Datenschutzbeauftragter des Kantons Zug

Tätigkeitsbericht 2003 [Nr. 5]

Datenschutzbeauftragter des Kantons Zug

Tätigkeitsbericht 2003 [Nr. 5]

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

Der vorliegende Tätigkeitsbericht Nr. 5 deckt den Zeitraum zwischen 1. Januar 2003 und 31. Dezember 2003 ab.

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

Zug, 26. Januar 2004

Datenschutzbeauftragter des Kantons Zug
Dr. iur. René Huber

Ein paar häufig verwendete Abkürzungen:

Abs.	Absatz
BGS	Bereinigte Gesetzessammlung [Kanton Zug]
Bst.	Buchstabe
DS	Datenschutz
DSB	Datenschutzbeauftragter
DSG	Datenschutzgesetz
EDSB	Eidg. Datenschutzbeauftragter
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. Datenschutzbeauftragter, Feldeggweg 1, 3003 Bern, Tel. 031 322 43 95, «www.edsb.ch».

Ein wichtiger Hinweis

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

Für die Datenbearbeitung von privaten Unternehmen [Versicherern, Banken, Arbeitgebern usw.] sowie der Bundesverwaltung ist der Eidg. Datenschutzbeauftragte[2] zuständig.

ISSN 1424-4756

Inhaltsverzeichnis

Fünf Jahre Datenschutzstelle im Kanton Zug

Am 1. März 1999 hat die Datenschutzstelle des Kantons Zug ihren Betrieb aufgenommen. Fünf Jahre sind seit damals vergangen. Anlass genug für eine Standortbestimmung, eine kritische Rückschau und einen kurzen Ausblick.

Wozu Datenschutz?

Die öffentliche Verwaltung des Kantons und der Gemeinden bearbeitet eine Vielzahl von Daten über die Zugerinnen und Zuger – mehr als 1'200 registrierte Datensammlungen sind vorhanden.[3] Darunter befinden sich sehr viele sehr sensible Personendaten. Bei missbräuchlicher Bearbeitung dieser Daten kann den Betroffenen Schaden entstehen, der in vielen Fällen kaum mehr behoben werden kann.

Der Datenschutzbeauftragte setzt sich dafür ein, dass in der Verwaltung von Kanton und Gemeinden die rechtlichen Rahmenbedingungen den Schutz der Privatsphäre von Bürgerinnen und Bürgern gewährleisten und dass Missbräuche verhindert werden. Er ist zudem dafür besorgt, dass die Mitarbeitenden der Verwaltung die Personendaten nur so bearbeiten, wie es das Recht vorsieht.

Was ist erreicht worden?

In den letzten fünf Jahren konnte mit personellen Ressourcen im Rahmen eines 80%-Pensums folgende Dienstleistungen erbracht werden:

- Anfragen: Beratung oder Ausarbeitung von Lösungen in mehr als 540 grösseren Fällen [Herkunft der Anfragen: Privatpersonen: 150; Gemeindeverwaltungen: 150; kantonale Verwaltung: 240].
- Ausbildung: Über 20 Schulungen durchgeführt.
- Datensicherheit: Initiierung/Begleitung von vier IT-Sicherheitsüberprüfungen; Betreuung von IT-Projekten; Schulung Datensicherheit.
- Register: 1'200 Datensammlungen von kantonalen und gemeindlichen Verwaltungsstellen erfasst.
- Gesetzgebung: Bei über 30 Vernehmlassungen wurde eine Stellungnahme verfasst.
- Medienarbeit: Die Medien berichteten in mehr als 50 Beiträgen über den Zuger Datenschutz.
- Internet: Die wichtigsten Informationen sind publiziert und werden alle zwei Wochen aktualisiert.
- Mailing-Liste: 500 Abonnierte erhielten per E-Mail mehr als 560 Kurzinformationen zu Datenschutz und Datensicherheit.
- Publikationen: DSB-Tätigkeitsberichte; jährliche Beiträge in GVP[4]; Leitfaden «Datenschutz in der Schule».
- Weiteres: Konzeption, Organisation und Leitung der Konferenz der schweizerischen Datenschutzbeauftragten in Zug im Jahr 2002.

Es ist somit gelungen, Verwaltungsmitarbeitende aller Stufen und Funktionen ein stückweit auszubilden und im Umgang mit Personendaten zu sensibilisieren.

Dieser Standard konnte nur erreicht werden, weil der Regierungsrat, die oberste Führung, klare Entscheide zum Schutz der Privatsphäre traf.

Was ist zu tun?

Die Datenschutzstelle verfügt nur über sehr beschränkte personelle Ressourcen: am Ende des Berichtsjahres handelte es sich um zwei 60%-Pensen[5]. Neben der täglichen operativen Arbeit müssen die personellen Ressourcen zukünftig noch vermehrt im Bereich der Gesetzgebung eingesetzt werden. Schwerpunkt muss die Verbesserung der rechtlichen Rahmenbedingungen bilden. Gewährleisten diese den Schutz der Privatsphäre im Grundsätzlichen, so entfallen später die Probleme in vielen Einzelfällen. Weitere Schwerpunkte: Verfassen von konkreten bereichsspezifischen Handlungsanweisungen[6] für die Mitarbeitenden der Verwaltung sowie die Ausbildung der Mitarbeitenden der Verwaltung. Ein zentrales Schulungsthema ist der Grundsatz, dass Daten auch innerhalb der Verwaltung nicht frei fliessen,

3 Die näheren Informationen zum Projekt des «Registers der Datensammlungen» finden Sie hinten S. 31.

4 Gerichts- und Verwaltungspraxis des Kantons Zug.

5 Davon ist ein 20%-Pensum [befristete Aushilfsstelle] für das Projekt «Register der Datensammlungen» reserviert, s. dazu hinten Kapitel II Ziff. 7.

6 Leitfäden, Merkblätter usw.

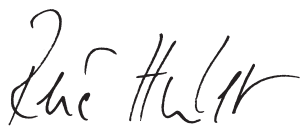
vielmehr das Amtsgeheimnis grundsätzlich auch innerhalb der Verwaltung gilt.[7]

Betrachten wir die Lage der klassischen bürgerlichen Freiheiten – wozu der Schutz des Privaten die Grundlage bildet – auf einer europa- oder gar weltweiten Ebene, so ist eine zunehmende und starke Bedrohung des Privaten festzustellen.[8]
Der Schutz des Privaten muss konsequenter und energischer geführt werden, kann doch nur so unsere freiheitliche, demokratische Gesellschaftsordnung erhalten bleiben.

Datenschutz im Jahr 2003

Der vorliegende Tätigkeitsbericht stellt einen Querschnitt durch die Arbeit der Datenschutzstelle im Jahre 2003 dar. Den Schwerpunkt bildet der Einblick in die Praxis: Anhand der Präsentation von 59 Fällen soll beispielhaft aufgezeigt werden, wo Aspekte des Datenschutzes oder der Datensicherheit tangiert sind – und welche Lösungen gefunden wurden.
Im Gegensatz zu den bisherigen Berichten sind die Fälle neu *thematisch* gruppiert, nicht mehr nach der betroffenen Amtsstelle. In Verbindung mit dem stark ausgebauten Sachverzeichnis[9] soll Ihnen damit der Zugang zu den einzelnen Informationen erleichtert werden. Aus Platzgründen musste die Darstellung vieler Fälle auf die wesentlichsten Punkten reduziert werden. Wenn Sie an Hintergrundinformationen interessiert sind, finden Sie am Ende gewisser Fälle neu den Hinweis, dass beim Datenschutzbeauftragten zusätzliche Informationen kostenlos erhältlich sind.

Ich wünsche Ihnen eine anregende Lektüre. Sollten Sie Fragen, Hinweise oder Anregungen haben – ich freue mich auf Ihre Rückmeldung!



Dr. iur. René Huber
Datenschutzbeauftragter des Kantons Zug

7 Siehe dazu hinten den Fall Nr. 2 S. 8.

8 Nicht zuletzt wegen des zunehmenden Ausbaus des Bereiches der inneren Sicherheit, aber auch aufgrund der neuen technischen Möglichkeiten, die in jeder Hinsicht umfassende Vernetzungen erlauben.

9 Siehe hinten S. 37.

Sind Sie in Eile? – Das Wichtigste des Jahres 2003

Zusammenarbeit mit der Verwaltung

Die Zusammenarbeit mit der kantonalen und gemeindlichen Verwaltung ist als effizient, intensiv und insgesamt als ausgezeichnet zu bezeichnen. Im Berichtsjahr fanden wiederum Besprechungen zur grundsätzlichen Standortbestimmung bezüglich Datenschutz und Datensicherheit mit Regierungsräten statt. Diese Gespräche sind für Umsetzung und Planung sehr wichtig.

Näheres → S. 5

Register der Datensammlungen

Die Datensammlungen der kantonalen Verwaltung sowie der Einwohnergemeinden sind erfasst. Ende 2003 umfasste das Register insgesamt 1'209 Datensammlungen. Ausblick: Seit anfangs 2004 ist das Register im Internet öffentlich zugänglich.

Näheres → S. 31

Hilfsmittel für die Praxis: Weisungen und Merkblätter

Das Datenschutzgesetz ist sehr abstrakt. Die Mitarbeitenden der Verwaltung finden die Lösung bei anstehenden Fragen selten direkt im Gesetz. Deshalb ist es wichtig, dass bereichsspezifische Handlungsanweisungen zur Verfügung stehen. Zwei gute Beispiele: Leitfaden «Datenschutz in der Schule» und die «Weisungen zum Datenschutz im Sozialamt».

Näheres → S. 5 f.

Beratung

Die 59 Beispiele bilden einen Querschnitt durch die Beratungspraxis des Jahres 2003.

Näheres → S. 8 ff.

Datensicherheit

Der DSB hat eine externe Firma damit beauftragt, bei der kantonsinternen Informatik [im Folgenden: ITL[10]] drei Bereiche einem IT-Sicherheitstest zu unterziehen. Grundsätzlich waren die Strukturen sicher. Wo Mängel festgestellt wurden, sind Massnahmen ergriffen worden.

Näheres → S. 6

Ausbildung des Verwaltungspersonals

Im Rahmen der halbtägigen Schulung des neuen Betriebssystems konnte der DSB die Mitarbeitenden der Verwaltung mit den Grundlagen von Datenschutz und Datensicherheit vertraut machen. Zudem stellt die Datenschutzstelle diese Bereiche nun auch am «Einführungstag der neuen Mitarbeitenden» vor.

Näheres → S. 32

Internet-Auftritt und Mailing-Liste des Datenschutzbeauftragten

Aktuelles aus den Bereichen Datenschutz und Datensicherheit wird den eingeschriebenen Interessierten kostenlos per E-Mail in Form von Kurzmeldungen zugestellt. Damit entfällt mühseliges Absuchen der DSB-Website auf Neuigkeiten. Auf der Website sind die grundlegenden Informationen zu finden. Die Nutzung von Internet und Mailing-Liste hat im Berichtsjahr um rund 10% beziehungsweise 20% zugenommen.

Näheres → S. 28

Nutzung des Telefons

Der Regierungsrat hat die Nutzung des Telefons durch die Mitarbeitenden der Verwaltung näher umschrieben. Private Nutzung ist in einem gewissen Umfang zulässig – Abhören, Aufzeichnen oder Überwachen durch den Arbeitgeber sind verboten.

Näheres → S. 29 f.

Internationales

Der DSB nahm an drei wichtigen internationalen Veranstaltungen teil. Informieren Sie sich in diesem Abschnitt, was in Sachen Datenschutz und Datensicherheit weltweit aktuell ist.

[Hinweis: Die Teilnahme des DSB an diesen drei Konferenzen erfolgte in der Freizeit und auf eigene Kosten.]

Näheres → S. 33 f.

10 Der kantonsinterne Informatikdienstleister wird als ITL bezeichnet [Informationstechnik-Leistungszentrum].

I. Grundlegende Themen und Projekte

1. Zusammenarbeit mit der Verwaltung

Der positive Ausgangspunkt

Die Datenschutzstelle arbeitet fachlich absolut unabhängig von der kantonalen Verwaltung.[11] Es bestehen aber häufige und vielfältige Kontakte und Zusammenarbeitsformen mit den einzelnen Verwaltungsstellen. Auch wenn der Schutz der Privatsphäre der Bürgerinnen und Bürger gegenüber der Verwaltung manchmal hart erkämpft werden muss, funktioniert die Zusammenarbeit mit den jeweiligen Verwaltungsstellen stets sehr gut.

Gespräche mit der Regierung

Die gesetzmässige Umsetzung der Bestimmungen des Datenschutzes und der Datensicherheit sind in den Grundzügen Chefsache. Es finden deshalb regelmässig «anlassfreie»[12] Besprechungen mit Regierungsräten statt, um die wichtigsten aktuellen Themen zu besprechen, geplante Projekte frühzeitig auf die Aspekte Datenschutz und Datensicherheit zu überprüfen und um auf das aktuelle Dienstleistungsangebot des DSB hinzuweisen, insbesondere auch bezüglich Ausbildung.
Im Berichtsjahr führte der DSB mit dem Finanzdirektor Peter Hegglin und mit dem Bildungsdirektor Matthias Michel [in Anwesenheit der jeweiligen Direktionssekretäre] je ein Gespräch. Diese Besprechungen sind aus der Sicht des DSB in jeder Hinsicht sehr wertvoll, ermöglichen sie doch einen frühzeitigen Informationsaustausch und eine rechtzeitige Weichenstellung im Grundsätzlichen.
Es ist sinnvoll, etwa alle zwei Jahren eine solche Standortbestimmung mit der Direktionsvorsteherin, mit dem jeweiligen Direktionsvorsteher vorzunehmen.

Kontakt zu den Gemeinden

Auch die Zusammenarbeit mit den Gemeinden kann als ausgezeichnet bezeichnet werden. Da keine Gemeinde vom Recht Gebrauch gemacht hat,[13] eine unabhängige gemeindliche Datenschutzstelle einzurichten, wird das Dienstleistungsangebot des DSB – wenn auch in sehr unterschiedlichem Ausmass – genützt. Die Kontakte laufen dabei in der Regel über die GemeindeschreiberInnen, viele Anfragen kommen auch direkt aus den betroffenen Verwaltungsstellen.

Vermittler in Konfliktsituationen

Seit März 2003 verfügt die kantonale Verwaltung in der Person von Rechtsanwalt und Mediator Beat Gsell über einen fachlich unabhängigen «Vermittler in Konfliktsituationen», der administrativ bei der Sicherheitsdirektion angegliedert ist. Es fanden verschiedene Besprechungen statt, wobei es insbesondere auch um Fragen der jeweiligen thematischen Abgrenzung ging.

2. Hilfsmittel für die Praxis

Leitfaden «Datenschutz in der Schule»

Im Bereich der Schulen werden sehr viele, zum Teil auch sehr heikle Daten bearbeitet – so etwa: Beurteilungen von Schülerinnen und Schülern bezüglich Leistung und Leistungsverhalten, Angaben zum persönlichen Umfeld und zum Elternhaus, zu Religion und zu Gesundheit.[14] Wer von welchen Daten Kenntnis haben darf, ist oft nicht einfach zu beurteilen. Gelangen Informationen über ein Kind oder einen Jugendlichen, dessen Eltern oder andere Bezugspersonen an Unberechtigte, können gravierende Persönlichkeitsverletzungen resultieren. Dies kann für die fehlbare Person disziplinarische, zivilrechtliche oder auch strafrechtliche Folgen haben.
Der rechtmässige Umgang mit den Daten des Schulbereichs ist somit für alle Beteiligten ein zentrales Anliegen.
Die Direktion für Bildung und Kultur hat deshalb zusammen mit dem Datenschutzbeauftragten die Broschüre «Datenschutz – Leitfaden für die Schule im Kanton Zug» verfasst. Zielpublikum sind in erster Linie Lehrpersonen [auch aus den Bereichen Logopädie und Psychomotorik] und Schulleitungen, aber auch Eltern. Praxisbezogen und gut verständlich wird auf sieben Seiten kurz und knapp über die wichtigsten Grundsätze informiert.
Der Leitfaden behandelt die folgenden Vorgänge: Datenerhebung, Datenbearbeitung, Datenvernichtung/Datenarchivierung. So wird etwa im Abschnitt «Keine Daten auf Vorrat» auf den wichtigen datenschutzrechtlichen Grundsatz der Datensparsamkeit eingegangen, es wird erläutert, dass Daten grundsätzlich bei den betroffenen Personen – und nicht etwa bei Dritten – zu erheben sind, und im Kapitel «Behandeln Sie Personendaten sorgfältig» erhalten die Lehrperso-

11 Sie ist nur in administrativer Hinsicht der Staatskanzlei zugeordnet.

12 Daneben ergeben sich auch Sitzungen im Zusammenhang mit konkreten und aktuellen Fragestellungen.

13 Siehe § 18 Abs. 3 Datenschutzgesetz.

14 Siehe auch die Fälle hinten Kapitel II Ziff. 1.6, S. 17 ff.

nen grundlegende Hinweise zur Datensicherheit. Der Leitfaden wurde an sämtliche Lehrpersonen im Kanton abgegeben. Soweit wir erfahren haben, stiess er bei den Betroffenen auf eine sehr gute Aufnahme.

Weisungen im Sozialbereich

Das Sozialamt der Stadt Zug hat in Zusammenarbeit mit dem DSB eine interne «Weisung Datenschutz» ausgearbeitet. Dabei werden auf fünf Seiten die Rahmenbedingungen für den Umgang mit Daten im Sozialamt definiert. Diese Weisung ist ein nützliches Hilfsmittel für die Mitarbeitenden des Sozialamtes, werden sie doch nicht nur im Umgang mit schützenswerten Daten sensibilisiert, sondern erhalten Anweisungen, wie sie in konkreten Situationen vorzugehen haben. Die Weisung wird den Mitarbeitenden nicht nur in die Hand gedrückt, sondern im Rahmen einer halbtägigen Veranstaltung auch erläutert und vermittelt.

Der Erlass von Weisungen – oder Merkblättern oder Informations-Broschüren – im Bereiche des Datenschutzes ist *sehr zu begrüssen,* handelt es sich doch bei den datenschutzrechtlichen gesetzlichen Bestimmungen um sehr abstrakt formulierte Sachverhalte. Damit die Mitarbeitenden der Verwaltung wissen, was diese abstrakten Bestimmungen für ihre tägliche Arbeit genau bedeuten, sind ihnen konkrete, auf ihren Bereich bezogene Informationen bereit zu stellen. Der DSB wird deshalb zukünftig vermehrt versuchen, zusammen mit den jeweiligen Amtsstellen, bereichsspezifische Unterlagen zu erarbeiten und zu schulen.

3. Datensicherheit[15]

Technische Sicherheitsüberprüfungen

Die Bearbeitung von Daten der Zuger Bevölkerung ist das Kerngeschäft der Verwaltung. Darunter befinden sich sehr viele, sehr sensible Daten. Aufgrund des Datenschutzgesetzes ist die Verwaltung verpflichtet,[16] ihre besondere Verantwortung wahrzunehmen und die Datensicherheit gemäss dem aktuellen Stand der Technik zu garantieren. Weil die Datensicherheit die *Grundlage* jeglichen Datenschutzes ist, wird der DSB denn auch von Gesetzes wegen in die Pflicht genommen,[17] diesbezüglich entsprechend aktiv zu sein.

