unter welchen Umständen, in welcher Form, wie lange einsehen, nutzen und weitergeben darf.

Nachdem geklärt war, dass weder Patientinnen noch Ärzte, Spitäler oder Labors gezwungen werden sollten, dem Krebsregister Krankendaten zur Verfügung zu stellen, sondern grundsätzlich alles auf Freiwilligkeit beruhen sollte, erschien dem DSB die Regelung in einer Verordnung – anstatt in einem formellen Gesetz – plausibel.

Die federführende Gesundheitsdirektion ermöglichte es dem DSB verschiedentlich, Hinweise zum Entwurf der Verordnung über das Krebsregister zu geben. Zu dieser Verordnung, wie sie der Regierungsrat am 14. Dezember 2010 verabschiedete, kann Folgendes festgehalten werden:

Positiv ist zu vermerken:
- Die Bekanntgabe der Daten beruht auf Freiwilligkeit seitens der Krebspatienten [sowie auch der Ärzte, Spitäler etc.].
- Die Krebspatienten können jederzeit verlangen, dass ihre Daten nicht beziehungsweise nicht mehr dem Krebsregister zugestellt werden.

Kritisch zu beurteilen:
- Es ist nicht vorgesehen, dass die Krebspatienten der Bekanntgabe ihrer Daten aktiv und unterschriftlich – und somit beweisbar – zustimmen müssen. Es ist bloss vorgesehen, dass sie durch die Arztperson informiert werden sollen und der Datenbekanntgabe dann nicht widersprechen.

Gemäss Hinweisen des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten funktioniert dieses Vorgehen in der Praxis jedoch nicht. Insbesondere kommen offenbar die Ärzte, Spitäler und Labors ihrer Informationspflicht nicht oder nicht korrekt nach, werden doch Patienten weder umfassend noch objektiv über diese sehr weitreichende Datenbekanntgabe informiert.

Da die Verordnung keine unterschriftliche Zustimmung verlangt, sind keinerlei Beweise vorhanden, ob die Patientin tatsächlich informiert wurde und der Datenbekanntgabe nicht widersprochen hat. Werden Patientendaten weitergegeben, ohne dass die Patienten informiert werden [dann erst können sie ja von ihrem Vetorecht Gebrauch machen], machen sich Arzt- oder Spitalpersonen allenfalls strafbar.[70]

- Es ist geplant, dass das Krebsregister Zürich einen Online-Zugriff auf die Daten der Zuger Einwohnerkontrollen aller elf Gemeinden erhalten soll, um die aktuelle Adresse der gemeldeten Zuger Krebspatienten à jour halten zu können. Das Krebsregister wird gestützt auf die Online-Verordnung ein Gesuch zu stellen haben. Dazu werden wir eine Stellungnahme abgeben, wobei wir zu prüfen haben, ob es allenfalls nicht eine weniger weit gehende Lösung gibt.

68 Näheres dazu unter «www.krebsregister.usz.ch».

69 Folgende Daten werden gemäss § 9 der Verordnung über das Krebsregister [BGS 821.13] von jeder Person erfasst: Personendaten: Name und Vorname; Geburtsdatum; Geschlecht; Staatsangehörigkeit bei Geburt; Wohnadresse; BFS-Gemeindenummer; Beruf; Zivilstand; Vitalstatus. Medizinische Daten: Datum der Diagnose; Grundlage der Diagnose; Anlass der Konsultation, die zur Diagnose führte; Lokalisation, Histologie, Dignität und Grading des Tumors; Tumorstadium bei Diagnose; Art der Erstbehandlungen während der ersten sechs Monate nach Diagnosestellung.

70 Verletzung des Berufsgeheimnisses nach Art. 321 Strafgesetzbuch.

4. Register der Datensammlungen

Was ist das Register der Datensammlungen?
Die Behörden dürfen in einem Rechtsstaat nicht im Geheimen Daten über Bürgerinnen und Bürger sammeln und bearbeiten. Die staatlichen Datenbearbeitungen müssen gegenüber den Betroffenen und der Öffentlichkeit vielmehr *transparent* sein. Für die Verwaltung gilt beim Datensammeln somit das Motto «Zeigt her eure Schuh!».