Im Berichtsjahr hat der DSB eine Firma beauftragt, Aspekte der Netzwerksicherheit, die Konfiguration der neuen PC bezüglich gewisser Sicherheitsmassnahmen und ein Tool, das den Zugriff auf Mail-Konten von extern ermöglicht, bei der kantonsinternen Informatikabteilung [im Folgenden: ITL] zu überprüfen. Diese technischen Sicherheitsüberprüfungen fanden in enger Zusammenarbeit zwischen ITL, der beauftragten Firma und dem DSB als Auftraggeber statt.
Ohne auf Einzelheiten einzugehen, kann festgehalten werden, dass das ITL die geprüften Bereiche grundsätzlich sicher betreibt. Wo Mängel oder Sicherheitslücken festgestellt wurden, sind entsprechende Massnahmen eingeleitet worden.
Da die IT-Landschaft zwangsläufig dauernden Veränderungen unterworfen ist,[18] und Risiken und Gefahren aufgrund der zunehmenden Komplexität der Systeme steigen, ist eine regelmässige Überprüfung der Systeme sehr wichtig.

Datensicherheitsverordnung

Gemäss der verbindlichen Anweisung im Datenschutzgesetz[19] hätte der Regierungsrat bis Ende 2001 eine Datensicherheitsverordnung erlassen müssen. Im Berichtsjahr blieb die Finanzdirektion diesbezüglich untätig – und dies trotz eines Beschlusses des Regierungsrates, demgemäss ihm bis im Sommer 2002 ein entsprechender Rechtserlass vorzulegen sei.
Es ist davon auszugehen, dass die Datensicherheitsverordnung im Jahr 2004 erlassen wird, handelt es sich dabei doch um ein Jahresziel der Finanzdirektion. Im nächsten Tätigkeitsbericht werden Sie an dieser Stelle über den weiteren Verlauf dieses Projekts informiert.

Fachgruppe Informatiksicherheit

Die im Herbst 2000 eingesetzte Fachgruppe Informatik-Security[20] hat die Aufgabe, das Thema Informatiksicherheit in der kantonalen Informatik kontinuierlich zu begleiten. Die Leitung der Fachgruppe hat im Berichtsjahr zu keinen Sitzungen eingeladen – trotz unerledigter Pendenzen aus den Vorjahren.

15 Fälle aus der Beratungspraxis zum Thema Datensicherheit finden Sie hinten auf S. 26 f.

16 § 7 Abs. 1 Datenschutzgesetz [«Datensicherung»]: «Daten sind insbesondere vor Verlust, Fälschung, Entwendung, Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte zu sichern.»

17 § 19 Abs. 1 Bst. a Datenschutzgesetz.

18 Zu denken ist an neue Hardware, neue Software sowie Upgrades und Aktualisierungen usw.

19 Siehe § 7 Abs. 2 Datenschutzgesetz.

20 Zusammensetzung: Finanzdirektion [Leitung], AIO/ITL, Obergericht und DSB.

4. Regelung des Online-Zugriffs auf Datensammlungen

Der Online-Zugriff auf eine Datensammlung ist etwas Spezielles und aus den beiden folgenden zwei Gründen problematisch:

1. Der Online-Zugriff richtet dem Zugriffsberechtigten einen frei zugänglichen, grundsätzlich unkontrollierten «Selbstbedienungsladen» ein. Der Datenherr muss der einzelnen Abfrage weder zustimmen, noch hat er überhaupt Kenntnis vom Abrufvorgang. Es ist ihm zum vornherein jegliche Möglichkeit genommen, eine Kontrolle des Datenbezugs auszuüben. Potenzielle Missbräuche können nicht festgestellt werden, beziehungsweise erst im Nachhinein und auch dies nur, sofern entsprechende Protokolle – so genannte Log-Files – vorhanden sind.[21]
   Missbräuche können insbesondere dann leicht entstehen, wenn Passwörter von Zugangsberechtigten unerlaubterweise weitergegeben oder Abfragen für nicht auftragsrelevante Zwecke vorgenommen werden. Beides kommt in der Praxis nicht allzu selten vor. Zudem werden die Zugriffsmöglichkeiten häufig zu umfassend und damit unter Missachtung des Verhältnismässigkeitsgebotes auf zu viele Datenfelder bewilligt.[22]
2. Meist ergeben sich Risiken bezüglich der Datensicherheit: Spielt sich der Online-Zugriff nicht innerhalb einer sicheren und gegen aussen abgeschlossenen Netzwerkumgebung ab, ist für den Zugriff zwingend eine sichere Verschlüsselungstechnologie einzusetzen.

Das Datenschutzgesetz verpflichtet den Regierungsrat[23] aus diesen Gründen, bis Ende 2001 das Bewilligungsverfahren bezüglich des Online-Zugriffs – auch als Zugriff im Abrufverfahren bezeichnet – in einer Verordnung speziell zu regeln. Diesbezüglich sind bis anhin jedoch *keinerlei* gesetzgeberische Arbeiten in Angriff genommen worden.
Hingegen haben die beiden Gemeinden Hünenberg und Neuheim kommunale gesetzliche Grundlagen für das Abrufverfahren geschaffen. Der DSB hat hier Input geleistet. Die gemeindlichen Verordnungen regeln das Bewilligungsverfahren, die Rechte und Pflichten von Datenlieferant und Datenbezüger sowie die zu beachtenden Rahmenbedingungen. Als Bewilligungsinstanz ist zu Recht der Gemeinderat bezeichnet worden. Der DSB erhält jeweils automatisch eine Kopie des Gemeinderatsbeschlusses bei Zulassung oder Verweigerung eines Abrufverfahrens.
Diese beiden gemeindlichen Rechtserlasse regeln den Online-Zugriff in vorbildlicher Weise. Gestützt auf diese beiden Erlasse wurden verschiedene Abrufverfahren bewilligt – siehe dazu den ausführlichen Fall aus der Beratungspraxis.[24]

21 In der Praxis werden Aufzeichnungen von Zugriffen selten überprüft, da diese Kontrollen sehr zeitintensiv sind.

22 Der Datenbezüger will einen Zugriff auf möglichst viele Daten, um jede auch nur erdenkliche Situation abdecken zu können.

23 § 7 Abs. 2 Datenschutzgesetz.

24 Hinten Fall Nr. 8 S. 10.

II. Berichterstattung 2003

1. Fälle aus der Beratungspraxis

Falls Sie im Folgenden wichtige Themen vermissen, konsultieren Sie doch die früheren Tätigkeitsberichte – Sie finden dort über 150 weitere Fallbeispiele.[25]

1.1 Recht auf Einsicht in die eigenen Daten

Fall 1 Darf ich meine eigenen Daten einsehen?

Der DSB erhält sehr häufig Anfragen von Privatpersonen, die wissen möchten, welche Daten die Verwaltung über sie hat. Sie möchten Einsicht nehmen oder Kopien von Dokumenten erhalten, die sie betreffen. Wie ist die Rechtslage?

Jede Person kann beim datenführenden Organ mündlich oder schriftlich Auskunft über alle ihre Daten verlangen.[26] Soweit technisch und organisatorisch möglich, wird Einsicht in die Daten beim Organ, das die Datensammlung führt, gewährt. Die betroffene Person kann von ihren Daten Kopien verlangen, und diese sind grundsätzlich kostenlos.[27]

Das Einsichtsrecht kann unter gewissen Umständen eingeschränkt werden: Ein Organ kann die Auskunft und Einsicht über Daten im überwiegenden Interesse der Öffentlichkeit oder Dritter begründet einschränken, mit Auflagen versehen, aufschieben oder verweigern.[28]

Diese Ausnahmen sind aber *restriktiv* zu handhaben. Eine Verwaltungsstelle, die einem Gesuch nicht oder nicht vollständig entspricht, muss einen begründeten, mit einer Rechtsmittelbelehrung versehenen Entscheid erlassen.[29] Gegen diesen Entscheid kann sich der betroffene Private wehren, indem er den Rechtsweg beschreitet. Die Rechtspflege richtet sich nach dem Verwaltungsrechtspflegegesetz.[30]

Heutzutage erfüllen sehr viele private Institutionen aufgrund von Leistungsaufträgen öffentliche Aufgaben für die Gemeinden oder den Kanton. In diesem Fall spricht man von ausgelagerter Datenbearbeitung. Da die betroffene Person durch die Auslagerung rechtlich nicht schlechter gestellt werden darf, stehen ihr bei ausgelagerter Datenbearbeitung die gleichen Rechte zu, wie wenn diese durch ein öffentliches Organ erfüllt worden wäre. Für die Einschränkung des Einsichtsrechts ist das Organ zuständig, das die Datenbearbeitung ausgelagert hat.

Es spielt für die Einsichtsrechte keine Rolle, auf welchem Medium sich die Daten befinden und welcher Art sie sind: Handnotizen, Papier, EDV, Fotos, Ton- oder Bildaufzeichnungen usw. Da zudem immer wieder Unklarheiten bezüglich handschriftlicher Akten, wie Protokolle oder Notizen, bestehen, sei folgender Hinweis angefügt: Daten müssen aktuell, richtig und vollständig sein, soweit es der Bearbeitungszweck verlangt.[31] Daraus lässt sich ableiten, dass Handnotizen, Protokolle oder Tagebucheinträge zu datieren sind und es zudem möglich sein muss, die Urheberin oder den Urheber der entsprechenden Schriftstücke eruieren zu können.[32]

Befinden sich Daten bei den Akten, die sich auf Dritte beziehen, so sind die entsprechenden Daten für die Einsicht verlangende Person unkenntlich zu machen.

Zuhanden der Verwaltungsstellen ist abschliessend zu betonen, dass es sich beim Einsichtsrecht von Bürgerinnen und Bürgern um ein *fundamentales Recht* handelt. Unrichtig ist es, wenn Verwaltungsstellen Einsicht verlangende Personen als «Störer» des Verwaltungsablaufs behandeln.

1.2 Allgemeine Verwaltung von Kanton und Gemeinden

Fall 2 Kein freier Informationsaustausch innerhalb der Verwaltung!

Auch in diesem Jahr betrafen viele Anfragen die Datenbekanntgabe innerhalb der Verwaltung. Es muss immer wieder betont werden: Das Amtsgeheimnis gilt auch innerhalb der Verwaltung.[33] Daten dürfen deshalb weder beim Kanton noch bei den Gemeinden zwischen Amtsstellen oder Mitarbeitenden frei ausgetauscht werden – auch nicht in der Kaffeepause oder beim gemeinsamen Mittagessen in der Kantine.

Zulässig ist die Datenbekanntgabe nur, wenn
- eine ausdrückliche gesetzliche Grundlage vorhanden ist;
- die Zustimmung des Betroffenen vorliegt;
- die Datenbekanntgabe für die gesetzlich vorgegebene Aufgabe unentbehrlich [wenn es um «gewöhnliche» Personendaten geht] bzw. offensichtlich unentbehrlich ist [wenn es sich um besonders schützenswerte Personendaten handelt];
- der Weg des Amtshilfeverfahrens beschritten wird.

25 Die Tätigkeitsberichte 1999–2002 können Sie 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».

26 § 13 Datenschutzgesetz.

27 § 17 Abs. 2 Datenschutzgesetz.

28 § 14 Abs. 1 Datenschutzgesetz.

29 § 16 Datenschutzgesetz.

30 § 22 Datenschutzgesetz.

31 § 4 Bst. a Datenschutzgesetz.

32 Zum Beispiel mittels Unterschrift, Namenskürzel oder aus dem direkten Zusammenhang.

33 § 29 Personalgesetz [BGS 154.21] i. V. m. § 11 Personalverordnung [BGS 154.211].

Die Datenbekanntgabe ist streng geregelt. Verstösse werden sanktioniert.[34] Die Datenbekanntgabe ist somit eher die Ausnahme als die Regel.
Dies hängt insbesondere mit der Zweckbestimmung der Daten zusammen: Eine Verwaltungsstelle erhebt spezifisch die für ihre Aufgabenerfüllung notwendigen Daten, nicht mehr, nicht weniger, nicht andere. Im Kontext einer *anderen* Verwaltungsstelle können die *gleichen* Daten unvollständig, missverständlich oder vielleicht sogar falsch sein. Jede Verwaltungsstelle muss deshalb grundsätzlich die für ihre Aufgabe erforderlichen Daten direkt *beim Betroffenen* erheben. Nur so ist die Datenbearbeitung der Verwaltung für die Betroffenen transparent. Diese haben auch nur so die Möglichkeit, veraltete, unvollständige oder gar falsche Daten über sie berichtigen zu lassen.
Würden hingegen Daten innerhalb der Verwaltung beliebig zirkulieren, erhielte die Bürgerin, der Bürger, davon keine Kenntnisse. Damit wären wir wieder in den «Fichen-Zeiten» angelangt …

Fall 3 Das Wichtigste zur Amtshilfe

Wie im vorstehenden Fall dargestellt, bilden die Datenbestände der öffentlichen Verwaltung keinen Selbstbedienungsladen für die diversen Amtsstellen. Das Amtsgeheimnis verlangt vielmehr – unter Strafandrohung bei Missachtung –, dass Daten grundsätzlich *nicht* anderen Amtsstellen oder Dritten bekannt gegeben werden dürfen.
Vielmehr braucht es dazu eine gesetzliche Grundlage, die Zustimmung der Betroffenen, oder der Datenbezug muss für die Aufgabenerfüllung unentbehrlich sein.[35] Sind diese Voraussetzungen nicht erfüllt, ist zu prüfen, ob *Amtshilfe* zu leisten ist.
Ist ein Organ der Ansicht, es benötige für die Erfüllung seiner Aufgaben Daten einer anderen Stelle, so hat es bei dieser ein *begründetes Gesuch* um Amtshilfe zu stellen.[36] Diese prüft das Gesuch in Kenntnis der Sachlage und nimmt eine *Interessenabwägung* vor. Wird dem Gesuch stattgegeben, hat die Entbindung vom Amtsgeheimnis durch den Direktionsvorsteher[37] zu erfolgen.[38]

Fall 4 Amtshilfe: Liefert die Gebäudeversicherung der Steuerverwaltung Daten?

Ein Steuerpflichtiger erkundigte sich, ob die Steuerverwaltung mit Daten der Gebäudeversicherung beliefert werde – insbesondere bezüglich des Wertes eines Gebäudes.

Im Veranlagungsverfahren ist der Partner und Datenlieferant der Steuerverwaltung der jeweilige Steuerpflichtige. Dieser muss alles tun, um eine vollständige und richtige Veranlagung zu ermöglichen.[39] Die Steuerverwaltung hat demgegenüber die Pflicht, die Steuererklärung zu prüfen und die erforderlichen Untersuchungen vorzunehmen.[40]
In Übereinstimmung mit den datenschutzrechtlichen Grundsätzen beschafft sich die Steuerverwaltung somit die erforderlichen Daten *beim Betroffenen*. Erfüllt die steuerpflichtige Person ihre Verfahrenspflichten nicht oder können die Steuerfaktoren mangels zuverlässiger Unterlagen nicht einwandfrei ermittelt werden, so kann die Steuerverwaltung eine Ermessenseinschätzung vornehmen.[41]
Daneben hat die Steuerverwaltung die Möglichkeit, bei Behörden *amtshilfeweise* Auskunft zu verlangen.[42] Das Verhältnismässigkeitsprinzip verlangt jedoch, dass die fraglichen Daten vorerst beim Steuerpflichtigen selber erhoben werden müssen. Die Amtshilfe greift somit erst, wenn die für die Steuerbehörden notwendigen Daten vom Steuerpflichtigen nicht bekannt gegeben werden [bzw. konkreter Anlass für die Annahme vorliegt, dass die bekannt gegebenen Daten nicht korrekt sind].
Zudem ist einschränkend festzuhalten, dass die Steuerverwaltung von anderen Organen – unter Einschluss der Gebäudeversicherung bzw. des Grundbuchamtes – Auskunft nur in bestimmten, genau bezeichneten Einzelfällen verlangen kann. Für *systematische Erhebungen* bildet § 110 des Steuergesetzes hingegen *keine* Rechtsgrundlage. Der Steuerverwaltung ist diese Rechtslage bekannt, und sie geht dementsprechend vor.

Fall 5 Gibt die Gebäudeversicherung Kundendaten an Dritte weiter?

Ein privates Unternehmen des Immobiliensektors möchte bei den Eigentümern der hundert grössten Gebäude im Kanton Zug Werbung für seine Dienstleistungen machen. Die Gebäudeversicherung verfügt über diese Informationen. Können sie dort auch bezogen werden?
Auf die Gebäudeversicherung ist das Datenschutzgesetz anwendbar. Sie darf Daten an Private demnach nur aufgrund einer ausdrücklichen gesetzlichen Grundlage oder mit der ausdrücklichen Zustimmung der Betroffenen bekannt geben. Beide Voraussetzungen sind nicht gegeben.

34 Amtsgeheimnisverletzungen können disziplinarische, zivilrechtliche und strafrechtliche Konsequenzen haben.

35 § 5 Datenschutzgesetz.

36 Vorausgesetzt, es gebe keine ausdrückliche gesetzliche Grundlage für die Datenbekanntgabe bzw. die Zustimmung der betroffenen Person liege nicht vor.

37 In der Gemeinde durch den zuständigen Gemeinderat.

38 § 29 Personalgesetz [BGS 154.211].

39 § 127 Abs. 1 Steuergesetz [BGS 632.1].

40 § 130 Abs. 1 Steuergesetz.

41 § 130 Abs. 3 Steuergesetz.

42 § 110 Steuergesetz.

Fazit: Die Gebäudeversicherung darf die gewünschten Daten *nicht* herausgeben.

Fall 6 Verletzt die briefliche Abstimmung das Abstimmungsgeheimnis?

Im Nachgang zu Wahlen und Abstimmungen beanstanden Privatpersonen immer wieder, der Zuger Modus der brieflichen Stimmabgabe verletze das Stimmgeheimnis, weil auf dem Rücksendeumschlag der Name der stimmenden Person aufgeführt ist.
Diese Thematik führte bereits 2001 zu einer als erheblich erklärten Motion.[43] Der DSB gab gegenüber dem Regierungsrat eine Stellungnahme ab, die zusammengefasst[44] Folgendes beinhaltet:
Im Zusammenhang mit Abstimmungen und Wahlen auf Bundesebene sind zwingend die entsprechenden *Bundesvorschriften* zu beachten. Diese sehen vor, dass das Stimmgeheimnis zu gewährleisten ist und Missbräuche zu verhindern sind. Die Anforderungen des Bundes und die Rechtsprechung des Bundesgerichts sind bezüglich der Garantie des Stimmgeheimnisses *sehr streng*. Es ist deshalb jede auch noch so konstruierte Möglichkeit einer Verletzung des Stimmgeheimnisses auszuschliessen.

Fazit: Um die bundesrechtlichen Vorgaben bezüglich des Stimmgeheimnisses in jedem Fall zu erfüllen, ist möglichst umgehend ein Vorgehen zu wählen, das auf die Angaben zur Person des Abstimmenden auf dem Rücksendeumschlag *verzichtet*.[45] Der DSB kam im Weiteren zum Schluss, dass eine *klare Verbesserung* der Gewährleistung des Stimmgeheimnisses auch ohne Änderung des geltenden Zuger Wahlgesetzes umgesetzt werden kann.

[Ausblick: Der Regierungsrat hat die Direktion des Innern im Januar 2004 beauftragt, bis März 2004 eine entsprechende Revision des Wahlgesetzes auszuarbeiten. Ziel ist, dass die neue Regelung am 1. Januar 2005 in Kraft tritt.]

Fall 7 Informiert das Grundbuchamt die Steuerbehörden?