Das Zuger Datenschutzgesetz sieht denn auch vor, dass jedermann das Recht hat, grundsätzlich jederzeit und umfassend Einsicht in alle *seine eigenen* Daten nehmen zu können.[71] Woher weiss der Interessierte nun aber, welche Stelle Daten über ihn hat?

Die Daten über die Zugerinnen und Zuger werden nicht zentral bei einer einzigen Stelle geführt. Vielmehr führt die jeweilige Verwaltungsstelle der Gemeinde oder des Kantons ihre Daten *dezentral*. Will eine Einwohnerin wissen, welche Daten die Verwaltung über sie hat, muss sie sich deshalb an diejenige Stelle wenden, deren Datenführung sie interessiert [z.B. gemeindliche Schule, Einwohnerkontrolle, Polizei, Steuerverwaltung etc.]. Wie erfährt man nun aber, welche Verwaltungsstelle welche Daten bearbeitet und in welcher Datensammlung sie diese führt?

Dafür gibt es ein Verzeichnis – das Register der Datensammlungen aller Zuger Amtsstellen. Dieses führt der Datenschutzbeauftragte. Damit dieses Verzeichnis auch vollständig ist, sind sämtliche Verwaltungsstellen von Kanton und Gemeinden verpflichtet, ihre Datensammlungen dem DSB zu melden.[72] Durch dieses Register wird gegenüber der Öffentlichkeit Transparenz geschaffen, und jedermann kann sich ein Bild machen, welche Daten bei welcher Verwaltungsstelle bearbeitet werden.

Dieses Verzeichnis ist somit die zwingend erforderliche Grundlage für die Ausübung des Einsichtsrechts. Das Register selber enthält übrigens *keinerlei* Personendaten. Ersichtlich ist nur, unter welcher Bezeichnung eine Verwaltungsstelle eine Datensammlung führt und welche Art von Daten dort in welcher Form gesammelt wird.

Das Register dient aber auch der Verwaltung selber. Die einzelnen Verwaltungsstellen von Kanton und Gemeinden erhalten einen Überblick über die bei ihnen vorhandenen Daten und über die Datenflüsse zwischen den Verwaltungsstellen.

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

Wer führt das Register?
Für die Führung des Registers der *kantonalen Verwaltung* ist der Datenschutzbeauftragte zuständig. Die *Gemeinden* haben ihr Register an und für sich selber zu führen.[73] Um die Einheitlichkeit des Registers zu gewährleisten, war der DSB bereits bei Projektbeginn im Jahr 2000 bereit, auch die Datensammlungen der Gemeinden[74] zu betreuen.

1496 Zuger Datensammlungen!
Das Register umfasste Ende 2010 insgesamt 1496 Zuger Datensammlungen [Abnahme aufgrund der Zusammenführung verschiedener Datensammlungen] im Vergleich zum Vorjahr: -11]:
- kantonale Verwaltung: 310 [-10]
- externe Beauftragte: 22 [-1]
- Einwohnergemeinden: 897 [keine Änderung]
- Bürgergemeinden: 112 [keine Änderung]
- römisch-katholische Kirchgemeinden: 92 [keine Änderung]
- evangelisch-reformierte Kirchgemeinde: 12 [keine Änderung]
- Korporationsgemeinden: 51 [keine Änderung].

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

71 § 13 und § 14 Datenschutzgesetz.

72 § 12 und § 26 Abs. 1 Datenschutzgesetz. Davon ausgenommen sind gemäss § 12 Abs. 2 Datenschutzgesetz die Hilfsdatensammlungen und Datensammlungen, die nur bis maximal sechs Monate geführt werden. Ebenfalls nicht in das Register aufgenommen werden Datensammlungen, die keine Personendaten, sondern ausschliesslich Sachdaten beinhalten.

73 § 12 Abs. 5 Datenschutzgesetz.

74 Einwohnergemeinden, Bürgergemeinden, Kirchgemeinden sowie Korporationsgemeinden.

5. Unsere Weiterbildungsangebote

Sensibilisierung, Sensibilisierung, Sensibilisierung ...

Gesetze, Reglemente und Weisungen sind das Eine, die korrekte Umsetzung durch die Mitarbeitenden in der Praxis das Andere. Wenn Mitarbeitende nicht oder nicht genau wissen, was bezüglich der Datenbearbeitung zu tun ist oder in der Eile etwas Wichtiges übersehen – schnell können gravierende Fehler mit grossen Schäden passieren.

Ein Teil der Verantwortung wird den Mitarbeitenden durch Organisation oder Technik abgenommen: auf Daten, die sie nichts angehen, haben sie gar keinen Zugriff, Notebooks werden ohne ihr Zutun wirksam vor unberechtigtem Zugriff geschützt oder Konfigurationsänderungen an Geräten können nur durch Administratoren vorgenommen werden.

Sehr vieles bleibt aber in der Verantwortung jedes Mitarbeitenden, so insbesondere die Frage: An welche Verwaltungsstelle dürfen welche Daten in welcher Form weitergegeben werden? Schulung, Weiterbildung und insbesondere Sensibilisierung bleibt deshalb eine der Hauptaufgaben des Datenschutzbeauftragten.

Sensibilisierung 1:
Die neuen Kantonsmitarbeitenden

Alle neuen Mitarbeitenden der kantonalen Verwaltung müssen obligatorisch an einem «Einführungstag», der durch das Personalamt organisiert wird, teilnehmen. Dabei werden sie über wichtige Aspekte und Anliegen der Zuger Verwaltung informiert.

Da die Verwaltung heute grundsätzlich nichts anderes macht, als «Daten zu bearbeiten», ist es wichtig, dass die neuen Mitarbeitenden über die zentralen Grundsätze von Datenschutz und Datensicherheit informiert werden. Dafür stellt das Personalamt dem DSB eine halbe Stunde zur Verfügung. Hier kann es somit nicht um eine vertiefte Ausbildung gehen. Das Ziel dieser Veranstaltung ist deshalb erreicht, wenn die neuen Mitarbeitenden wissen, dass es eine Datenschutzstelle gibt, die sie bei Fragen gerne unterstützt. Kennen die neuen Mitarbeitenden zudem noch die wichtigsten Grundsätze, ist bereits viel erreicht.

Im Berichtsjahr fanden zwei solche Ausbildungstage statt. So konnten insgesamt gegen 100 neue Mitarbeitende mit dem Datenschutz bekannt gemacht werden.

Sensibilisierung 2:
Die angehenden Lehrpersonen

Lehrpersonen für Datenschutz und Datensicherheit zu sensibilisieren ist aus zwei Gründen sehr wichtig: Erstens verfügen Lehrpersonen über viele, teilweise sehr heikle Daten über die Schülerinnen und Schüler, deren Umfeld und deren Elternhaus. Zweitens können sie bei der Lehrtätigkeit ihre Schülerinnen und Schüler im Umgang mit Daten sensibilisieren, ein Thema, das in den Zeiten von Facebook immer wichtiger wird. Im Berichtsjahr hat der DSB an der Pädagogischen Hochschule Zug gegen 90 Studienabgängerinnen und Studienabgänger im Rahmen von zwei Lektionen auf das Wichtigste im Datenschutz an der Schule hinweisen können – eine sehr wertvolle Informationsveranstaltung!

Sensibilisierung 3:
Präsentationen des DSB

Regelmässig laden Verwaltungsstellen von Kanton und Gemeinden und auch private Institutionen den Datenschutzbeauftragten zu Referaten oder Präsentationen ein, um ihre Mitarbeitenden über Datenschutz oder Datensicherheit zu informieren. Im Berichtsjahr ergab sich etwa die Gelegenheit, Studierende im Gesundheitsbereich am Gewerblich-Industriellen Bildungszentrum Zug [GIBZ] über die wichtigsten Punkte des Datenschutzes im Gesundheitswesen zu informieren, zudem hielt der DSB ein Referat mit Diskussion bei den Leiterinnen und Leitern der Zuger Gemeindebibliotheken und anlässlich von verschiedenen Veranstaltungen und Besprechungen bestand die Möglichkeit, Hinweise auf wichtige Aspekte des Datenschutzes und der Datensicherheit zu geben.