Gewisse Rechtsgeschäfte sind gemäss Steuergesetz[46] Handänderungen an Grundstücken gleichgestellt und unterliegen deshalb der Grundstückgewinnsteuer.[47] Diese Verträge können ohne Mitwirkung der gemeindlichen Urkundsperson abgeschlossen werden und zur Eintragung ins Grundbuch angemeldet werden. Steuerpflichtig ist die veräussernde Person.[48] Sie hat innerhalb von 60 Tagen der Veranlagungsbehörde eine Steuererklärung einzureichen.[49]
Darf das Grundbuchamt dem zuständigen Grundstückgewinnsteueramt von sich aus, somit unaufgefordert, solche Rechtsgeschäfte melden? Im Einzelfall? Systematisch?
Die Stellungnahme des DSB kam zusammengefasst[50] zu folgenden Schlüssen: Es handelt sich um eine Frage der *Amtshilfe*. Die Steuerbehörde kann gestützt auf § 110 des Steuergesetzes von anderen Organen – unter Einschluss des Grundbuchamtes – Auskunft nur in *bestimmten, genau bezeichneten Einzelfällen* verlangen. Das Verhältnismässigkeitsprinzip verlangt, dass die fraglichen Daten vorerst beim Steuerpflichtigen selber erhoben werden müssen. Die Amtshilfe greift somit erst, wenn die für die Steuerbehörden notwendigen Daten vom Steuerpflichtigen *nicht* bekannt gegeben werden [bzw. konkreter Anlass für den Verdacht vorliegt, dass die bekannt gegebenen Daten nicht korrekt sind]. Für systematische Erhebungen bildet § 110 Steuergesetz dagegen *keine Rechtsgrundlage*.
Es ist darauf hinzuweisen, dass der Steuerpflichtige gemäss Steuergesetz[51] *von sich aus* die Steuerbehörden darauf hinzuweisen hat, dass ein der Steuerpflicht unterliegendes Rechtsgeschäft vorgenommen wurde. Kommt der Steuerpflichtige diesen gesetzlichen Verpflichtungen nicht nach, löst dies – wie ganz allgemein bei Steuerhinterziehung oder Steuerbetrug – die entsprechenden Sanktionen[52] nach sich.
Hier[53] finden Sie einen ergänzenden rechtspolitischen Hinweis.

Fall 8 Online-Zugriff auf die Daten der Einwohnerkontrolle?

Die Einwohnerkontrolle jeder Gemeinde verfügt über die tagesaktuellen Daten ihrer Einwohnerinnen und Einwohner. Kantonale Organe möchten online, somit aufgrund eines Abrufverfahrens, auf diese Datenbank zugreifen. Wie ist die Rechtslage?

Besonderheit der Datenbekanntgabe via Online-Zugriff
Vorweg ist zu betonen, dass es sich bei der Datenbekanntgabe im Abrufverfahren *nicht* um eine «gewöhnliche» Datenbekanntgabe handelt, können doch die Berechtigten in den Datenbeständen

43 Motion Stuber/Schmid [vom 8. Januar 2001, Vorlage Nr. 863.1/Laufnummer 10413], die entgegen dem Bericht und Antrag des Regierungsrates [vom 28. August 2001; Vorlage 863.2/Laufnummer 10679] durch den Kantonsrat erheblich erklärt worden ist.

44 Die ausführliche Stellungnahme ist in GVP 2003 veröffentlicht.

45 Siehe etwa die Lösungen der Kantone Luzern, Nidwalden, Obwalden oder Zürich usw.

46 § 189 Abs. 3 Steuergesetz [BGS 632.1].

47 Zum Beispiel Gewährung eines Überbaurechts oder Verträge bezüglich der Übertragung von Benützungsrechten an Autoabstellplätzen.

48 § 192 Steuergesetz.

49 § 200 Steuergesetz.

50 Die ausführliche Stellungnahme ist in GVP 2003 veröffentlicht.

51 § 200 Steuergesetz.

52 Gemäss §§ 203–228 Steuergesetz.

53 Sollte der Gesetzgeber der Überzeugung sein, dass hier ein Missstand besteht, der zu beheben ist, so steht es ihm selbstverständlich frei, *im Steuergesetz* [ungenügend wäre eine Regelung auf Verordnungsstufe, da die jetzige Regelung im Steuergesetz statuiert ist] eine entsprechende Änderung vorzunehmen, um einen systematischen Datenaustausch zwischen dem Grundbuchamt und den zuständigen Steuerbehörden vorzusehen. Es ist zu beachten, dass die Steuerbehörde ganz grundsätzlich und umfassend durch den Steuerpflichtigen zu informieren ist. Verletzt dieser seine Verfahrenspflichten, kann sich die Frage nach strafrechtlichen Sanktionen stellen.

grundsätzlich beliebige Abfragen vornehmen[54], ohne dass die Datenherrin dies im Moment des Zugriffs kontrollieren kann.[55] Der Online-Zugriff ermöglicht dem Berechtigten somit den Zugang zu einem «datenmässigen Selbstbedienungsladen», in dem er sich jederzeit nach Belieben bedienen kann. Damit verbunden ist die Gefahr des Datenmissbrauchs. Das Datenschutzgesetz sieht deshalb vor, dass der Regierungsrat bezüglich des Abrufverfahrens eine spezielle gesetzliche Regelung zu schaffen hat. Diese Verordnung hätte bis Ende 2001 in Kraft gesetzt werden müssen[56] – bis dato ist diesbezüglich noch nichts unternommen worden.

Datensammlung der Einwohnerkontrolle
Bei der Datensammlung der Einwohnerkontrolle handelt es sich um eine *gemeindliche* Datensammlung. Datenherrin ist somit die Gemeinde, die im Rahmen der Rechtsordnung über Bekanntgabe und Modalitäten entscheidet. Dass diese Datensammlung für alle Gemeinden zentralisiert durch den kantonalen Informatik-Dienstleister betreut wird, hat diesbezüglich keine Bedeutung. Es handelt sich dabei um eine ausgelagerte Datenbearbeitung.

Zum gemeindlichen Bewilligungsverfahren
Verfügt die Gemeinde über eine eigene kommunale gesetzliche Grundlage bezüglich Online-Zugriff, so ist diese anwendbar.[57] Liegt keine gemeindliche gesetzliche Grundlage vor, so hat der Gemeinderat im Einzelfall selber über Gesuche um Online-Zugriffe zu entscheiden.

Checkliste der Rahmenbedingungen des Online-Zugriffs:
- Erste Voraussetzung ist, dass die Datenbekanntgabe an die anfragende Stelle im geforderten Rahmen an und für sich – via mündliche oder schriftliche Anfrage – zulässig ist.
- Falls die Datenbekanntgabe mit herkömmlichen Mitteln[58] genügt, ist *kein* Abrufverfahren einzurichten.
- Der Umfang des Zugriffs auf die einzelnen Datenkategorien ist zurückhaltend zu definieren. Informationen, die nur sehr selten benötigt werden, sind auf dem herkömmlichen Weg [schriftlich oder telefonisch] zu beschaffen.
- Es sind grundsätzlich nur Einzel-, nicht aber Sammelanfragen möglich.
- Damit gewährleistet ist, dass nur geschäftsrelevante Abfragen erfolgen, werden zwingend gewisse minimale Eingaben benötigt,[59] ohne die keine Abfrage vorgenommen werden kann.
- Die Abfragemöglichkeit ist auf einen eng beschränkten Personenkreis mit persönlicher User-ID zu beschränken. In der Regel genügen zwei Personen [Haupt-User und Stellvertretung]. Die berechtigten Personen sind dem Datenherrn namentlich zu melden.
- Die zugeteilte User-ID ist eine technische und organisatorische Massnahme gegen Einsichtnehmen durch Unberechtigte. Die User-ID darf nicht an andere Personen weiter gegeben werden.
- Jede Abfrage muss automatisch protokolliert werden.
- Die Protokollierung aller Abfragen [Log-Files] sowie eine Auswertung dieser Protokolle sind dem Datenherrn einmal jährlich unaufgefordert zur Kontrolle zuzustellen.
- Die Daten dürfen ausschliesslich für die Erfüllung der Aufgaben des Datenbezügers verwendet werden. Sie dürfen somit für keinerlei bearbeitungsfremde oder private Zwecke verwendet werden.
- Es dürfen keine Auskünfte über bezogene Personendaten an Dritte erteilt, keine Personendaten an solche weiter gegeben, auf andere Weise Dritten zugänglich gemacht oder veröffentlicht werden.
- Es muss eine Risikobeurteilung in technischer Hinsicht vorgenommen werden. Es sind Sicherheitsmassnahmen zu ergreifen, damit der Zugriff in jeder Hinsicht sicher ist.
- Falls der Zugang nicht in einer gesicherten Netzwerkumgebung realisiert wird, muss der Datenzugriff *verschlüsselt* erfolgen.
- Beim Zugriff auf besonders schützenswerte Daten sind entsprechend zusätzliche Massnahmen zu ergreifen.
- Wird ein Abrufverfahren eingerichtet, so fallen Kosten an. Es ist zu regeln, wer diese zu tragen hat.

Fazit: Da der Datenherr durch den Online-Zugriff in der Praxis *jegliche Kontrolle* über seine Daten verliert, sind Abrufverfahren zurückhaltend, kritisch und nur in sorgfältig abgestecktem Rahmen zuzulassen.
Werden diese Vorgaben und Rahmenbedingungen erfüllt, so sind durchaus auch positive Aspekte zu

54 Im Rahmen der definierten Zugriffsberechtigung.

55 Werden die Zugriffe edv-mässig aufgezeichnet [sogenannte Log-Files], so kann immerhin im Nachhinein eine Kontrolle ausgeübt werden. Die Auswertung solcher Zugriffsaufzeichnungen ist jedoch sehr arbeitsintensiv. In der Praxis werden solche Überprüfungen deshalb denn auch kaum je vorgenommen.

56 § 7 Abs. 2 Datenschutzgesetz.

57 Die Gemeinden Hünenberg und Neuheim haben beispielsweise solche Verordnungen geschaffen, Näheres dazu siehe vorne S. 7.

58 Mündliche, schriftliche Auskünfte; regelmässige Zustellung auf Datenträger.

59 Zum Beispiel: Name, Vorname, Geburtsdatum der betroffenen Person.

sehen. Es kann grundsätzlich die Qualität der Datenbearbeitung verbessert werden, da auf aktuelle und richtige Daten zugegriffen wird, zudem Übermittlungsfehler ausgeschlossen werden.

Der DSB wurde beim Erlass der gemeindlichen Online-Verordnung der Gemeinden Hünenberg und Neuheim[60] sowie bei den Gesuchen des Einzelrichteramtes, des Rettungsdienstes Zug sowie des Amtes für Militär beigezogen.

Fall 9 Büroumzug einer Verwaltungsstelle – was ist zu beachten?

Eine Verwaltungsstelle, die einen Büroumzug zu organisieren hat, erkundigt sich, ob sie alle ihre Akten zu versiegeln hat bzw. ob es diesbezüglich besondere gesetzliche Vorschriften gibt. Letzteres ist zu verneinen. Ein Grundsatz des Datenschutzgesetzes verlangt von der Verwaltung jedoch, dass ihre Daten insbesondere vor Verlust, Entwendung oder Kenntnisnahme zu schützen sind.[61] Der Umzug ist so zu organisieren, dass weder Umzugspersonal noch Dritte Kenntnis von den Akten nehmen können. Besonders sensible Akten sind in verschliessbaren Behältnissen zu transportieren und von einer Person der Verwaltung lückenlos zu begleiten.

1.3 Auslagerung von Verwaltungsaufgaben

Vorbemerkung

Verschiedene Gründe führen dazu, dass die Verwaltung je länger, je häufiger, *Private* mit der Erfüllung öffentlicher Aufgaben betraut. Dieser Trend kann auch direkt aus den Anfragen, die beim DSB eingehen, abgelesen werden. Im Folgenden wird dieser Begriff *sehr breit* verstanden. Miteingeschlossen ist jede Tätigkeit, die nicht selber durch die öffentliche Verwaltung erledigt wird. Auf das Rechtsverhältnis zwischen der Verwaltung und der externen Stelle wird nicht geachtet. Eingeschlossen sind somit Aufträge, Leistungsverträge und gegebenenfalls Subventionierungen.

Fall 10 Ist Auslagerung überhaupt mit dem Datenschutzgesetz vereinbar?

Grundsätzlich kennt das Datenschutzgesetz das Thema der Auslagerung, regelt es doch in verschiedenen Bestimmungen die ausgelagerte Datenbearbeitung.[62] Es schliesst die Auslagerung von Datenbearbeitung dann aus, wenn gesetzliche oder vertragliche Geheimhaltungspflichten es verbieten. Ist Auslagerung zulässig, darf dadurch für die Bürgerinnen und Bürger keine Verschlechterung in ihren Rechten resultieren. Die Externen dürfen die Daten nicht anders bearbeiten, als es die Verwaltung selbst tun dürfte. Sämtliche Rechtsansprüche der Bürger richten sich nach wie vor direkt gegen die Verwaltung – und nicht etwa an die Beauftragten. Auch die Aufsicht des DSB wird durch die Auslagerung nicht tangiert. Im ausgelagerten Bereich untersteht der Externe den Aufsicht- und Kontrollbefugnissen[63] des DSB.

Fall 11 Regelwerk «Leistungsvereinbarungen mit privaten Dritten»

Der Regierungsrat hat im Dezember 2003 ein Regelwerk bezüglich «Leistungsvereinbarungen mit privaten Dritten» verabschiedet. Dieses kommt grundsätzlich zwingend bei jeder Leistungsvereinbarung, die eine Verwaltungsstelle mit Externen abschliesst, im Sinne eines verbindlichen Standardvertrags zur Anwendung. Der DSB hat die Bereiche Datenschutz und Datensicherheit konzipiert. Zusätzlich hat er dazu einen ergänzenden Anhang «Datenschutz und Datensicherheit» verfasst. Wichtig ist auch, wie die Dritten mit den Daten zu verfahren haben, die nicht mehr benötigt werden – die Frage von Anonymisierung, Vernichtung oder Archivierung ist angesprochen.[64] Diesen Bereich hat das Staatsarchiv betreut, das einen ergänzenden Anhang zur Archivierung verfasst hat.
Dieser Standardvertrag bringt eine Vereinheitlichung, die als sehr positiv zu beurteilen ist. Sie vereinfacht, verbessert und klärt die Rechtslage im Verhältnis zu den Leistungserbringern. Die grundlegenden Anforderungen in den Bereichen Datenschutz und Datensicherheit sind nun klar und verbindlich festgehalten.
Da nicht nur der Kanton, sondern auch die Gemeinden Leistungsvereinbarungen abschliessen, wäre es sehr zu begrüssen, wenn auch die Gemeinden diese Musterverträge übernehmen würden.

Fall 12 Servicearbeiten an PC und EDV-Anlagen

Für solche Arbeiten werden sehr häufig private Firmen beigezogen. Ob der Auftrag bei der Verwaltung vor Ort oder aber extern bei der Firma ausgeführt wird, oft besteht die Gefahr, dass Externe Kenntnis von besonders schützenswerten Daten von Bürgerinnen und Bürgern erhalten.

60 Siehe dazu vorne S. 7.

61 § 7 Abs. 1 Datenschutzgesetz.

62 § 6, § 14 und § 24 Datenschutzgesetz.

63 Gemäss § 19 und § 20 Datenschutzgesetz.

64 § 11 Datenschutzgesetz.

Organisatorisch und technisch muss diese Gefahr so weit als möglich minimiert werden. Muss der PC oder Laptop in den Service, sind die Daten vorgängig, wenn immer möglich, zu entfernen. Bei Arbeiten an Servern sind die Zugriffsrechte auf das notwendige Minimum zu beschränken.
Es kann jedoch selten erreicht werden, dass EDV-Auftragnehmer nicht Einsicht in Daten nehmen können. In einem zweiten Schritt sind deshalb *vertragliche* Absicherungen zu treffen. Die Firma und alle für den Auftrag eingesetzten Mitarbeitenden haben eine *Verpflichtungserklärung* zu unterzeichnen. Darin wird vertraglich die Geheimhaltungspflicht umschrieben und auf zivilrechtliche und strafrechtliche[65] Sanktionen bei Verstössen hingewiesen. Sinnvoll ist die Sicherung der Verpflichtungserklärung durch eine Konventionalstrafe.
Es ist denkbar, dass gewisse Aufgaben aus Sicherheitsgründen zwingend nur durch Verwaltungspersonal ausgeführt werden dürfen, andere nur unter direkter Aufsicht von Verwaltungspersonal vor Ort.[66]

Der DSB hat auf seiner Website [Rubrik «Kanton Zug/Aktuelles»] eine Muster-Verpflichtungserklärung veröffentlicht.

Fall 13 Wenn externe Experten auf die Kenntnisse von vertraulichen Dokumenten angewiesen sind

Werden externe Experten für Gutachten, Analysen von Verwaltungsstellen oder bei Gesetzgebungsprojekten eingesetzt, erhalten sie dadurch zwingend Einsicht in sensible Daten. Auch hier gilt: Die Möglichkeit der Kenntnisnahme ist auf das notwendige Minimum zu beschränken, so weit als möglich sind Unterlagen zu anonymisieren und durch die Unterzeichnung einer Verpflichtungserklärung sind die vertraglichen Abmachungen zu sichern. Zur Kommunikation mit Externen siehe den nächsten Fall.

Fall 14 Kommunikation per E-Mail mit Externen?

Die unverschlüsselte Kommunikation per E-Mail via Internet ist in jeder Hinsicht unsicher. Den Mitarbeitenden der Verwaltung ist es deshalb aus Sicherheitsgründen untersagt, Personendaten oder vertrauliche Sachdaten unverschlüsselt per Internet-E-Mail zu versenden.[67] Diese Vorschrift ist direkt auch auf externe Beauftragte anwendbar.

Fazit: Entweder ist demnach keine E-Mail-Kommunikation zulässig, oder es ist für den Datenaustausch mit Externen verschlüsselte Kommunikation vorzusehen. Entsprechende Tools sind auf dem Markt für wenig Geld erhältlich.

Fall 15 Auslagerung – ist die Zustimmung der Betroffenen erforderlich?

Ist die Auslagerung der Aufgabe an und für sich zulässig und wird sie gemäss den anwendbaren Vorschriften umgesetzt, so benötigt die auslagernde Verwaltungsstelle nicht zusätzlich noch die Zustimmung der betroffenen Personen, damit der Beauftragte im Rahmen der Auftragserfüllung deren Daten bearbeiten darf.

Fall 16 In welchem Umfang sind dem Beauftragten Daten zuzustellen?

Bei zulässiger und rechtmässiger Auslagerung sind dem Beauftragten sämtliche für die Erfüllung der Aufgabe erforderlichen Daten zur Verfügung zu stellen. Nicht mehr – aber auch nicht weniger. Die Rechtslage unterscheidet sich somit grundsätzlich nicht von derjenigen, bei der die entsprechende Verwaltungsstelle die Aufgabe selber erledigt.

Fall 17 Auslagerung von Druckaufträgen durch die Steuerverwaltung?

Bis anhin wurden sämtliche bei der Steuerverwaltung anfallenden Massenversände *verwaltungsintern* gedruckt und verpackt. Neu sollen diese Druckaufträge an ein *privates Unternehmen* ausgelagert werden. Bei den zu druckenden Dokumenten handelt es sich etwa um Eröffnung der Hauptveranlagung, Begründung von Veranlagungen, Abrechnung der Quellensteuer, Einspracheentscheide, Rückerstattungsentscheide, Rechnungen, Mahnungen und Steuerausscheidungen usw.
Zusammengefasst[68] wies der DSB in seiner Stellungnahme an den Regierungsrat darauf hin, dass es sich bei der vorliegenden Datenbearbeitung um einen in jeder Beziehung *äusserst sensiblen* Bereich handelt. Einerseits, was die einzelnen Daten selber betrifft, andererseits auch, was mögliche Folgen von Fehlmanipulationen, Kenntnisnahme durch Unbefugte oder gar absichtliche Schädigungen betrifft. Er empfahl und stellte fest, dass:

- die vorliegende Datenbearbeitung, wenn immer möglich, wie bis anhin verwaltungsintern zu erledigen sei;

65 § 24 Datenschutzgesetz sowie gegebenenfalls Art. 320 Strafgesetzbuch.

66 Zu denken ist etwa an heikle Bereiche bezüglich Polizei, Gesundheit oder Steuern usw.

67 § 3 Verordnung über die Benutzung von elektronischen Kommunikationsmitteln im Arbeitsverhältnis [BGS 154.28].

68 Die ausführliche Stellungnahme ist in GVP 2003 veröffentlicht.

- die Auslagerung nur rechtmässig ist, wenn der Auftrag umfassend in der Schweiz abgewickelt wird;
- der Anbieter sich bezüglich den Aspekten Datensicherheit und Datenschutz auf die Zürcher «AGB Sicherheit» verpflichtet.

Die zuständige Direktion hat sich in der Folge Ende Jahr gegen die Auslagerung entschieden.

Fall 18 Wie dürfen die Beauftragten kontrolliert werden?

In welche Unterlagen darf die Gemeinde bei den Institutionen Einblick nehmen, denen sie mit einem Leistungsvertrag die Führung der Kinderkrippe oder des Mittagstischs übertragen hat?
Kontrolle und Überwachung sollten im Leistungsvertrag ausdrücklich definiert werden. Ist dies nicht der Fall, so ist davon auszugehen, dass zu anonymisierten Unterlagen unbeschränkter Zugang zu gewähren ist. Jedenfalls im Rahmen von Stichproben ist Einsicht in nicht anonymisierte Unterlagen ebenfalls möglich. Systematische Kontrolle und Überwachung widersprechen an und für sich der Auslagerung, sind aber in besonderen Umständen und falls sachlich begründet, nicht auszuschliessen.

Fazit: Grundsätzlich bearbeitet der Beauftragte Daten für bzw. an Stelle der Verwaltung. Diese bleibt somit grundsätzlich Datenherrin. Sie muss sich, soweit sachlich notwendig, auch ein vertieftes Bild machen können.

1.4 Arbeitsrechtliches

Fall 19 Kann die Steuerbehörde den Lohnausweis beim Arbeitgeber verlangen?

Eine gemeindliche Steuerbehörde verlangte vom kantonalen Personalamt den Lohnausweis eines Mitarbeiters der kantonalen Verwaltung. Ist dies zulässig?
Der Arbeitgeber ist aufgrund des Steuergesetzes verpflichtet, dem Mitarbeitenden einen Lohnausweis abzugeben.[69] Der Steuerpflichtige seinerseits hat alles zu tun, um eine vollständige und richtige Veranlagung zu ermöglichen.[70] «Reicht die steuerpflichtige Person trotz Mahnung die nötigen Bescheinigungen nicht ein, so kann die Veranlagungsbehörde diese vom Dritten einfordern.» Dies sieht das Steuergesetz ausdrücklich vor.[71]

Fazit: Nach erfolgter Mahnung kann die gemeindliche Steuerbehörde somit den Lohnausweis beim Arbeitgeber einfordern. Zu betonen ist, dass es hier nur um die Zustellung des Lohnausweises geht. Eigentliche Auskünfte über den Steuerpflichtigen dürfen hingegen beim Arbeitgeber nicht eingeholt werden.

Fall 20 Nutzung des Telefons in der kantonalen Verwaltung – wird mitgehört?

Die Telefonzentrale der kantonalen Verwaltung liess das sogenannte «Aufschalten» zu. Dadurch war es der Telefonistin möglich, sich in ein laufendes Telefongespräch aufzuschalten und so, wie bei einem Konferenztelefongespräch, als dritte Partei am Gespräch teilzunehmen.
Beschweren sich beispielsweise Anrufende bei der Zentrale, dass ein bestimmter Anschluss ständig besetzt ist, konnte die Telefonistin prüfen, ob etwa der Hörer des betreffenden Anschlusses nicht richtig aufgelegt war oder ob der Hörer einfach auf dem Tisch lag, während sich der Mitarbeiter an einer Sitzung befand. In privaten Unternehmen haben die Telefonistinnen teilweise auch den Auftrag, mittels Aufschalten interne Gespräche zu unterbrechen, weil Kundschaft den Mitarbeitenden zu sprechen wünscht.
Von verschiedenen Mitarbeitenden der Verwaltung wurde der Verdacht geäussert, dass sich die Zentrale in laufende Gespräche aufschalte und geschäftliche oder private Gespräche mithöre – was die Technik denn auch tatsächlich zuliess. Anzumerken ist, dass beim und während des Aufschaltens ein gewisses akustisches Signal zu hören war. Wem dieses jedoch nicht bekannt war, schenkte dem keine Bedeutung oder nahm an, die Verbindung mit dem Gesprächspartner sei etwas schlechter als gewöhnlich. Insbesondere bei einer Verbindung mit einem mobilen Telefon hätte unbemerkt aufgeschaltet werden können.
Im letzten Jahr wurde an dieser Stelle angekündigt, dass der Regierungsrat die Nutzung des Telefons am Arbeitsplatz für die gesamte kantonale Verwaltung regeln wird.[72] Dieser Beschluss ist im September 2003 verabschiedet worden.[73] Er sieht ausdrücklich vor, dass weder Systembetreiber, noch vorgesetzte Stellen, noch Dritte Gespräche abhören oder aufzeichnen dürfen.[74] Da jegliche Überwachung verboten ist, ist auch die Möglichkeit des Abhörens mit technischen Massnahmen auszuschliessen.

69 § 128 Abs. 1 Bst. a Steuergesetz [BGS 632.1].

70 § 125 und § 127 Steuergesetz.

71 § 128 Abs. 2 Steuergesetz.

72 DSB TB 2002 S. 23.

73 Er steht auf der DSB-Website [Rubrik «Kanton Zug/Gesetze»] zur Verfügung.

74 Vorbehalten sind die besonderen Dienste Tel. 117, 118, 144 sowie Überwachung im Rahmen von Strafverfahren.

Im Oktober 2003 wurde die Funktion des Aufschaltens ausser Betrieb gesetzt. Damit ist der Beschluss des Regierungsrates, der den Schutz der Privatsphäre der Mitarbeitenden der Verwaltung bei der Nutzung des Telefons statuiert, umgesetzt – und gleichzeitig der unschöne, bisher auf der Telefonzentrale lastende «Generalverdacht» des Abhörens laufender Gespräche ein für allemal aus der Welt geschafft.

Fall 21 Auditverfahren – Personaldossier verlässt das Büro des Arbeitgebers nicht

Die Anfrage an den DSB in dieser Sache kam von einem privaten Arbeitgeber, könnte sich aber auch bei der öffentlichen Verwaltung abspielen: Im Rahmen eines Audits verlangte die externe Prüfstelle vom privaten Arbeitgeber die Herausgabe der Personaldossiers zur Überprüfung, ob die Mitarbeitenden die geforderten Voraussetzungen erfüllten.
Das Personaldossier enthält teilweise sehr sensible Daten.[75] Übergibt der Arbeitgeber das ganze Dossier an externe Dritte ausser Haus, hat er keinerlei Kontrolle, was damit geschieht. Dies insbesondere dann, wenn die Unterlagen in elektronischer Form herausgegeben werden.
Ohne Zustimmung des betroffenen Mitarbeiters darf es deshalb nicht an Dritte ausser Haus gegeben werden. Die vorgesehene Prüfung hat vielmehr unter Aufsicht des Arbeitgebers in seinen Büroräumlichkeiten zu erfolgen. Zudem sind aufgrund des Verhältnismässigkeitsprinzips nur jene Dokumente vorzulegen, die einen direkten Bezug zur Auditierung haben.
Dieses Vorgehen ist auch dann zu wählen, wenn die Prüfstelle und deren Fachexperten sich vertraglich zur Geheimhaltung verpflichtet haben.

Fall 22 Wird der PC der Mitarbeitenden der Verwaltung überwacht?

Verschiedene Verwaltungsmitarbeitende haben via E-Mail Angebote für sogenannte «Spy-Software» erhalten. Gemäss dem Werbetext kann damit via Internet im Verborgenen jeder Tastaturklick eines damit überwachten PC aufgezeichnet und ausgewertet werden.[76]
Vorweg stellte sich die Frage, ob der Handel mit dieser Software in der Schweiz überhaupt zulässig sei. Dies ist zu bejahen, ist doch – jedenfalls theoretisch – nicht auszuschliessen, dass auch ein legaler Einsatz möglich ist. So beispielsweise, wenn die Software auf dem eigenen PC installiert wird oder eine rechtskonforme Zustimmung des Überwachten vorliegt.
Der Einsatz ohne Zustimmung des Betroffenen ist hingegen klar unzulässig. Ein Verstoss dagegen kann strafrechtlich und zivilrechtlich verfolgt werden. Allerdings wird der Nachweis des Spionierens aus technischen Gründen wohl nicht leicht zu führen sein.

Fazit: Ohne Wissen des betroffenen Mitarbeiters ist der Einsatz von Spionier-Programmen sowohl in der öffentlichen Verwaltung wie auch an jedem anderen Arbeitsplatz in der Schweiz verboten.[77]

Fall 23 Regelung der Nutzung von E-Mail und Internet am Arbeitsplatz

Für die Mitarbeitenden der kantonalen Verwaltung hat der Regierungsrat Ende 2002 eine entsprechende Verordnung erlassen.[78] Verschiedene Gemeinden sind dem Beispiel gefolgt und haben analoge Regelungen für ihre Mitarbeitenden getroffen. Anders als beim Kanton haben die Gemeinden jedoch verordnet, dass die Kenntnisnahme der neuen Bestimmungen durch die Mitarbeitenden *unterschriftlich* zu bestätigen ist. Dies ist zu begrüssen, weil dadurch die Rechtssicherheit verstärkt wird.

Fall 24 Heikle Fragen rund um das Arbeitszeugnis

Ist der frühere Arbeitgeber berechtigt oder gar verpflichtet, dem neuen Arbeitgeber *unaufgefordert* Informationen über seinen früheren Mitarbeiter bekannt zu geben?
Bei Angaben aus dem Personaldossier handelt es sich in der Regel um besonders schützenswerte Daten bzw. um ein Persönlichkeitsprofil. Diese dürfen nur bekannt gegeben werden, wenn diesbezüglich eine gesetzliche Grundlage vorliegt. Dies ist im vorliegenden Fall nicht gegeben. Ohne Zustimmung der betroffenen Person ist der frühere Arbeitgeber deshalb grundsätzlich weder verpflichtet, noch berechtigt, dem neuen Arbeitgeber *unaufgefordert* Daten aus dem früheren Arbeitsverhältnis bekannt zu geben.

Fall 25 Stellenvermittlung arbeitsloser Personen im Internet

Eine private Institution, die weitgehend durch die öffentliche Hand finanziert wird, bietet arbeits-

75 Gesundheitsangaben, Qualifikationsberichte, Bewerbungsdossier, Konkurrenzverbot usw.

76 Der Werbetext besagt: «'PC Surveillance' ist die erste und einzige Spion-Software, die ortsunabhängig und in Echtzeit eingesetzt werden kann. Sie gibt Ihnen die Möglichkeit, weltweit und rund um die Uhr beliebige PC in Echtzeit auszuspionieren. Sie können dadurch Passwörter und Benutzernamen, E-Mail-Verkehr, Chat-Unterhaltungen und sämtliche Tastaturbewegungen völlig unbemerkt aufzeichnen. Dieses Spion-Programm arbeitet auf dem Ziel-Computer stets vollständig verborgen und kann somit vom betroffenen Nutzer nicht entdeckt werden.»

77 Siehe dazu auch EDSB-Tätigkeitsbericht 2002/2003, S. 61/62.

78 Verordnung über die Benutzung von elektronischen Kommunikationsmitteln im Arbeitsverhältnis [E-Mail und Abruf von Webseiten] [BGS 154.28].

losen Personen unter anderem die Möglichkeit, kostenlos ihre Stellenbewerbung im Internet zu veröffentlichen. Es stellt sich die Frage, wie der Schutz der Privatsphäre der arbeitslosen Stellenbewerbenden zu gewährleisten ist. Es ist darauf hinzuweisen, dass arbeitslose Personen unter Umständen mit schweren Nachteilen rechnen müssen, sollte ihre momentane Situation in weiten Kreisen bekannt werden. Die rechtmässige Umsetzung dieses Web-Angebots liegt in erster Linie in der Verantwortung der Institution. Sie hat dafür zu sorgen, dass die Privatsphäre der Betroffenen nicht verletzt werden kann.

Es ist konsequent, auf die Publikation von Fotos zu verzichten. In kleinräumigen Verhältnissen geht die Veröffentlichung eines Fotos mit dem Verzicht auf Anonymität einher. Werden von Stellenbewerbenden Fotos veröffentlicht, von anderen hingegen nicht, fragt sich der Betrachter nach dem Grund der unterschiedlichen Handhabung.

Sollen die jeweiligen Stellensuchenden direkt per E-Mail angeschrieben werden können, hat die Institution dafür zu sorgen, dass Mail-Adressen verwendet werden, die keine direkten Hinweise auf den Stellenbewerbenden geben.

1.5 Einbürgerung

Vorbemerkungen: Zur Datenbearbeitung im Einbürgerungsverfahren

Auch dieses Jahr gingen beim DSB wieder sehr viele Anfragen zum Datenschutz beim Einbürgerungsverfahren ein. Dies erstaunt nicht, stellen sich doch hier in der Tat sehr viele heikle Fragen in Sachen «Privacy». Zudem stellt es allen mitbeteiligten Behördenmitgliedern ein sehr gutes Zeugnis aus, zeigt es doch, dass sie sensibilisiert sind, dass ihnen klar bewusst ist, auf welcher Gratwanderung sie sich bei der Datenbearbeitung befinden. Die entsprechenden Hinweise des DSB stiessen auf offene Ohren.

Im Einbürgerungsverfahren stellen sich insbesondere die beiden folgenden Fragen: Welche Daten darf der Bürgerrat über die einbürgerungswillige Person und sein Umfeld erheben? Welche Daten dürfen der Gemeindeversammlung bekannt gegeben werden?

Es ist hier nicht der Ort, näher auf die Frage einzugehen, ob die bundesrechtlichen und die kantonalen Rechtsgrundlagen vor der Bundesverfassung und der Europäischen Menschenrechtskonvention standhalten – ein Literaturhinweis dazu möge genügen.[79] Es ist auch nicht der Ort, die Frage zu stellen, ob für das Einbürgerungsverfahren in der Schweiz die richtigen Konzepte und Verfahren eingesetzt werden. In Anbetracht der aktuellen Praxis des Bundesgerichts ist hier der Gesetzgeber gefordert.

Ein Hinweis zum Geltungsbereich des Datenschutzgesetzes: Im Kanton Zug ist das Datenschutzgesetz auf die gesamte Datenbearbeitung des Verfahrens selber, somit auf die Datenerhebung durch den Bürgerrat und die beauftragten Verwaltungsstellen sowie die befassten Stellen der Direktion des Innern *uneingeschränkt* anwendbar. Hingegen ist es nicht [direkt] anwendbar auf das Abstimmungsverfahren, somit auf die Datenbekanntgabe an die Gemeindeversammlung.[80] Dies hat jedoch nicht zur Folge, dass diesbezüglich keine Regelung vorhanden wäre, muss doch die Privatsphäre der Einbürgerungswilligen auch hier geachtet werden – im Rahmen der allgemeinen verfassungs-, verwaltungs- und datenschutzrechtlichen Grundsätze.

Fall 26 Dürfen nur gesunde Ausländer Schweizer werden?

Einbürgerungswillige mussten im Rahmen des Lebenslaufs nähere «Angaben über Krankheiten, Unfälle, Folgen» machen. Zudem mussten sie einen Fragebogen mit den folgenden vier Fragen ausfüllen: «Fühlen Sie sich gegenwärtig völlig gesund und leistungsfähig? Bestanden oder bestehen bei Ihnen schwere gesundheitliche Störungen? Mussten Sie jemals während mehr als vier Wochen mit der Arbeit aus gesundheitlichen Gründen aussetzen? Beziehen oder bezogen Sie Leistungen der IV?»

Fragen zur Gesundheit sind im Einbürgerungsverfahren grundsätzlich als *unzulässig* zu betrachten. Gemäss Bürgerrechtsgesetz haben jedoch die Einbürgerungswilligen geordnete finanzielle Verhältnisse nachzuweisen.[81] Es kann deshalb von einer *gewissen Grauzone* gesprochen werden, sofern der Gesundheitszustand direkte und massive Auswirkungen auf die «geordneten finanziellen Verhältnisse» haben könnte.

Da dies in der Regel jedoch nicht der Fall ist, sind Fragen zur Gesundheit grundsätzlich unzulässig. Die betreffende Bürgergemeinde hat den Fragebogen in der Folge auch diskussionslos zurückgezogen.

79 Yvo Hangartner, Grundsätzliche Fragen des Einbürgerungsrechts, AJP/PJA 8/2001, S. 949–967, mit vielen weiterführenden Literaturhinweisen.

80 § 3 Abs. 2 Bst. b Datenschutzgesetz.

81 § 5 Bürgerrechtsgesetz [BGS 121.3].

Fall 27 Dauerbrenner – welche Daten dürfen an der Bürgerversammlung bekannt gegeben werden?

Wie einleitend bereits angemerkt, ist das Datenschutzgesetz auf die Datenbekanntgabe an die Bürgerversammlung nicht anwendbar. Das Verfassungsrecht sowie die allgemeinen Grundsätze des Verwaltungsrechts müssen eingehalten werden. Im Vordergrund steht das Verhältnismässigkeitsprinzip. Folglich sind so wenige Informationen wie möglich bekannt zu geben – um den Schutz der Privatsphäre der Betroffenen zu wahren –, jedoch auf der anderen Seite so viel wie nötig, damit die Stimmberechtigten überhaupt einen plausiblen Entscheid treffen können. Durch die viel zitierten Entscheide des Bundesgerichts[82] in diesem Jahr ist die Sache nicht einfacher geworden, muss doch der Entscheid der Gemeindeversammlung im Ablehnungsfall *begründet* werden. Dies kann aber nur dann gewährleistet werden, wenn die Versammlung über ein minimales Wissen verfügt. Es ist somit stets eine heikle Abwägung zwischen Offenlegung und Persönlichkeitsschutz zu treffen.

Fall 28 Zu den Abklärungen bezüglich der finanziellen Verhältnisse

Das Bürgerrechtsgesetz sieht vor, dass die finanziellen Verhältnisse abzuklären sind. Darf der Bürgerrat die entsprechenden Daten bei der Steuerbehörde erfragen?