6. Zusammenarbeit der Datenschutzbeauftragten

«privatim»
Die Datenschutzbehörden aller 26 Kantone[75] sind im Verein «privatim – Die schweizerischen Datenschutzbeauftragten» zusammengeschlossen.[76] Gemeinsam, somit effizienter und effektiver sollen Themen und Projekte bearbeitet werden. Ein grosser Teil dieser Arbeit wird von Arbeitsgruppen geleistet.[77]

Konferenzen von «privatim»
Die Frühjahrestagung fand am 5./6. Mai 2010 in Basel statt. Eines der zentralen Themen war die Festlegung der Strategie von «privatim» für den Zeitraum 2011-2014. Daneben informierten Vertreter des Bundesamtes für Statistik über die Registerharmonisierung und die Volkszählung 2010.

An der Herbstkonferenz vom 11. November 2010 in Bern referierte Prof. Astrid Epiney/Universität Freiburg über «Neue europarechtliche Entwicklungen und die Auswirkungen auf das Datenschutzrecht in der Schweiz». Im Sinne einer Weiterbildungsveranstaltung wurde am Nachmittag das Thema «Vorabkontrolle – best practices» präsentiert und diskutiert.

Zusammenarbeit mit dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten
Seit Anfang 2006 ist der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte [EDÖB] nicht mehr Mitglied des Zusammenschlusses der schweizerischen Datenschutzstellen. Die Zusammenarbeit zwischen dem EDÖB und den kantonalen DSB ergibt sich seit damals aber fall- und anlassbezogen.

Das Bundesrecht sieht im Bereich Schengen ausdrücklich vor,[78] dass der EDÖB und die kantonalen DSB bezüglich der Aufsicht über die Datenbearbeitung bei der Polizei «aktiv» zusammenarbeiten. Dafür wurde im Jahr 2009 die «Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Umsetzung des Schengen Assoziierungsabkommens» [SDSB] gegründet. Diese Zusammenarbeit mit dem EDÖB ist wichtig, da dieser über Know-how, Erfahrung und Ressourcen bezüglich Kontrollen im Rahmen von Schengen verfügt und er aufgrund der Schengen-Vorgaben auch regelmässig solche Kontrollen bei Bundesstellen im In- und Ausland durchführt. Da die kantonalen Datenschutzbeauftragten analoge Kontrollen bei den kantonalen Polizeiorganen machen müssen, ist die Unterstützung seitens des EDÖB auf diesem Gebiet wertvoll.

Im Berichtsjahr fand eine Sitzung der Arbeitsgruppe SDSB am 16. September in Bern statt. Dabei referierte der DSB über die bei der Zuger Polizei durchgeführte SIS-Kontrolle.[79]

Internationale Zusammenarbeit

Ausgangslage
Das Schengen-Recht sieht eine stärkere Zusammenarbeit der Datenschutzbehörden auf europäischer Ebene vor. Diese Vorgabe der EU – wonach der Zuger DSB auch mit den Datenschutzbehörden des Auslandes kooperieren kann – wurde im Jahre 2008 in das Zuger Datenschutzgesetz eingefügt.[80]

«Virtuelles Datenschutzbüro»
Der Zuger Datenschutzbeauftragte ist seit 2008 Projektpartner des «Virtuellen Datenschutzbüros». Dieses betreibt im deutschsprachigen Raum eine Internet-Plattform zu Datenschutz und Informationssicherheit. Die Projektpartner sind berechtigt, ihre Informationen auf der Website des «Virtuellen Datenschutzbüros» zu veröffentlichen. Zudem wird die Zusammenarbeit unter den deutschsprachigen Datenschutzstellen vernetzt und verstärkt.

Konferenzen
Der DSB hat weder an der Frühjahreskonferenz der europäischen Datenschutzstellen [vom 29./30. April in Prag] noch an der 32. Internationalen Datenschutzkonferenz [vom 27.–29. Oktober in Jerusalem] teilgenommen.