Nein – die Steuerbehörden dürfen aufgrund des Steuergeheimnisses auch an andere Organe *keinerlei* Auskünfte bezüglich Einkommen und Vermögen erteilen. Der Steuerausweis ist durch die Einbürgerungswilligen selber zu beschaffen und anschliessend dem Bürgerrat vorzulegen. Bei ausländischen Einbürgerungskandidaten ist er auch für die Festlegung der Einbürgerungstaxe notwendig.

Sollten die Kandidaten übrigens der Aufforderung zur Einreichung des Steuerausweises nicht nachkommen, so erhielte deshalb der Bürgerrat nicht die Möglichkeit, nun direkt bei der Steuerbehörde anzufragen. Vielmehr ist das Verfahren zu sistieren, bis die notwendigen Unterlagen vorliegen.

1.6 Schule

Fall 29 Datenschutz in der Schule – hier erhalten Sie die wichtigsten Informationen

Im Bereich der Schulen werden sehr viele, zum Teil auch sehr heikle Daten bearbeitet – so etwa: Beurteilungen von Schülerinnen und Schülern bezüglich Leistung und Leistungsverhalten, Angaben zum persönlichen Umfeld und Elternhaus, zu Religion und zu Gesundheit. Wer von welchen Daten Kenntnis haben darf, ist oft nicht einfach zu beurteilen. Gelangen Informationen über ein Kind oder einen Jugendlichen, dessen Eltern oder andere Bezugspersonen an Unberechtigte, können gravierende Persönlichkeitsverletzungen resultieren. Dies kann für die fehlbare Person disziplinarische, zivilrechtliche oder auch strafrechtliche Folgen haben. Der rechtmässige Umgang mit den Daten des Schulbereichs ist somit für alle Beteiligten ein *zentrales* Anliegen.

Die Direktion für Bildung und Kultur hat deshalb zusammen mit dem Datenschutzbeauftragten die Broschüre «Datenschutz – Leitfaden für die Schule im Kanton Zug» verfasst. Zielpublikum sind in erster Linie Lehrpersonen – auch aus den Bereichen Logopädie und Psychomotorik - und Schulleitungen, aber auch Eltern. Praxisbezogen und gut verständlich wird auf sieben Seiten kurz und knapp über die wichtigsten Grundsätze informiert.[83] Der Leitfaden kann kostenlos beim DSB bezogen werden und steht layoutgetreu auch auf der Website[84] des DSB zur Verfügung.

Fall 30 Wenn der Schüler Bäcker werden will …

Ein Schüler, der Bäcker werden will, darf nicht an einer Mehl-Allergie leiden. Kann sich der zukünftige Lehrmeister direkt beim Schul- oder Hausarzt erkundigen, ob beim Lehrling möglicherweise eine Mehl-Allergie vorliegt?

Nein – ohne entsprechenden Auftrag des Schülers oder dessen Eltern darf der Arzt keinerlei Informationen über den Gesundheitszustand seiner Patienten an Dritte weitergeben. Falls er dies trotzdem tut, ist zu prüfen, ob eine Verletzung des Berufsgeheimnisses vorliegt, was strafbar ist.[85]

Wie richtigerweise vorzugehen ist: Der mögliche zukünftige Lehrmeister spricht den Lehrling bei Vorliegen gewisser Anhaltspunkte auf das Problem

82 BGE 129 I 217 [betr. Emmen] und BGE 129 I 232 [betr. SVP-Initiative in der Stadt Zürich].

83 Der Leitfaden behandelt die Vorgänge Datenerhebung, Datenbearbeitung, Datenvernichtung, Datenarchivierung und gibt grundlegende Hinweise zur Datensicherheit.

84 Rubrik «Kanton Zug/Aktuelles».

85 Art. 321 Strafgesetzbuch.

der Mehl-Allergie an und bittet ihn, eine entsprechende ärztliche Abklärung vornehmen zu lassen. Den ärztlichen Befund erhält aber der Lehrmeister nicht direkt durch den Arzt, vielmehr hat der Lehrling selber Rückmeldung zu erstatten.

Fall 31 Die papierlose Schule – Bekanntgabe des Prüfungsresultats via Internet?

Wie können Lehrlinge schnell, einfach und günstig über Erfolg oder Misserfolg bei der Lehrabschlussprüfung informiert werden? Heutzutage ist die Antwort klar – via Internet!

So ist vorzugehen, damit die Privatsphäre der Lehrlinge geschützt ist:

- der entsprechende Bereich der Schul-Website ist nicht öffentlich zugänglich; Zugang hat nur, wer über das entsprechende Passwort verfügt;
- der Lehrling hat nur Zugang zu seinen eigenen Informationen, nicht aber auf die seiner Klasse oder gar der ganzen Schule;
- die Information beschränkt sich auf «bestanden/nicht bestanden», es sind keine weiteren Details anzuführen;
- zentral ist ein sicherer Passwortschutz: der Zugang kann durch die persönliche Kandidatennummer und eine zusätzliche Angabe zur Person, etwa das Geburtsdatum, gewährt werden. Die persönliche Kandidatennummer sollte aus mindestens sechs Ziffern in Kombination mit Buchstaben bestehen und muss willkürlich vergeben werden. Die Lehrlinge dürfen somit von ihrer eigenen Nummer nicht auf diejenige der Kolleginnen und Kollegen schliessen können. Es darf sich auch nicht um eine «sprechende» Nummer handeln;[86]
- um «Hacker-Angriffe» und andere Missbräuche zu vereiteln, ist der Zugang zu den Informationen nach höchstens zehn erfolglosen Versuchen definitiv zu sperren.

Der ausführliche Bescheid über den Erfolg ist natürlich nach wie vor per Post zu verschicken, handelt es sich doch um eine Verfügung, welche entsprechende Rechtswirkungen auslöst, nicht zuletzt etwa das Rekursrecht bei Misserfolg.

Ergänzender Hinweis: Dass heute jeder Lehrling Zugang zum Internet hat, ist offenbar vorausgesetzt …

Fall 32 Welche Informationen gehören auf den Studentenausweis?

Eine Hochschule gibt einen Studentenausweis heraus. Welche Angaben soll er enthalten? Ausreichend sind: Foto, Name, Vorname und Unterschrift. Nicht notwendig sind Geburtsdatum und Adresse. Das Geburtsdatum ist nicht aufzuführen, da es in diesem Zusammenhang für keinen Zweck notwendig ist. Die Adresse ist eine Angabe, die bei Studierenden recht häufigen Wechseln unterliegt und deshalb schnell nicht mehr richtig ist.

Der datenschutzrechtliche Grundsatz der Sparsamkeit verlangt, dass nur Daten bearbeitet werden, die für die Aufgabenerfüllung zwingend erforderlich sind. Mit dem Studentenausweis in der vorliegenden Art ist dies durch die Hochschule entsprechend korrekt umgesetzt worden.

Fall 33 Video- und Tonbandaufnahmen

Regelmässig erkundigen sich Lehr- und Therapiepersonen, wie vorzugehen ist, wenn zu Weiterbildungszwecken Video- oder Tonbandaufnahmen gemacht werden sollen. Folgende Hinweise sind zu beachten:

Wenn immer möglich ist dasjenige Vorgehen zu wählen, das die Privatsphäre der aufgenommenen Person besser schützt: Genügen für den vorgesehenen Zweck Tonbandaufnahmen, so sind keine Videoaufnahmen zu machen. Genügt es bei Video die Person von hinten oder von der Seite aufzunehmen, ist nicht eine Frontalaufnahme zu wählen. Insbesondere in sensiblen Bereichen – Aufzeichnungen von Therapiesessionen oder von behinderten Personen – ist die schriftliche Zustimmung der Betroffenen oder ihrer Eltern erforderlich. Die Zustimmungserklärung soll sich jedenfalls auf die folgenden Aspekte beziehen:

- Was ist der genaue Verwendungszweck?
- Wem werden die Aufnahmen zugänglich gemacht?
- Werden Kopien weitergegeben?
- Wann werden die Aufnahmen gelöscht?
- Erweiterungen oder wichtige Änderungen dieser Zustimmung müssen neu vorgelegt werden.
- Die Zustimmung kann jederzeit und ohne Angabe eines Grundes zurückgenommen werden.
- Je nach Situation sind weitere Aspekte zu regeln.

Fazit: Es ist zu bedenken, dass insbesondere durch Videoaufnahmen sehr stark in sensible Persönlichkeitsbereiche eingegriffen werden kann. Es ist deshalb zwingend erforderlich, dass optimale Schutzmassnahmen getroffen werden.

86 Eine «sprechende» Nummer ist beispielsweise die AHV-Nummer, der direkt Angaben zur Person entnommen werden können oder die Postleitzahl des Wohnorts mit angehängten Initialen des Kandidaten usw.

Fall 34 Alle Noten – an alle …

Eltern erkundigten sich, ob es aus datenschutzrechtlicher Sicht zulässig sei, dass ein Klassenlehrer der ganzen Klasse die Übersichtstabelle mit den Noten aller Fächer sämtlicher Schülerinnen und Schüler abgibt.

Die Rechtslage ist klar – das Vorgehen ist unzulässig. Jede Schülerin, jeder Schüler erhält nur die eigenen Noten, nicht aber diejenigen der ganzen Klasse und aller Fächer des ganzen Quartals.

Die Schulleitung kümmerte sich umgehend in vorbildlicher Weise um diesen Vorfall: Am gleichen Tag entschuldigte sie sich in eigener Verantwortung schriftlich bei allen Eltern der betroffenen Klasse und informierte im Weiteren die gesamte Lehrerschaft per E-Mail und machte dabei auf die Bestimmungen des Datenschutzes aufmerksam. Auch der Lehrer entschuldigte sich für sein Vorgehen schriftlich bei allen Eltern der Klasse.

Fazit: Eine massive Verletzung der Privatsphäre, die in der Hitze des Gefechts seinen Lauf nahm – und mit einer vorbildlichen und professionellen Schadensbegrenzung beendet wurde. Zu Letzterem hat der DSB denn auch der Schulleitung ein grosses Kompliment ausgesprochen.

Fall 35 Abschlussprüfung misslungen – kann ich die Handnotizen des Prüfungsexperten einsehen?

Wichtige Prüfungen werden aus Beweisgründen in Anwesenheit von Prüfungsexperten durchgeführt. Diese Experten machen sich während der Prüfung Notizen über den Verlauf der Prüfung. Es stellt sich verschiedentlich die Frage, welche Bedeutung diese Handnotizen haben, insbesondere, ob Kandidaten, die die Prüfung nicht bestanden haben, Einsicht nehmen können.

Betroffene Personen haben grundsätzlich das Recht, in *alle* sie betreffenden Daten Einsicht nehmen zu können. Das Speichermedium oder die Form der Bearbeitung spielt dabei *keine* Rolle. Ob es sich um Handnotizen, auf Tonband oder Fotos festgehaltene Informationen oder mit PC oder Schreibmaschine verfasste Dokumente handelt, ist nicht von Bedeutung. Handschriftliche Protokollnotizen bilden einen wichtigen Teil des Prüfungsverfahrens und gehören deshalb aus Beweisgründen ins entsprechende Dossier.

Sobald Daten über Personen bearbeitet werden – unabhängig von der Form –, kommt das Datenschutzrecht zur Anwendung. Sinn und Zweck liegen darin, dass die Betroffenen das Recht haben, wissen zu dürfen, welche Daten die öffentliche Verwaltung über sie bearbeitet. Nur so können sie die ihnen zustehenden Rechte wahrnehmen. Der Kandidat kann demnach beim zuständigen Organ grundsätzlich jederzeit Einsicht in seine eigenen Daten nehmen. Nur so kann er sich ein Bild machen, ob es sinnvoll ist, ein Rechtsmittel gegen den negativen Entscheid zu ergreifen.

Fazit: Man hat grundsätzlich das Recht, die Handnotizen eines Prüfungsexperten einsehen zu können.

Ausführliche Informationen zu diesem Fall sind beim DSB erhältlich.

Fall 36 Internet-Nutzung an der gemeindlichen Schule

Die Gemeinde Hünenberg hat mit Unterstützung des DSB die Internet-Nutzung der Schülerschaft ab 5. Primarschule durch einen Beschluss des Gemeinderats klar geregelt. Zum Inhalt der sogenannten «Internet-Charta»: Regelung von Rechten und Pflichten der Schülerschaft und der Eltern, Kontrollmechanismen, Sanktionen bei Verstössen, Pflicht der Erklärung und Kommunikation der Charta durch die Lehrpersonen gegenüber der Schülerschaft, Unterzeichnung der Charta durch Kind und Eltern. Die Eltern können übrigens von der Schule verlangen, dass ihr Kind keinen Internet-Zugang erhält.

Fazit: Eine klare, gut verständliche und gut kommunizierte Internet-Regelung ist zentrale Grundlage einer rechtmässigen Internet- und E-Mail-Nutzung.

Das Muster einer Internet-Regelung ist beim DSB erhältlich.

Fall 37 Internet-Nutzung zur freien Verfügung der Lehrlinge: Hier die Leitplanken

Eine kantonale Schule stellt ihren Lehrlingen im Schulgebäude eine grössere Anzahl von PC zur freien und in der Regel unbeaufsichtigten Benützung zur Verfügung. Es hat sich gezeigt, dass einerseits Hard- und Software häufig mutwillig beschädigt werden und andererseits die Internetbenützung nicht immer so ist, wie sich dies das Rektorat wünscht.

Die Schulleitung hat deshalb eine Informatik-Benutzungsordnung erlassen. Darin sind Rechte und Pflichten aller Nutzungsberechtigten – somit

auch von Lehrpersonen und Mitarbeitenden – umschrieben. Insbesondere wird auch darauf hingewiesen, dass unerlaubte Handlungen disziplinarische, zivilrechtliche oder strafrechtliche Konsequenzen haben können.
Sämtlichen Nutzungsberechtigten wurde ein Exemplar der Informatik-Benutzungsordnung abgegeben. Kenntnisnahme und Einhaltung müssen unterschriftlich bestätigt werden. Bei Lehrlingen müssen auch Lehrmeister und Eltern unterzeichnen.

Fazit: Eine klare, gut verständliche und gut kommunizierte Internet-Regelung ist zentrale Grundlage einer rechtmässigen Internet- und E-Mail-Nutzung.

Diese Regelung ist beim DSB erhältlich.

1.7 Gesundheitswesen

Fall 38 Zuger Kantonsspital führt elektronische Krankengeschichte ein

Bis anhin wurde im Zuger Kantonsspital die Krankengeschichte im Wesentlichen in Papierform geführt. Das Spital befasst sich seit längerem zusammen mit dem Kantonsspital Schwyz mit der Umstellung auf eine umfassende und durchgängige elektronische Krankengeschichte. Damit verbunden ist eine Reihe heikler Fragen bezüglich Datenschutz und Datensicherheit: Wer hat Zugriff auf welche Daten? Wer darf Daten ändern und löschen? Wie steht es um die technische Sicherheit bei Übertragung via Kabel- oder Funknetzwerken und Speicherung von Daten? Wie wird der Laptop gesichert, der zudem über ein Funknetz betrieben wird? Welche Daten sehen Administratoren, Hard- und Softwarelieferanten und weitere Dritte? Wie wird archiviert? Wie können Einsichtsrechte der Patientinnen garantiert werden? Es ist offensichtlich, dass diese Umstellung sehr weitreichende Konsequenzen für den Schutz der Privatsphäre der Patienten hat. Genügte es früher grundsätzlich, das Dossier in einem Schrank unter Verschluss zu halten, sind bei der elektronischen Krankengeschichte ganz andere Massnahmen erforderlich.
Die Projektleitung hat die Datenschutzkommission des Kantons Schwyz und den DSB Zug eingeladen, hier Input zu leisten. Es wird durch die Projektleitung ein Datenschutz- und Datensicherheitskonzept zu erstellen sein. Darin sind die wichtigsten Aspekte und deren Lösungen aufzuzeigen. Dazu werden die entsprechenden Datenschutzstellen Stellung nehmen. Voraussichtlich wird das Projekt im Jahr 2004 umgesetzt.

Fazit: Wenn die entsprechenden Massnahmen bezüglich Datenschutz und Datensicherheit getroffen werden, kann eine EDV-Krankengeschichte auch Vorteile haben: die Zugriffe können genau definiert und jederzeit kontrolliert werden, jede Änderung der Daten ist nachvollziehbar.

Fall 39 Keine Spitaldaten an einen Verein

Ein Verein hat zum Ziel, die Öffentlichkeit bezüglich einer bestimmten Krankheit zu informieren und Betroffenen Unterstützung anzubieten. Ein Klinikmitarbeiter, der in diesem Verein engagiert ist, fragte sich, ob er entsprechende Patientenadressen, über welche die Klinik verfügt, für einen Versand des Vereins benützen dürfe. Es sollte für den Verein geworben, auf seine Aktivitäten und Angebote aufmerksam gemacht werden.
Auch wenn die Verwendung der Patientenadressen gut gemeint war – sie ist absolut ausgeschlossen. Die Klinik darf die Adressen ihrer Patienten keinesfalls an Dritte herausgeben, ist doch vom Arzt- bzw. Patientengeheimnis nur schon die Tatsache erfasst, dass jemand Patient eines Arztes, einer Klinik ist. Bei einer diesbezüglichen Datenbekanntgabe wäre zu prüfen, ob sich die entsprechenden Beteiligten nicht strafbar machen.[87]
Die Aktivitäten und Ziele des Vereins sind durchaus sinnvoll und auch unterstützungswürdig. Ein mögliches – und zudem wohl viel versprechenderes – Vorgehen wäre es, wenn die behandelnden Ärzte ihre Patienten direkt auf den Verein aufmerksam machen und dessen Broschüre abgeben.

Fazit: Patientendaten dürfen von Kliniken oder Arztpraxen keinesfalls an Dritte weiter gegeben werden. Es sind rechtmässige Alternativen ins Auge zu fassen. Im vorliegenden Fall: Ärzte können die Informationen gezielt an die entsprechenden Patienten abgeben.

Fall 40 Psychiatrisches Gutachten im Strafverfahren

Im Rahmen eines Strafverfahrens verlangt ein Untersuchungsrichter vom Ambulanten Psychiatrischen Dienst eine psychiatrische Abklärung eines Angeschuldigten. Es wurde die Frage ge-

87 Verletzung des Berufsgeheimnisses, Art. 321 Strafgesetzbuch.

stellt, ob die betroffene Person ihre Zustimmung zur Abklärung erteilen müsse, und zudem, ob ohne ihre Zustimmung bei Dritten Auskünfte eingeholt werden dürften.
Die Strafprozessordnung sieht ausdrücklich vor, dass der Untersuchungsrichter eine körperliche Untersuchung des Beschuldigten anordnen kann, wozu ausdrücklich auch eine stationäre oder ambulante psychiatrische Begutachtung gehört.[88]
Die Begutachtung hat somit eine ausdrückliche gesetzliche Grundlage und bedarf deshalb der Zustimmung der betroffenen Person *nicht*.
Ob der Gutachter berechtigt ist, Auskünfte ohne Zustimmung des Betroffenen bei Dritten einzuholen, hängt davon ab, ob die fraglichen Auskünfte für die Erstellung des Gutachtens «offensichtlich unentbehrlich» sind. Hier hat der Gesetzgeber die Messlatte mit Absicht *hoch* angesetzt. Ob diese Voraussetzung gegeben ist, muss der Gutachter in Kenntnis der Sachlage prüfen und bejahendenfalls begründen.[89]

Diesbezüglich sind beim DSB ergänzende Hinweise erhältlich.

Fall 41 Datenbekanntgabe zwischen der Psychiatrischen Klinik und dem Amt für Straf- und Massnahmenvollzug?