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

76 Alles Näheres zu «privatim» findet sich auf deren Homepage: «www.privatim.ch».

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

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

79 Vgl. dazu vorne S. 4.

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

7. Wir über uns

Pensen
Das Arbeitspensum von René Huber [Datenschutzbeauftragter] betrug im Berichtsjahr 100%. Im Herbst unterstützte lic. iur. Ion Eglin die Datenschutzstelle im Rahmen eines befristeten Arbeitsvertrages [Pensum von 100%].

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

Unser Aufwand für die verschiedenen Aufgaben
Statistische Angaben über die Anzahl der geführten Telefongespräche oder der behandelten Anfragen sind nur sehr beschränkt aussagekräftig: Eine einfache Anfrage lässt sich innerhalb von einer Stunde erledigen, ein komplexes Projekt kann dagegen einen Aufwand von vielen Arbeitstagen erfordern. In der folgenden Übersicht sehen Sie deshalb, für welche Tätigkeitsbereiche im Berichtsjahr wie viel Arbeitszeit eingesetzt wurde.

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

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

Bereich	2010	[2009]	[2008]	Hinweise			
Beratung der Zuger Einwohnerinnen und Einwohner	39 %	[45 %]	[44 %]	Erstkontakt mit:			
				kantonaler Verwaltung	25 %	[28 %]	[28 %]
				Gemeinde	6 %	[8 %]	[7 %]
				Private direkt	8 %	[9 %]	[9 %]
Ausbildungsangebote	4 %	[4 %]	[15 %][81]	Schulungen, Referate und Präsentationen für kantonale oder gemeindliche Verwaltungen			
Betreuung grösserer Projekte	10 %	[8 %]	[10 %]	Register der Datensammlungen, Gesetzgebung, Tätigkeitsbericht, Rechenschaftsbericht und Beitrag GVP			
Datensicherheit	3 %	[4 %][82]		Beratung kantonaler und gemeindlicher Verwaltungen			
Schengen/Dublin	7 %	[7 %]	[8 %]	Berichterstattungen, Kontrolle, Vorarbeiten zur Revision des Datenschutzgesetzes			
Öffentlichkeitsarbeit	8 %	[8 %]	[5 %]	Medienarbeit, Fachbeiträge, Homepage, Newsletter			
Zusammenarbeit mit EDÖB und kantonalen DSB	2 %	[2 %]	[2 %]	Informationsaustausch, Teilnahme an den Veranstaltungen des CH-DSB-Vereins «privatim»			
Weiterbildung	3 %	[3 %]	[1 %]	Tagungsbesuche [insbesondere im IT-Bereich]			
Diverses	24 %	[19 %]	[15 %]	Korrespondenz, Rechnungswesen, Personelles, Betreuung der eigenen IT-Infrastruktur, Bibliothek, Besprechungen – alles soweit nicht direkt einzelnen Projekten zuweisbar			
Total	100 %	[100 %]	[100 %]				

81 Im Vordergrund stand die Schulung im Zusammenhang mit der Umsetzung der Datensicherheitsverordnung.

82 Wurde in den Vorjahren nicht separat ausgewiesen.

III. Wichtige Tipps für Sie!

1. Sperren Sie Ihre Daten

Bei der Gemeinde

Wussten Sie, dass bei der Einwohnerkontrolle Ihrer Wohngemeinde
- jedermann Ihre Adresse erfragen kann?
- jedermann, der ein Interesse glaubhaft macht, Ihr Geburtsdatum, Ihren Zivilstand, Ihren Heimatort, Ihre Staatsangehörigkeit und Ihren Zuzugsort erfragen kann?
- jede Zuger Person oder Vereinigung, die einen schützenswerten ideellen Zweck glaubhaft macht, die vorstehend genannten Daten über Sie erhält?[83]
- Forschungsinstitutionen ohne Ihre Zustimmung Daten über Sie erhalten?

Wenn Sie das nicht möchten, dann können Sie Ihre Daten *bei der Einwohnerkontrolle in Ihrer Wohngemeinde kostenlos sperren lassen.* Es genügt, wenn Sie eine kurze Mitteilung machen. Eine Begründung ist nicht nötig. Einen Muster-Brief zum Herunterladen finden Sie auf unserer Website.[84] Die Einwohnerkontrolle muss die Sperre anschliessend schriftlich bestätigen.[85] Nun wissen Sie, dass Ihre Daten gesperrt sind.