Die Psychiatrische Klinik behandelt Personen, die im Massnahmenvollzug sind. Diese werden durch das Amt für Straf- und Massnahmenvollzug betreut. Es fragt sich, ob die Klinik dem Amt medizinische Beurteilungen mitteilen darf – oder muss.
Es gibt diesbezüglich keine ausdrückliche gesetzliche Regelung. Es gelten die allgemeinen Grundsätze. Das Amt muss aufgrund einer umfassenden Lagebeurteilung Entscheidungen treffen. Dabei ist die medizinische Beurteilung von zentraler Bedeutung. Ohne diese Kenntnisse kann das Amt seine gesetzlich vorgegebene Aufgabe nicht erfüllen. Es ist deshalb darauf angewiesen, von der Klinik die für seine Aufgabenerfüllung zwingend erforderlichen Angaben zu erhalten.

Fall 42 Muss ein Psychiater gegen seinen Patienten Strafanzeige erstatten?

Im Rahmen seiner therapeutischen Tätigkeit erhält ein Psychiater Kenntnisse über [möglicherweise] strafbares Verhalten seines Patienten. Darf oder muss er ihn bei der Polizei anzeigen?
Ärzte unterstehen dem Berufsgeheimnis. Verletzen sie dieses, machen sie sich grundsätzlich strafbar.[90] Das Berufsgeheimnis ist für eine wirkungsvolle Therapie *grundlegend*, da sich der Patient andernfalls gar nicht frei äussern könnte.
Zur Schweigepflicht gibt es gewisse Ausnahmen. So ist die Verletzung des Berufsgeheimnisses nicht strafbar, wenn der Berechtigte eingewilligt hat oder wenn die vorgesetzte Behörde schriftlich eine Bewilligung zur Offenbarung erteilt hat.[91] Im Weiteren ist eine Offenbarung ebenfalls dann nicht strafbar, wenn kantonale Bestimmungen eine solche vorschreiben.[92]
Das kantonale Recht sieht in der Strafprozessordnung[93] eine Anzeigepflicht für Mitglieder von Behörden, Beamte und Angestellte des Gemeinwesens vor, jedoch nur für strafbare Handlungen, die ihnen im Rahmen ihrer amtlichen Tätigkeit zur Kenntnis gelangen, sofern es sich um Delikte handelt, die von Amtes wegen verfolgt werden [sogenannte «Offizialdelikte»].
Zudem verpflichtet das Zuger Einführungsgesetz zum ZGB[94] *jede Person*, Anzeige an die Vormundschaftsbehörde zu erstatten, wenn sie eine Gefährdung des Kindeswohls wahrnimmt. Diese Vorschrift gilt insbesondere auch für Personen, die in medizinischen und therapeutischen Berufen tätig sind. Ist somit in einem konkreten Fall das Wohl eines Kindes gefährdet, so ist der Arzt verpflichtet, Anzeige zu erstatten. Allerdings ist die Anzeige der Vormundschaftsbehörde zu erstatten – und nicht etwa der Polizei. Die Vormundschaftsbehörde ist dann ihrerseits verpflichtet, zu prüfen, ob sie eine Anzeige an die Polizei zu erstatten hat. Sollte der Arzt die Ansicht vertreten, er müsse Strafanzeige erheben, so muss er bei der Gesundheitsdirektion einen begründeten Antrag auf Entbindung vom Berufsgeheimnis für den konkreten Fall stellen. In der Begründung sind nur diejenigen Angaben über die fragliche Person zu machen, die für die Beurteilung des Gesuchs zwingend erforderlich sind.

Fazit: Der Arzt steht unter einem *strengen Berufsgeheimnis*. Verletzt er es, macht er sich grundsätzlich strafbar. Eine Anzeigepflicht ist grundsätzlich *nicht* gegeben.[95] Eine Ausnahme besteht bei Gefährdung des Kindeswohls. Ist der Arzt der Ansicht, das Berufsgeheimnis müsse aufgehoben werden, ist zwingend eine Einwilligung der kantonalen Gesundheitsdirektion erforderlich.

Die ausführliche Stellungnahme ist beim DSB erhältlich.

88 § 21[bis] Abs. 1 Strafprozessordnung [BGS 321.1].

89 Ergänzend ist darauf hinzuweisen, dass sich anschliessend die Frage stellt, ob der Dritte berechtigt oder gar verpflichtet ist, dem Gutachter Auskünfte über den Betroffenen zu geben. Hier stellen sich Fragen des Prozessrechts, auf die im vorliegenden Rahmen nicht eingegangen werden kann.

90 Art. 321 Strafgesetzbuch [SR 311.0].

91 Art. 321 Ziff. 2 Strafgesetzbuch.

92 Art. 321 Ziff. 3 Strafgesetzbuch.

93 § 6 Strafprozessordnung.

94 § 34 Einführungsgesetz zum ZGB [BGS 211.1].

95 Siehe dazu auch die Berichterstattung in der NZZ vom 9. Oktober 2003, S. 55, «Versuchter Mord und ärztliche Schweigepflicht» bezüglich eines Mordprozesses vor dem Zürcher Obergericht: Eine behandelnde Psychiaterin hat einen Mordversuch ihrer Patientin angezeigt – der Paartherapeut hingegen nicht.

1.8 Sicherheit und Polizei

Videoüberwachung – ein Wundermittel?

Über den Einsatz von Videoüberwachung wurde an dieser Stelle bereits früher berichtet.[96] Da der DSB auch dieses Jahr wieder viele Anfragen zu diesem Thema bearbeitet hat, lohnt es sich, kurz auf ein paar diesbezügliche Situationen einzugehen.

Fall 43 Videoüberwachung einer Abfallsammelstelle

Videoüberwachung ist grundsätzlich ein *schwerer Eingriff* in die Privatsphäre. Beabsichtigt deshalb eine Gemeinde eine Abfallsammelstelle mit Videogeräten zu überwachen, benötigt sie dafür eine *formelle Rechtsgrundlage* im gemeindlichen Recht. Ein Beschluss des Gemeinderates genügt somit grundsätzlich nicht. Zudem muss der Einsatz vorweg überhaupt geeignet und verhältnismässig sein. Gibt es Alternativen, die massvoller sind? Dann sind diese zu wählen. Videoüberwachung kann höchstens als ultima ratio eingesetzt werden.

Die Datenschutzbeauftragten des Kantons Zürich[97] und Basel-Landschaft[98] haben übrigens sehr nützliche Unterlagen zur Videoüberwachung im kommunalen Bereich verfasst.

Fall 44 Videoüberwachung in der Schule

Nicht überall sind heutzutage die Schulen der Hort des Schönen und Guten. Aus der Schulbibliothek werden Bücher gestohlen, im Informatikraum wird der PC beschädigt, auf dem Pausenplatz finden Schlägereien statt, und nachts wird das Schulhaus besprayt. Auch hier gilt: Videoüberwachung kann höchstens punktuell und als letzter möglicher Schritt in Frage kommen. Was den öffentlich zugänglichen Bereich betrifft, ist Voraussetzung auch hier, dass eine ausdrückliche gesetzliche Grundlage vorhanden ist. Da es diesbezüglich im kantonalen Recht keine Bestimmungen gibt, müsste eine solche auf gemeindlicher Ebene geschaffen werden.
In Schulräumen ist die Situation insofern anders, als gestützt auf das Hausrecht der Einsatz von Videoüberwachung geprüft werden kann. Diese Prüfung muss sorgfältig vorgenommen werden und insbesondere auch politisch abgestützt sein, steht doch ein schwerer Eingriff in die Privatsphäre all jener zur Diskussion, die sich rechtskonform verhalten.

Fall 45 Videoüberwachung im Altersheim

Aus Zimmern von Betagten eines Alters- und Pflegeheimes werden immer wieder Schmuck und Geld gestohlen. Anzunehmen ist, dass es sich bei der Täterschaft um fremde Personen handelt, die untertags als Besucher durch einen der Haupteingänge das Haus betreten. Von der Leitung wird den Betagten dringend empfohlen, Wertsachen und grössere Geldbeträge zur sicheren Verwahrung abzugeben und das Zimmer bei Abwesenheit stets abzuschliessen. Beidem wird oft nicht nachgelebt. Die Heimleitung möchte deshalb die Haupteingänge dauernd mit Videokameras überwachen und den Besucherstrom aufzeichnen lassen – in der Hoffnung, bei einem Vorfall möglicherweise den Täter eruieren zu können.
Vorerst ist zu prüfen, ob alternative Lösungen weiterhelfen: Schnappschlösser an den Zimmertüren, damit die Türen nie offen stehen; kleine Zimmertresore für die Wertsachen, wie in vielen Hotels üblich; besetzte Loge am Eingang, die sich bei unbekannten Personen nach dem Wohin erkundigt; regelmässige Information der betagten Personen bezüglich der Vermeidung von Diebstählen.
Eine permanente Videoüberwachung der Eingänge wird wohl am Erfordernis der Geeignetheit scheitern: Wer mit schlechten Absichten das Haus betreten will, kann sein Gesicht mit einer Mütze verdecken oder im entscheidenden Moment wegschauen, so dass er oder sie nicht erkennbar aufgenommen wird. Ein Einschleichdiebstahl wird zudem oft nicht sofort bemerkt, vielleicht erst nach Tagen oder sogar Wochen. Diesfalls müssten Aufzeichnungen von Hunderten von Stunden ausgewertet werden, was niemandem zugemutet werden kann. Zudem ist der Publikumsverkehr derart stark, dass es wohl unmöglich wäre, einen Täter ausfindig zu machen. All diese Komplikationen würde auch ein potenzieller Einschleichdieb in Betracht ziehen – so dass auch nicht auf die Wirkung eines «Abschreckungs-Effekts» gebaut werden kann.

Fazit: Ein Videoeinsatz im vorliegenden Fall wäre wohl zum vornherein wirkungslos, ungeeignet und deshalb kaum sinnvoll. Die Heimleitung verzichtete in der Folge denn auch auf den Einsatz von Videoüberwachung.

96 DSB TB 2000 S. 17 Fall Nr. 17 [betr. Vandalismus gegen Fahrräder beim Zuger Bahnhof].

97 Auf der Homepage «www.datenschutz.ch», Rubrik «Beratung/Themen».

98 «www.baselland.ch/docs/jpd/ds/prak/prak-015.pdf».

Fall 46 Videoüberwachung in der neuen Strafanstalt

Der DSB liess sich die Einrichtungen zur Videoüberwachung im Neubau der Strafanstalt vor Ort durch den Anstaltsleiter zeigen. Die interne Weisung bezüglich Videoüberwachung wurde dem DSB vorgelegt.

Aus naheliegenden Gründen kann in diesem Rahmen auf keinerlei Details eingegangen werden. Festzuhalten ist, dass die Einrichtungen und die in der Weisung vorgegebenen Regelungen des Einsatzes als rechtmässig zu beurteilen sind. Die datenschutzrechtlichen Anforderungen an Verhältnismässigkeit, Transparenz, Technik, Aufzeichnung und Löschung sind erfüllt.

Fall 47 Wenn der Nachbar mit Video den Nachbarn überwacht …

Jemand überwacht vom eigenen Grundstück aus seinen nächsten Nachbarn mit Videokameras. Dabei handelt es sich datenschutzrechtlich um Datenbearbeitung durch Private. Dafür ist der Eidg. Datenschutzbeauftragte zuständig. Dieser hat denn auch ein allgemeines Merkblatt zur Videoüberwachung durch Private herausgegeben.[99] Trotzdem sei hier kurz Folgendes festgehalten: Es ist zu prüfen, ob es sich bei dieser Art der Überwachung um strafbares Verhalten handelt.[100] Es steht dem überwachten Nachbarn frei, bei der Polizei Anzeige zu erstatten. Er kann unabhängig davon mit einer zivilrechtlichen Klage auf Unterlassung gegen den Nachbarn vorgehen.[101]

Fall 48 Sperrung der eigenen Fahrzeughalterdaten

Auf dieses Thema wurde schon in früheren Tätigkeitsberichten[102] eingegangen. Hier nur so viel: Im Kanton Zug ist eine *voraussetzungslose* Sperrung der eigenen Fahrzeughalterdaten möglich. Eine entsprechende Mitteilung an das Strassenverkehrsamt genügt. Eine Begründung ist nicht notwendig. Gesperrte Daten dürfen nicht an Private bekannt gegeben und nicht in gedruckten oder edv-mässigen Verzeichnissen veröffentlicht werden.

Im Jahr 2003 haben neu rund 130 Privatpersonen beim Strassenverkehrsamt die Sperrung ihrer Fahrzeughalterdaten verlangt.

Fall 49 Gemeinderat bittet Polizei um Informationen aus dem Asylbereich

Die Bevölkerung einer Gemeinde beschwerte sich beim Gemeinderat über angebliche Straftaten von Asylsuchenden, die in der gemeindlichen Unterkunft wohnten. Der Gemeinderat bat deshalb die Zuger Polizei um nähere Informationen bezüglich Straftaten Asylsuchender, um auf die Klagen der Bevölkerung entsprechend reagieren zu können. Der DSB wurde von der Zuger Polizei um eine Stellungnahme gebeten.

Eine Information bezüglich der Polizeiarbeit im Bereich Asylsuchende ist rechtlich zulässig, sofern einzelne Personen weder bestimmt noch bestimmbar sind. Es muss sich somit um statistische Angaben handeln, die keine Rückschlüsse auf einzelne Personen ermöglichen. Da eine Aufschlüsselung bezüglich strafbarer Handlungen Asylsuchender nach Gemeinden offenbar nicht erfolgt, kann ohne weiteres über den allgemeinen Stand der Dinge im Kanton und in der Gemeinde informiert werden.

Fall 50 Des Jägers Parkplatz im Wald …

Jäger haben bestimmte Parkplätze zu benützen und müssen das dort parkierte Auto mit einer Vignette kenntlich machen, damit bei einer polizeilichen Kontrolle die Berechtigung des Parkierens ausgewiesen ist. Auf dieser Klebe-Vignette steht gut sichtbar das Wort «Jäger». Ein Jäger macht gegenüber dem DSB geltend, dass es diskriminierend sei, wenn an seinem Auto das ganze Jahr über diese «Jäger-Vignette» kleben müsse. Er sei in der Öffentlichkeit immer als Jäger erkennbar, man werde zum Teil auch angepöbelt. Es komme auch immer wieder vor, dass Autos mit Jäger-Vignetten von Unbekannten beschädigt würden.

Eine Auskunft beim zuständigen Amt für Fischerei und Jagd ergab, dass es offenbar nicht erforderlich ist, dass die Vignette wie die «Autobahn-Vignette» ans Auto geklebt werden muss. Vielmehr genügt es, wenn sie auf einen Karton geklebt wird und beim Parkieren auf den entsprechenden Parkplätzen wie eine Parkkarte von aussen gut einsehbar im Wagen liegt.

Im Nachgang zu dieser Anfrage wurde entschieden, anlässlich der anstehenden Revision der Jagdverordnung auf diese Kennzeichnungspflicht ganz zu verzichten.[103]

Fazit: Manchmal genügen eine kooperative und kompetente Verwaltungsstelle und minime Massnahmen, um die Privatsphäre Betroffener besser zu schützen.

99 EDSB TB 2000/2001 S. 114/115.

100 Art. 179quater Strafgesetzbuch.

101 Art. 28 ZGB.

102 DSB TB 2002 S. 18 Fall Nr. 30, DSB TB 2000 S. 23 Fall Nr. 31 und DSB TB 1999 S. 19 Fall Nr. 24.

103 Die geänderte Jagdverordnung wird voraussichtlich im Jahr 2004 in Kraft treten.

Fall 51 Wer darf das Polizei-Journal lesen?

Die Zuger Polizei führt ein sogenanntes «Journal», das polizeilich und dienstlich relevante Ereignisse kurz protokolliert. Ausgedruckt umfasst es täglich zwischen 20 und 30 Seiten. Diese polizeilichen Informationen stehen dem Korps für die Erfüllung seines Auftrags zur Verfügung. Der DSB wurde vom Sicherheitsdirektor um eine Stellungnahme angegangen, ob das Journal [bzw. Auszüge davon] täglich, automatisch und anlassfrei an Personen oder Stellen ausserhalb der Zuger Polizei weiter gegeben werden darf. An dieser Stelle wird nur zusammengefasst über die zentralen Punkte informiert.[104]

Das Journal ist ein Arbeitsinstrument, das den *polizeiinternen* Informationsaustausch gewährleistet. Es enthält in erster Linie polizeiliche Informationen. In aller Regel sind die festgehaltenen Daten *ungesichert* und müssen meist unter hohem zeitlichen Druck erfasst werden. Beispielsweise: Erste Eindrücke des Rapportierenden an einem Tatort, Aussagen Beteiligter oder Dritter an einem Unfallort oder erste Abklärungen aufgrund von Anzeigen usw. Es kann auch vorkommen, dass sich im Nachhinein ergibt, dass die erfassten ersten Informationen *falsch* sind. Daneben werden aber auch gewisse dienstlich relevante Informationen im Journal aufgenommen, welche an alle Mitarbeitenden der Zuger Polizei gelangen sollen.

Da die meisten Daten ungesichert sind, handelt es sich um *sehr sensible Daten, die keinesfalls an unberechtigte Personen gelangen dürfen*.

Werden Daten an Stellen oder Personen weitergegeben, ist meist festzustellen, dass durch den Vorgang der Weitergabe der Datenherr die Hoheit über seine Daten grundsätzlich verliert. Dadurch ist es praktisch unmöglich, eine *unkontrollierte Weiterverbreitung* von Daten zu verhindern.

Fazit: Das Journal der Zuger Polizei ist grundsätzlich ein rein intern zu verwendendes Arbeitsinstrument. Es sollte deshalb nicht automatisch und täglich an die Gemeindepolizeipräsidenten/innen, das Einzelrichteramt, das Untersuchungsrichteramt, die Staatsanwaltschaft, das Amt für Ausländerfragen sowie das Amt für Straf- und Massnahmenvollzug gehen.

Es steht im Übrigen dem Gesetzgeber frei – unter Beachtung der verfassungsmässigen Grundrechte und Grundsätze – die Weitergabe des Journals in einem formellen Gesetz näher zu regeln.

Ergänzend ist darauf hinzuweisen, dass auch in anderen Kantonen das Journal als rein polizeiinternes Arbeitsinstrument verstanden wird.[105] Ende Jahr war der Entscheid in dieser Angelegenheit noch pendent.

Fall 52 Ausländische Verkehrssünder: Busseninkasso im Ausland durch eine private Firma?

Ein ausländischer Fahrzeughalter fährt auf der Autobahn im Kanton Zug zu schnell und wird dabei von einer Messstelle erfasst – wie kann die Zuger Polizei die Busse eintreiben? Ein Inkasso-Unternehmen mit Sitz in Köln verspricht Hilfe. Die Firma hat sich bei der Zuger Polizei beworben, für diese im Auftragsverhältnis die Bussengelder von ausländischen Fahrzeuglenkern europaweit einzutreiben. Ist dies rechtlich zulässig?

Gestützt auf eine Stellungnahme des DSB der Stadt Zürich in der gleichen Sache, ist festzustellen, dass diese Auslagerung an eine private Firma dem geltenden Bundesrecht und dem kantonalen Datenschutzrecht widerspricht, somit *unzulässig* ist.[106]

Zu vermuten ist im Übrigen, dass das vorgeschlagene Vorgehen ohnehin kaum von Erfolg gekrönt wäre: Die ausländischen Temposünder würden die Zahlungsaufforderung einer privaten Firma für eine Zuger Busse wohl – direkt in den Papierkorb spedieren. Womit die Zuger Behörden die Sache auf dem ordentlichen Rechtshilfeweg verfolgen müssten.