Beim Strassenverkehrsamt

Wussten Sie, dass das Strassenverkehrsamt Ihre Fahrzeughalterdaten *für jedermann im Internet* zugänglich macht, an beliebige Private bekannt gibt und einem privaten Unternehmen für den Druck des «Motorfahrzeug Verzeichnis» zur Verfügung stellt? Allenfalls sind Ihre Daten somit auch via SMS auf dem Handy abrufbar und erscheinen in gedruckten und elektronischen Verzeichnissen.

Wenn Sie das nicht wollen, *so sperren Sie Ihre Daten beim Strassenverkehrsamt.* Wie bei der Sperre Ihrer Daten bei der Einwohnerkontrolle genügt eine kurze schriftliche Mitteilung an das Strassenverkehrsamt. Eine Begründung ist nicht nötig.

Im Jahr 2010 haben übrigens neu mehr als 1000 Privatpersonen[86] die Sperrung ihrer Halterdaten verlangt. Insgesamt haben in Zug nun etwas mehr als 2600 Private ihre Daten gesperrt.

2. Persönliches über Sie im Internet? Bei Facebook & Co.? Seien Sie vorsichtig!

Wussten Sie, dass das Internet nichts vergisst? Denken Sie daran, wenn Sie im Internet oder bei Facebook oder ähnlichen Websites etwas über sich selber veröffentlichen! Da grundsätzlich alles durch Suchmaschinen kopiert und archiviert wird, haben Sie im Moment der Publikation bereits die Herrschaft über Ihre Daten verloren. Löschen nützt nichts, Ihre Daten sind durch Google und Co. bereits weltweit verteilt archiviert. Diese bereiten die Daten über Sie auf und jedermann kann sich ein Bild von Ihnen machen: Ihr Arbeitgeber, ein möglicher Arbeitgeber bei einer Bewerbung[87], Ihre Krankenkasse, Ihre Nachbarschaft – wer auch immer. Ob die Daten über Sie richtig oder falsch, aktuell oder veraltet sind, das wissen nur Sie selber. Aufgrund der im Internet gefundenen Angaben und Fotos über Sie, machen sich aber Dritte ihre eigenen Gedanken.

Fazit: Ob am Arbeitsplatz oder im privaten Bereich, seien Sie vorsichtig, was Sie über sich selber im Internet veröffentlichen. Je weniger über Sie im Internet kursiert, desto besser ist Ihre Privatsphäre geschützt.

3. Wissen Sie, welche Daten die Zuger Verwaltung über Sie hat?

Sie können jederzeit Ihre eigenen Daten einsehen, die die Verwaltung über Sie hat.[88] Damit Sie sehen, wer welche Datensammlungen führt, gibt es das Register aller Zuger Datensammlungen von Kanton und Gemeinden im Internet.[89] Dort sehen Sie auch, an wen Sie sich wenden müssen, wenn Sie Einsicht oder Kopien Ihrer Daten wollen – was übrigens grundsätzlich alles kostenlos[90] ist. Weitere Hinweise zum Register finden Sie vorne S. 26.

4. Bleiben Sie informiert – abonnieren Sie unseren Newsletter!

Per E-Mail versenden wir kostenlos kurze Hinweise über Aktuelles zu Datenschutz und Datensicherheit. Schreiben Sie sich ein, dann sind Sie im Bild. Alles Nähere zu unserem Newsletter finden Sie vorne auf S. 20.

83 Im Rahmen einer Sammelauskunft gestützt auf § 8 Abs. 2 Bst. c Datenschutzgesetz.

84 «www.datenschutz-zug.ch» in der Rubrik «Kanton Zug/Aktuelles».