Mehr Erfolg versprechen völkerrechtliche Abkommen[107], welche die Zusammenarbeit der Polizeibehörden auf diesem Gebiet vorsehen. Diese beruhen auf Gegenseitigkeit, betreffen somit auch die rasenden Schweizer im Ausland …

Fall 53 Zuger Verstösse im Bereich Lebensmittelgesetzgebung – auch in Bern zu registrieren?

Das Amt für Lebensmittelkontrolle ist aufgrund des Bundesrechts verpflichtet, dem Bundesamt für Gesundheit [BAG] sämtliche Strafentscheide aus dem Bereich der Lebensmittelgesetzgebung umgehend nach ihrem Erlass in *vollständiger Ausfertigung* unentgeltlich mitzuteilen.[108] Ist somit eine Kopie des Entscheides zu schicken – oder genügt auch weniger? Die Datenbekanntgabe ist am Verwendungszweck zu messen. Das BAG erstellt aufgrund der erhaltenen Entscheide eine Statistik. Zudem muss es einen Überblick über

104 Die ausführliche Stellungnahme des DSB ist in GVP 2003 veröffentlicht.

105 Etwa in Luzern, Basel-Landschaft und in der Stadt Zürich.

106 Die ausführliche Stellungnahme des DSB ist in GVP 2003 veröffentlicht.

107 «www.admin.ch/ch/d/sr/0.36.html» und im Verhältnis zu den Niederlanden insbesondere «www.admin.ch/ch/d/sr/0_741_531_963_62/index.html».

108 Art. 5 Verordnung über die Mitteilung kantonaler Strafentscheide [SR 312.3].

das Geschehen in den Kantonen haben. Für beides ist es *nicht* notwendig, dass die vollständigen Angaben der Zuger Verurteilten auch noch in Bern vorhanden sind.

Fazit: Im Sinne des Prinzips der Datensparsamkeit und der Verhältnismässigkeit wurde mit dem BAG vereinbart, dass es genügt, wenn anonymisierte oder zusammengefasste Entscheide nach Bern gesandt werden.

Fall 54 Kann eine Privatperson Einsicht in den Polizeirapport nehmen?

Eine Privatperson, die bestohlen worden ist, hat bei der Polizei Anzeige erstattet. Im Zusammenhang mit der Schadensabwicklung ihres Versicherers möchte sie wissen, was im Polizeirapport steht. Es stellt sich die Frage, ob die Polizei Einsicht in den Rapport gewähren muss.
Grundsätzlich hat jedermann das Recht, Einsicht in seine eigenen Daten zu nehmen.[109] Ein Grund zur Einschränkung der Bekanntgabe[110] liegt nicht vor. Die Polizei hat der betroffenen Person denn auch umgehend die Kopie des Rapports zugestellt.

Fall 55 Welchen Stellen sind Entscheide des Haftrichters bekannt zu geben?

Der Haftrichter überprüft die fremdenpolizeilichen Anordnungen bezüglich Vorbereitungs- und Ausschaffungshaft. Diese Entscheide des Verwaltungsgerichts werden zurzeit in Kopie dem betroffenen Ausländer, dem Amt für Ausländerfragen, der Zuger Polizei sowie dem Bundesamt für Flüchtlinge mitgeteilt. Dürfen sie auch der Vorsteherin der Direktion des Innern sowie Mitarbeitenden im Asylbereich zur Kenntnis gebracht werden?
Zusammengefasst[111] führt der DSB in seiner Stellungnahme aus: Datenherrin ist das Verwaltungsgericht. Bei den Entscheiden handelt es sich um besonders schützenswerte Daten. Es ist deshalb zu prüfen, ob die Daten für die anfragenden Stellen «offensichtlich unentbehrlich» sind. Dies haben die anfragenden Stellen dem Verwaltungsgericht gegenüber darzulegen. Anschliessend entscheidet dieses, ob die Voraussetzungen zur Datenbekanntgabe gegeben sind. Wird dies bejaht, müsste in einem nächsten Schritt geklärt werden, in welchem Umfang die Entscheide weiterzugeben sind. Genügt das Dispositiv oder ist der ganze Entscheid in Kopie erforderlich?

1.9 Forschung, Planung und Statistik

Fall 56 Forschung im Schulbereich

Im Rahmen eines nationalen Forschungsprojekts verlangte ein Wissenschafter Einsicht in archivierte Schulakten von Gemeinden und Kanton. Untersucht werden sollten durch die Forschergruppe der Universität Zürich Hintergründe und Umfeld von Jugendlichen, die aus der Schule ausgeschlossen wurden. Beim Schulausschluss handelt es sich um die schärfste Massnahme des Schulwesens in schwierigen Situationen. Die diesbezüglichen Daten über Jugendliche, ihre Eltern und das Umfeld sind sehr sensibel. Es war deshalb zu prüfen, ob Einsicht zu gewähren ist und gegebenenfalls unter welchen Bedingungen.
Da man davon ausging, dass die wichtigsten Unterlagen beim Staatsarchiv vorhanden waren, warteten die involvierten Gemeinden vorerst den Entscheid der kantonalen Verwaltung ab.
Gemäss der Verordnung über das Staatsarchiv[112] sind die Archivalien für Private grundsätzlich erst nach einer Sperrfrist von 35 Jahren frei zugänglich. Der Regierungsrat kann jedoch die Erlaubnis zur Einsichtnahme in *gesperrte* Archivalien erteilen. Dabei ist sorgfältig zu prüfen, wie die Interessen der betroffenen Personen auf Schutz ihrer Privatsphäre gegenüber den Interessen der Forschung zu gewichten sind. Grundsätzlich hat der Schutz der Privatsphäre Vorrang, da nie ausgeschlossen werden kann, dass betroffene Personen geschädigt werden können, wenn ihre Daten in der Öffentlichkeit bekannt werden. Auf der anderen Seite ist auch dem Datenschutzgesetz das Thema Forschung nicht unbekannt. Es sieht vor,[113] dass Daten für die Forschung bearbeitet werden dürfen, wenn sie anonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt, wenn sie nicht weitergegeben werden und wenn die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.
Aufgrund der Stellungnahmen des Staatsarchivars und des DSB bewilligte der Regierungsrat die Einsicht in gesperrte Akten des Staatsarchivs unter den folgenden Auflagen:

- Die Bewilligung ist persönlich, darf somit nicht auf andere Mitarbeitende des Forschungsprojekts übertragen werden.
- Namen von Personen müssen durch den Gesuchsteller so anonymisiert werden, dass sich die Personen nicht bestimmen lassen. Zur Veröffent-

109 § 13 Datenschutzgesetz.

110 § 14 Datenschutzgesetz.

111 Die ausführliche Stellungnahme ist in GVP 2003 veröffentlicht.

112 § 2 Verordnung über das Staatsarchiv [BGS 152.4].

113 Siehe § 4 Bst. d Datenschutzgesetz.

lichung bestimmte Texte sind dem Staatsarchiv vorzulegen, damit es die Einhaltung dieser Bestimmung überprüfen kann.
- Der Gesuchsteller trägt die Verantwortung dafür, dass die im Zusammenhang mit der Recherche von ihm angelegten Materialsammlungen, Dateien usw. nicht in die Hände von unbeteiligten Dritten gelangen oder von unbeteiligten Dritten benützt werden können. Die Anonymisierung ist auch bei der Anlage dieser Materialsammlungen zu gewährleisten.
- Der Gesuchsteller ist nicht berechtigt, auf der Basis der im Archiv recherchierten Personenkenntnisse mit betroffenen Personen Kontakt aufzunehmen.
- Die vorliegende Genehmigung zur Akteneinsicht gilt nur für das vorliegende Forschungsvorhaben und eine allenfalls daraus hervorgehende Publikation. Der Gesuchsteller ist ohne spezielle Genehmigung des Staatsarchivs nicht berechtigt, sein im Zusammenhang mit diesem Projekt erworbenes Wissen, soweit es auf Informationen aus den Beständen des Staatsarchivs aufbaut, für anderweitige Veröffentlichungen irgendwelcher Art zu verwenden.
- Die erhobenen Daten dürfen nicht an Dritte weiter gegeben werden.
- Von Archivdokumenten dürfen keine Kopien erstellt werden.
- Alle Auflagen gelten auch nach Abschluss des Projekts.
- Sofern die Auflagen ganz oder teilweise nicht eingehalten werden, wird der Gesuchsteller gemäss Art. 292 Strafgesetzbuch mit Haft oder Busse bestraft.

Die involvierten Gemeinden bewilligten die Einsicht in die gesperrten Akten, wobei sie die analogen Rahmenbedingungen wie der Regierungsrat aufstellten.

Fazit: Auch in heiklen Bereichen kann der Forschung grundsätzlich Einsicht in gesperrte Unterlagen gewährt werden. Mögliche Gefahren von Persönlichkeitsverletzungen sind durch Auflagen einzuschränken. Zentrale Voraussetzung der Einsichtserlaubnis zugunsten der wissenschaftlichen Forschung ist, dass die Gesuchsteller die absolute Gewähr bieten, die Auflagen einzuhalten.

Fall 57 Planung im Bereich von IV-Sonderschulen – mit welchen Daten?

Früherzieherinnen, die Kinder mit einer geistigen Behinderung vor dem Schul- beziehungsweise Kindergarteneintritt betreuen, wollten wissen, ob sie den von der IV unterstützten Sonderschulen die Namen der Kinder, die *möglicherweise* später eine Sonderschule besuchen werden, bekannt geben dürfen. Die Sonderschulen wollten diese Angaben zu Planungszwecken. Für die Planung müssen anonyme Angaben genügen, können sich somit etwa auf Alter und Geschlecht beschränken. Namen sind nicht bekannt zu geben. Zu berücksichtigen ist, dass solche Bekanntgaben offenbar auf sehr unsicheren Situationen beruhen. In vielen Fällen wurden die nächsten Schritte, insbesondere die Frage nach dem Besuch einer Sonderschule, noch nicht einmal mit den Eltern besprochen. Ohne spezielle gesetzliche Grundlage ist es demnach unzulässig, persönliche Daten ohne Wissen der Eltern zu diesem frühen Zeitpunkt an die Sonderschulen weiter zu leiten.
Es ist in diesem Zusammenhang daran zu erinnern, dass Betroffene ihre Daten bei der Verwaltung jederzeit einsehen können. Leiten die Früherzieherinnen jedoch ohne Wissen der Eltern Daten über ihr Kind an bloss möglicherweise in Frage kommende IV-Sonderschulen, so werden sie an der Ausübung fundamentaler Rechte gehindert.

Fazit: Planung versucht Aussagen über die Zukunft zu machen. Diese sind immer mit Unsicherheit behaftet. Dies gilt im Besonderen auf dem vorliegenden Gebiet. Es muss genügen, mit anonymisierten Angaben zu planen.

1.10 Informatik und Datensicherheit

Fall 58 Wenn die Verwaltung die Bevölkerung zur Kommunikation via E-Mail einlädt …

Alle kantonalen und gemeindlichen Zuger Verwaltungsstellen verfügen über einen Internet-Auftritt. Benötigen Private über dieses Angebot hinausgehende zusätzliche Auskünfte, wird ihnen in der Regel ermöglicht, via E-Mail mit der Verwaltung in Kontakt zu treten. Meist fehlt jedoch ein gut sichtbarer Hinweis, dass keinerlei Personendaten – erst recht keine vertraulichen – per E-Mail zu versenden sind, da unverschlüsselte

E-Mail-Kommunikation via Internet weniger vertraulich ist – als der Versand einer Postkarte. Auf dem Übertragungsweg sind E-Mails an vielen Orten für Dritte direkt einsehbar, werden kopiert und können verändert oder gelöscht werden.
In diesem Zusammenhang ist darauf aufmerksam zu machen, dass die Mitarbeitenden der Verwaltung selber keinerlei Personendaten und keine vertraulichen Sachdaten unverschlüsselt per E-Mail via Internet[114] versenden dürfen. Dies hat der Regierungsrat aus guten Gründen in der «Verordnung über die Benutzung von elektronischen Kommunikationsmitteln im Arbeitsverhältnis» ausdrücklich so festgelegt.[115] Diese Rechtslage müssen die Verwaltungsstellen bedenken, wenn sie es dem Publikum ermöglichen, via E-Mail mit ihnen zu kommunizieren.

Fazit: Die Verwaltungsstellen müssen die Öffentlichkeit bei der Kommunikation auf der Homepage, in Broschüren und im mündlichen Kontakt darauf aufmerksam machen, dass keinerlei Personendaten via unverschlüsselte E-Mail zu versenden sind.

Fall 59 Der PC im Konkurs – am besten gleich mit allen Personendaten?

Ein Privater informierte den DSB, dass im Rahmen eines Konkursverfahrens die ganze EDV-Anlage einer Firma durch einen Liquidator verkauft wurde und sich noch sämtliche Daten auf den PC und Servern befanden – inklusive Personaldaten. Es stellte sich die Frage nach der Verantwortung der verschiedenen Akteure und nach einem Weg, um solche Vorgänge zukünftig zu verhindern.

Zur Verantwortung der konkursiten Firma: In erster Linie ist die in Konkurs befindliche Firma verantwortlich, dass den Arbeitnehmern, Kunden oder weiteren Kreisen keinerlei Schaden entsteht. Sie ist deshalb verpflichtet, die zu liquidierenden PC *vollständig gelöscht* abzugeben. Die Daten dürfen nicht mehr rekonstruierbar sein. Daten in den «Papierkorb» verschieben, anschliessend «Papierkorb leeren» genügt jedenfalls nicht.
Die Firma ist in der Regel denn auch am besten in der Lage, die Daten zu löschen, da sie Kenntnis hat, wie die Maschinen konfiguriert sind und wo sich welche Daten befinden. Entsteht bei Dritten ein Schaden, der sich auf eine nicht ordnungsgemäss durchgeführte Datenlöschung zurückführen lässt, ist eine zivil- bzw. strafrechtliche Verantwortlichkeit der Organe [insbesondere des Verwaltungsrats] der konkursiten Firma zu prüfen.

Konkursamt: Das Konkursamt hat jedenfalls die Möglichkeit, von der Firma zu verlangen, dass die Daten auf den zur Konkursmasse gehörenden PC ordnungsgemäss gelöscht werden müssen.

Liquidator: Wird für die Durchführung der Liquidation ein privates Unternehmen beauftragt, so stellt sich die Frage, welche Pflichten dieses hat. Ein privater Liquidator weiss in der Regel nicht, welche Daten auf den PC sind, ob Dokumente zu löschen sind, welche Systeme genutzt wurden usw. Eine Pflicht, selber aktiv zu werden, ist deshalb wohl kaum anzunehmen. Anders verhält es sich hingegen, wenn der Liquidator ausdrücklich beauftragt wird, Speichermedien zu löschen oder wenn er mit Sicherheit weiss, dass sich noch sensible Daten auf den Computern befinden.

Käufer der PC: Erhält ein Käufer Kenntnis von sensiblen Daten über Dritte, so darf er die Betroffenen nicht schädigen. Andernfalls kann sich die Frage nach der Leistung von Schadenersatz stellen. Er ist deshalb verpflichtet, die Daten zu löschen. Gegebenenfalls können Zuwiderhandlungen zivil- oder strafrechtliche Konsequenzen haben.

Es wird eine Empfehlung auszuarbeiten sein, wie zukünftig vorzugehen ist, damit verhindert werden kann, dass Datenbestände aus Unternehmen im Konkurs an Unberechtigte gelangen können. Insbesondere die folgenden Aspekte sind zu klären: Wie ist technisch zu prüfen, ob die im Konkurs stehende Firma ihren Pflichten nachgekommen ist? Wie ist vorzugehen, wenn niemand mehr von der Firma zur Verfügung steht oder wenn die Firma aus anderen Gründen nichts unternimmt? Wer kommt für Kosten auf, die durch die professionelle Löschung anfallen? Unter welchen Umständen ist die Hard-Disk aus Sicherheitsgründen auszubauen und zu zerstören? Im Sinne einer Sofortmassnahme wurden alle Mitarbeitenden des Konkursamtes mit einer speziellen Software zur Löschung von Daten auf PC ausgerüstet.

114 Das kantonsinterne Netz wird hingegen als sicher betrachtet, so dass innerhalb der kantonalen Verwaltungsstellen grundsätzlich auch Personendaten übermittelt werden dürfen.

115 § 3 der Verordnung [BGS 154.28].

2. Öffentlichkeitsarbeit

2.1 Zuger Datenschutz im Internet

Die Homepage des Datenschutzbeauftragten ist unter «www.datenschutz-zug.ch» zu finden. Der Inhalt wird etwa alle zwei Wochen überprüft und gegebenenfalls aktualisiert.

Besucherstatistik

Die Besuche der Website des DSB werden durch eine Statistik-Software anonymisiert ausgewertet. Solche Auswertungen sind sehr kritisch zu beurteilen, stehen doch hinter vielen Besuchern – nur Suchmaschinen und keine am Thema interessierten Menschen. Sind wir also vorsichtig und zurückhaltend, so kann festgehalten werden, dass täglich durchschnittlich etwa 35 einzelne Personen aus der Schweiz die DSB-Website während durchschnittlich etwa je 5 Minuten besuchen. Im Vergleich zum Vorjahr bedeutet dies einen Zuwachs von rund 10%.

Auf der DSB-Website stehen einige wichtige Dokumente zum Herunterladen zur Verfügung – hier die ersten zehn Plätze der Hitparade:

3'133	Tätigkeitsbericht 2000 [gedruckte Exemplare: 3'000]
1'665	Tätigkeitsbericht 2002 [gedruckte Exemplare: 3'000]
1'019	Tätigkeitsbericht 1999 [gedruckte Exemplare: 2'000]
966	DSB in der «Zuger Gerichts- und Verwaltungspraxis/GVP 2001»
951	Leitfaden «Datenschutz in der Schule»
763	Tätigkeitsbericht 2001 [gedruckte Exemplare: 3'000]
754	Botschaft zum Bundesgesetz über den Datenschutz [DSG] vom 23. März 1988
659	Information des Eidg. DSB «Internetüberwachung am Arbeitsplatz»
635	DSB in der «Zuger Gerichts- und Verwaltungspraxis/GVP 2002»
427	Tätigkeitsbericht des DSB im «Rechenschaftsbericht des Regierungsrates des eidgenössischen Standes Zug an den Kantonsrat über das Amtsjahr 2002»

Fazit: Das DSB-Informationsangebot im Internet entspricht einem Bedürfnis. Es wird in der Datenflut des Internets wahrgenommen und von interessierten Kreisen häufig zu Rate gezogen. Nicht unbedeutend ist insbesondere das Herunterladen von Publikationen des DSB. Dadurch reduziert sich die Arbeitsbelastung des DSB. Das Angebot des DSB im Internet stellt somit eine nützliche, kostenlose und effiziente Dienstleistung dar.