85 Ausführlichere Hinweise dazu im DSB TB 2006 S. 17 f. Fall Nr. 22.

86 Daneben sind alle Halterdaten der Zuger Polizei sowie weiterer öffentlichen Stellen gesperrt.

87 Google bzw. Facebook und ähnliche soziale Netzwerke sind je länger, je mehr wahre Fundgruben für Personalleiter.

88 Gestützt auf § 13 Datenschutzgesetz.

89 Auf unserer Website «www.datenschutz-zug.ch» in der Rubrik «Kanton Zug/Register der Datensammlungen».

90 Gemäss § 17 Abs. 2 Datenschutzgesetz.

Dank

Damit ich als Datenschutzbeauftragter alle meine Aufgaben und Dienstleistungen zugunsten der Privacy der Zugerinnen und Zuger erfüllen kann, bin ich auf die Hilfe, Unterstützung und Kooperation von sehr vielen Personen und Stellen angewiesen.

Gerne geht deshalb ein grosses und herzliches Dankeschön an

alle Mitarbeitenden kantonaler und gemeindlicher Verwaltungen aller Stufen, mit denen ich im Jahr 2010 zusammenarbeiten durfte, um konstruktive, gute und rechtmässige Lösungen zu erarbeiten;

kritische Geister, die durch konstruktive Kritik zur Weiterentwicklung des Datenschutzes beitragen;

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

Hildegard Steiner für die administrative, *alle Mitarbeiterinnen der Telefonzentrale* für die «telefonische» und *lic. iur. Ion Eglin* für seine wertvolle juristische Unterstützung;

Landschreiber Tino Jorio, für seine Bereitschaft, jederzeit als kompetenter, engagierter und auch kritischer Gesprächspartner in Sachen Datenschutz zur Verfügung zu stehen.

René Huber

Sachregister

Nützliche Adressen

Datenschutzstelle des Kantons Zug
Dr. iur. René Huber
[Datenschutzbeauftragter]
Regierungsgebäude
Seestrasse 2
Postfach 156
6301 Zug
Tel. 041 728 31 87
[direkt Huber]
Tel. 041 728 31 47
[Sekretariat]
Fax 041 728 37 01
www.datenschutz-zug.ch

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

Kantonale Verwaltung
Tel. 041 728 33 11
[Zentrale]

Gemeindeverwaltungen

Baar
Rathausstrasse 2
Postfach
6341 Baar
Tel. 041 769 01 20
Fax 041 769 01 91
www.baar.ch

Cham
Mandelhof
Postfach 265
6330 Cham
Tel. 041 723 87 03
Fax 041 723 87 02
www.cham.ch

Hünenberg
Chamerstrasse 11
Postfach 261
6331 Hünenberg
Tel. 041 784 44 44
Fax 041 784 44 99
www.huenenberg.ch

Menzingen
Rathaus
Alte Landstrasse 2A
Postfach 99
6313 Menzingen
Tel. 041 757 22 22
Fax 041 757 22 20
www.menzingen.ch

Neuheim
Dorfplatz 5
Postfach 161
6345 Neuheim
Tel. 041 757 21 30
Fax 041 757 21 40
www.neuheim.ch

Oberägeri
Rathaus
Alosenstrasse 2
Postfach 159
6315 Oberägeri
Tel. 041 723 80 25
Fax 041 723 80 01
www.oberaegeri.ch

Risch
Zentrum Dorfmatt
6343 Rotkreuz
Tel. 041 798 18 18
Fax 041 798 18 88
www.rischrotkreuz.ch

Steinhausen
Bahnhofstrasse 3
Postfach 164
6312 Steinhausen
Tel. 041 748 11 11
Fax 041 741 31 81
www.steinhausen.ch

Unterägeri
Seestrasse 2
Postfach 79
6314 Unterägeri
Tel. 041 754 55 00
Fax 041 754 55 55
www.unteraegeri.ch

Walchwil
Dorfstrasse 4
Postfach 93
6318 Walchwil
Tel. 041 759 80 10
Fax 041 758 80 07
www.walchwil.ch

Zug
Stadthaus am Kolinplatz
Postfach 1258
6301 Zug
Tel. 041 728 21 03
Fax 041 728 23 71
www.stadtzug.ch

www.datenschutz-zug.ch

Gestaltung: Christen Visuelle Gestaltung, Zug
Auflage: 1500 Exemplare
Druck: Multicolor Print AG, Baar
Gedruckt auf Refutura Recycling,
aus 100% Altpapier, CO_2-neutral, FSC