2.2 DSB-Mailing-Liste

Das Konzept des Internet-Auftritts sieht seit Juni 2000 wie folgt aus: Alle grundlegenden Informationen werden auf der Website veröffentlicht.[116] Alle *aktuellen* Informationen aus den Bereichen Datenschutz und Datensicherheit werden hingegen *per E-Mail* in der Form von Kurzhinweisen – versehen mit Links auf Fundstellen, wo sich ausführliche Informationen finden – verschickt.[117] Diese Dienstleistung kann auf einfachste Weise in Anspruch genommen werden. Es genügt, wenn man auf der entsprechenden Seite der DSB-Website[118] seine eigene E-Mail-Adresse bekannt gibt. Wenn man übrigens keine Nachrichten mehr erhalten möchte, kann man sich ebenso einfach selber wieder aus der Liste austragen.

Wer sich in der Mailing-Liste eingeschrieben hat, wird pro Woche automatisch mit 1 bis 3 Kurznachrichten beliefert und ist damit immer auf dem Laufenden. Sämtliche verschickten Nachrichten werden zudem in einer Datenbank gespeichert. Soweit sinnvoll, sind dort zusätzliche Dokumente abgelegt. Diese Datenbank ist via Website auch für nicht eingeschriebene Personen zugänglich. Besonders erwähnenswert ist eine sehr wirkungsvolle Suchmaschine, die auch die meisten archivierten PDF-Dokumente erfasst.

Diese Dienstleistung stösst allgemein auf ein positives Echo. Es erfolgten keine besonderen Werbemassnahmen, trotzdem haben sich im Berichtsjahr neu über 100 Abonnierte eingeschrieben. Im Jahr 2003 wurden etwas über 80 Kurz-Mitteilungen verschickt. Täglich besuchen rund 20 Personen das Archiv. Dabei werden durchschnittlich etwa 7 Seiten konsultiert und täglich rund 10 Archiv-Dokumente heruntergeladen. Diese Zahlen entsprechen in etwa denjenigen des Vorjahres.

2.3 Tätigkeitsbericht 2002

Der Tätigkeitsbericht ist eine gute Gelegenheit, die Themen Datenschutz und Datensicherheit praxisorientiert und verständlich einem breiten Publikum vorzustellen. Insbesondere sollen auch die Mitarbeitenden der Verwaltung bezüglich

116 Insbesondere Gesetze, Literatur, Adressen und Links.

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

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

Datenschutz und Datensicherheit sensibilisiert und auch ein Stück weit ausgebildet werden. Auch im letzten Jahr wurde deshalb der Tätigkeitsbericht im März mit der Personalzeitschrift an sämtliche kantonalen Mitarbeitenden, an die Gemeinden sowie an zusätzliche interessierte Stellen verschickt. Es gingen viele Bestellungen von weiteren Kreisen ein, so dass sich die Auflage von 3'000 Exemplaren auf einen kleinen Restbestand reduziert hat.

Wer die letztjährigen Tätigkeitsberichte zu Rate ziehen möchte, kann sie beim DSB kostenlos bestellen oder sich auf der DSB-Website[119] eine layoutgetreue Kopie ausdrucken.

2.4 Gerichts- und Verwaltungspraxis des Kantons Zug [GVP]

GVP ist die offizielle Zuger Publikation, die einem juristisch interessierten Fachpublikum einen Einblick in die Rechtsprechung der Zuger Gerichte und der Verwaltung ermöglicht. GVP erscheint jährlich in einer Auflage von 700 Exemplaren. Der DSB hat in GVP 2002 einen Beitrag verfasst,[120] der fünf exemplarische Fälle aus der Praxis des Datenschutzbeauftragten umfasst.

2.5 Medienarbeit

Die Medien berichten gerne über spannende Ereignisse. Je dramatischer, desto besser. Die Zuger Verwaltung bot erfreulicherweise auf dem Gebiet des Datenschutzes keinen Anlass, auf diese Weise in die Medien zu kommen …

Hingegen wurde verschiedentlich in der Tagespresse über die Arbeit des DSB berichtet, etwa im Zusammenhang mit der Publikation des Tätigkeitsberichts sowie bei diversen anderen aktuellen Gelegenheiten.

In der Dezemberausgabe von «digma»[121], der schweizerischen Fachpublikation für Datenschutz und Datensicherheit, wurde über den «Leitfaden – Datenschutz in der Schule»[122], den die Direktion für Bildung und Kultur zusammen mit dem DSB verfasst hat, berichtet.

Unter dem Titel «Visionen» erschien in der letzten Ausgabe der Personalzeitung im Berichtsjahr[123] ein Beitrag, in dem sich der DSB ein paar grundlegende Gedanken zur zukünftigen Entwicklung des Datenschutzes machen konnte. Ob es sich dabei tatsächlich um Visionen – oder vielleicht eher um Alpträume – handelt, sei an dieser Stelle offen gelassen …

3. Mitarbeit bei der Gesetzgebung

Die Mitarbeit bei der Gesetzgebung ist *zentral*. Werden die Grundsätze von Datenschutz und Datensicherheit in der Gesetzgebung korrekt berücksichtigt, entstehen später bei der Anwendung im Idealfall keine – jedenfalls aber weniger – Konflikte.

Die Erfahrung hat zudem gezeigt, dass eine *frühe* Beteiligung des DSB optimal ist. Wird der DSB zu einem späten Zeitpunkt einbezogen, ist es meist aufwändiger, Datenschutz und Datensicherheit systematisch und konsequent in eine Vorlage zu integrieren.

3.1 Abgeschlossene Rechtserlasse

Archivgesetz

Zur Vorgeschichte: Das Zuger Archivwesen wird zurzeit in einer Verordnung aus dem Jahre 1982 nur sehr lückenhaft geregelt.[124] Es besteht Handlungsbedarf, rechtlich sauber zu definieren, was mit den Daten zu geschehen hat, die von der kantonalen und auch der gemeindlichen Verwaltung nicht mehr benötigt werden.[125] Der Regierungsrat hat Ende 2002 zuhanden des Kantonsrats eine Gesetzesvorlage verabschiedet. Was die gegensätzlichen Interessen betrifft – Schutz der Privatsphäre hier, Forderung nach Zugangserleichterung für Forschung und Medien dort –, konnte ein für alle Beteiligten akzeptabler Kompromiss gefunden werden.[126]

Im Berichtsjahr bestellte der Kantonsrat im Januar die vorberatende Kommission, die den Entwurf an zwei Sitzungen beraten hat. Staatsarchivar und DSB nahmen daran als Experten teil. Nachdem zwei Bestimmungen, bei denen Mehrkosten für die Gemeinden befürchtet worden sind, gestrichen wurden, verabschiedete der Kantonsrat die Vorlage ohne Abänderungen im Oktober in der ersten und im Januar 2004 in der zweiten Lesung.

Weisung über die Nutzung des Telefons am Arbeitsplatz

Der Grossteil der Vorarbeiten zu dieser Weisung, bei denen auch der DSB mitbeteiligt war, erfolgte im Vorjahr.[127] Der Regierungsrat hat die Weisung im September 2003 erlassen; anschliessend wurden die entsprechenden technischen Umsetzungen vorgenommen. Die wichtigsten Punkte:

119 «www.datenschutz-zug.ch» [Rubrik «Kanton Zug/Tätigkeit»].

120 GVP 2002 S. 295–307.

121 Zeitschrift für Datenrecht und Informationssicherheit, 4/2003 S. 182, Schulthess Verlag, Zürich.

122 Siehe dazu vorne S. 5 f. Näheres.

123 Siehe den Beitrag in «Personalziitig», 4/2003, S. 26.

124 Verordnung über das Staatsarchiv [BGS 152.4].

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

126 Den Gesetzesentwurf und den erläuternden Bericht des Regierungsrates finden Sie auf der DSB-Website in der Rubrik «Zug/Aktuelles».

- In einem zurückhaltenden Ausmass ist privates Telefonieren erlaubt.
- Telefongespräche dürfen weder abgehört,[128] noch aufgezeichnet werden.[129]
- Die sogenannten Randdaten[130] einzelner Gespräche werden nach einem Monat gelöscht.
- Vorgesetzte erhalten grundsätzlich keine Einsicht in die Telefondaten [Ausnahme: Summe der Monatsgebühren].
- Bei Verdacht auf Missbrauch können Randdaten nach vorgängiger Information des Betroffenen ausgewertet werden.

3.2 Vernehmlassungen

Bundesrecht

Im Berichtsjahr hat der DSB zu folgenden Vorlagen im Rahmen von Mitberichtsverfahren Stellung genommen:

- Bundesgesetz über Waffen, Waffenzubehör und Munition [zweite Vernehmlassung]
- Bundesgesetz über Massnahmen gegen Rassismus, Hooliganismus und Gewaltpropaganda
- Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister.

Diese DSB-Stellungnahmen wurden vom Regierungsrat weitestgehend in dessen Vernehmlassungsantwort gegenüber dem Bund integriert.

Kantonales Recht

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

- Standesinitiative Bankkundengeheimnis
  Sowohl im Bund wie auch in vielen Kantonen sind Bestrebungen im Gang, die das Bankkundengeheimnis ausdrücklich in der Bundesverfassung verankern wollen. Aufgrund einer Motion aus dem Zuger Kantonsrat befasste sich auch der Zuger Regierungsrat mit diesem Thema. Im Rahmen der Beantwortung der Motion hat der Regierungsrat den DSB zu einer Stellungnahme eingeladen.
  Fazit der DSB-Stellungnahme: Aus der Sicht des Schutzes der Privatsphäre des Einzelnen ist das vorliegende Anliegen grundsätzlich zu *begrüssen*. Wird aber die Bundesverfassung im Bereich des Schutzes der Privatsphäre revidiert, so sind bei dieser Gelegenheit die übrigen *zentralen Schutzbereiche* [etwa: Gesundheitsdaten, DNS-Daten, Arbeitnehmerdaten usw.] ebenfalls explizit in Art. 13 Bundesverfassung aufzuführen.
- Entwurf zu Informatik-Leitbild, Informatik-Strategie und Informatik-Verordnung
  Der DSB konnte durch seine Stellungnahmen den Grundsatz, dass jegliche Datenbearbeitung der öffentlichen Verwaltung in einem sicheren Umfeld ablaufen muss, verstärken.

3.3 Vorarbeiten zu Rechtserlassen

Revision Finanzhaushaltsgesetz

Im Rahmen der Vorarbeiten zur Totalrevision des Finanzhaushaltsgesetzes nahm der DSB zur Frage der Datenbereitstellung durch die Verwaltung gegenüber der Finanzkontrolle Stellung. Strittig war insbesondere der vorgesehene umfassende Online-Zugriff. Der DSB kam diesbezüglich zum Schluss: Der hier zu prüfende Vorschlag, der der Finanzkontrolle einen allgemeinen und bedingungslosen Anspruch auf Online-Zugriffe auf die Datenbestände der zu prüfenden Stellen gibt, ist klar unverhältnismässig und deshalb *nicht rechtmässig*. Das geltende Recht bietet die Möglichkeit, dass der Regierungsrat *einzelfallweise* Online-Zugriffe bewilligen kann.

Polizeigesetz

Das Zuger Polizeigesetz[131] soll einer Totalrevision unterzogen werden.[132] Erste interne Vorarbeiten sind von der Sicherheitsdirektion bereits im Vorjahr in Angriff genommen worden. Dieses Gesetzesprojekt hat einen sehr engen datenschutzrechtlichen Zusammenhang: Welche Daten dürfen durch wen wie erhoben werden? Weitergabe von Daten? Archivierung, Löschung? Rechte der Betroffenen? Der DSB wurde deshalb von der Arbeitsgruppe von Anfang an bei der Behandlung entsprechender Bestimmungen beigezogen. Ende 2003 befanden sich die Vorarbeiten noch im Fluss, ein offizieller Entwurf liegt noch nicht vor. Es wird im nächsten DSB-Tätigkeitsbericht[133] darauf zurückzukommen sein.

127 Siehe dazu DSB TB 2002 S. 23.

128 Siehe dazu auch vorne Fall Nr. 20 S. 14.

129 Ausnahmen: besondere Dienste [so beispielsweise die Telefonnummern 117, 118 und 144] sowie im Rahmen von Strafverfahren.

130 Zielnummer, Zeit/Datum des Anrufs, Gesprächsdauer, Gebührenhöhe.

131 Gesetz über die Kantonspolizei [BGS 512.1].

132 Es handelt sich dabei um ein Schwerpunktgeschäft der Zuger Sicherheitsdirektion für das Jahr 2004.

133 Aktuelles wird zudem umgehend in der DSB-Mailing-Liste vermeldet werden.

4. Register der Datensammlungen

Grundsätzliches

Aufgrund des Datenschutzgesetzes sind die kantonale und die gemeindlichen Verwaltungen verpflichtet, ein Register grundsätzlich aller[134] durch sie geführten Datensammlungen zu erstellen.[135]
Dadurch wird gegenüber der Öffentlichkeit Transparenz geschaffen: Es ist für jedermann ersichtlich, welche Daten bei welcher Verwaltungsstelle bearbeitet werden. Das Register ist somit auch Grundlage für das Einsichtsrecht. Wer Einsicht in seine eigenen Daten erhalten möchte, erfährt, an welche Verwaltungsstelle er sich wenden muss.
Das Register ist aber auch für die Verwaltung selber nützlich, erhält sie doch einen besseren Überblick über die vorhandenen Daten und über die Datenflüsse unter den Verwaltungsstellen. Es bietet zudem die Möglichkeit, kritisch zu überprüfen, ob die vorhandenen Datensammlungen zu Recht geführt werden, inhaltlich in Ordnung und sachlich überhaupt notwendig sind.
Selbstverständlich enthält das Register selbst keinerlei Personendaten. Vielmehr werden *nur Art, Umfang und Inhalt* der verschiedenen Datensammlungen aufgeführt. Zusätzlich gibt das Register auch Aufschluss darüber, von welcher Amtsstelle die jeweilige Datensammlung geführt wird.

Zuständigkeiten und Projektleitung

Der DSB ist für die Führung des Registers der Datensammlungen der kantonalen Verwaltung zuständig, die Gemeinden haben ihrerseits eine Person mit der Registerführung zu beauftragen.[136]
Damit der Bevölkerung ein einheitliches Register aller öffentlichen Verwaltungen[137] zur Verfügung steht, hat die Datenschutzstelle die erstmalige Erfassung aller Datensammlungen bei sämtlichen Verwaltungen übernommen. Sie verfügt zudem über eine EDV-Lösung, in welcher die Angaben zu den Datensammlungen verwaltet werden und die es ermöglicht, das gesamte Register im Internet zu veröffentlichen.
Bei der Datenschutzstelle leiteten bis März 2003 Fürsprecherin Christine Andres, anschliessend bis Ende Juni Rechtsanwältin Dr. iur. Yvonne Artho und seit August Rechtsanwalt lic. iur. Carl-Rudolf Meier das Projekt. Für die Erfassung und Übertragung der Daten in das EDV-Tool erhielten sie tatkräftige Unterstützung eines Teilnehmers des «Programms zur vorübergehenden Beschäftigung [PvB]» des «Vereins für Arbeitsmarktmassnahmen [VAM]». Ihnen allen sei für ihr Engagement ganz herzlich gedankt!

Stand des Projekts

Hinweise zu Grundlagen und Verlauf des Projekts finden Sie in den früheren Tätigkeitsberichten.[138]
Im Berichtsjahr konnten die Arbeiten an diesem wichtigen Projekt weiter vorangetrieben werden. Per Ende Jahr enthält das Register 1'209 Datensammlungen von Kanton und Einwohnergemeinden.
Wir benützen gerne die Gelegenheit, an dieser Stelle allen beteiligten Amtsstellen in Kanton und Gemeinden für ihre Mitarbeit sehr herzlich zu danken.
Der Einsatz hat sich gelohnt, verfügt die Zuger Verwaltung doch nun über die gesetzlich geforderte Transparenz. Aufgrund der Publikation des Registers der Datensammlung im Internet ist es nun allen Einwohnerinnen und Einwohnern möglich, von ihren Rechten auch tatsächlich Gebrauch zu machen.

Ausblick

Die Veröffentlichung des Registers der Datensammlungen der kantonalen Verwaltung und der Einwohnergemeinden im Internet war auf Ende 2003 geplant. Aufgrund verschiedener Verzögerungen kann sie nun anfangs 2004 erfolgen. So wird jede interessierte Person die Möglichkeit haben, von zu Hause aus abzuklären, welche Daten von den verschiedenen Amtsstellen gesammelt werden.

134 Ausnahmen gemäss § 12 Abs. 2 Datenschutzgesetz: Hilfsdatensammlungen [gemäss Umschreibung in § 2 Bst. e Datenschutzgesetz] und Datensammlungen, die nur bis maximal sechs Monate geführt werden; Datensammlungen, die keine Personendaten, sondern ausschliesslich Sachdaten beinhalten, sind nicht im Register nachzuweisen.

135 § 12 in Verbindung mit § 26 Abs. 1 Datenschutzgesetz.

136 § 12 Abs. 5 Datenschutzgesetz.

137 Kantonale Verwaltung sowie diejenigen der Einwohner-, Bürger-, Kirch- und Korporationsgemeinden.

138 DSB TB 2000 S. 30, DSB TB 2001 S. 22/23 sowie DSB TB 2002 S. 23–25.

5. Weiterbildung

5.1 Weiterbildungsangebot des Datenschutzbeauftragten

«Die Verwaltung kennen lernen»

Neue Mitarbeitende der kantonalen Verwaltung werden im Rahmen einer obligatorischen eintägigen Veranstaltung mit Grundlagen, Struktur und «Philosophie» ihres neuen Arbeitgebers bekannt gemacht. Diese Veranstaltung wird vom Personalamt drei- bis viermal pro Jahr durchgeführt und von etwa 30 Personen besucht. Die Datenschutzstelle hat erfreulicherweise vom federführenden Personalamt erstmals die Gelegenheit erhalten, den neuen Mitarbeitenden die Grundlagen zu Datenschutz und Datensicherheit kurz zu präsentieren, ihnen die zentralen Rechte und Pflichten zu skizzieren und sie auf die Dienstleistungen der Datenschutzstelle aufmerksam zu machen.

Das Ziel einer solchen Veranstaltung kann nicht sein, die Mitarbeitenden in Datenschutz und Datensicherheit auszubilden. Wichtig ist vielmehr, dass die neuen Mitarbeitenden aller Stufen einen ersten Kontakt mit der Datenschutzstelle haben und dadurch wissen, wo sie bei Bedarf Hilfe erhalten.

Flächendeckende EDV-Weiterbildung – mit Datenschutz-Modul

Die Hersteller von Betriebssystemen zwingen ihre Kundschaft in regelmässigen Abständen – insbesondere durch die Verweigerung von Support und Aktualisierung – auf neue Systeme umzurüsten. Die kantonale Informatik sah sich aus diesen Gründen gezwungen, ab Ende 2003 auf das neue XP-Betriebssystem von Microsoft zu wechseln. Positiv an dieser Umstellung ist, dass sie ermöglicht, eine grundsätzlich einheitliche Informatik-Landschaft zu schaffen und dadurch die Effizienz von Betrieb und Unterhalt nachhaltig zu verbessern.

Dieser Wechsel auf XP hat auch direkte Auswirkungen auf die PC-Nutzung durch die Mitarbeitenden der Verwaltung. Das Projekt dieser Umstellung sah deshalb vor, dass alle Anwenderinnen und Anwender im Rahmen einer halbtägigen Schulung mit den wichtigsten Änderungen vertraut gemacht werden.

Nachdem schon seit längerem feststand, dass sämtliche Verwaltungsmitarbeitende bezüglich der Grundzüge von Datenschutz und Datensicherheit auszubilden sind, bot sich bei der XP-Schulung eine gute Gelegenheit, ein Modul «Datenschutz und Datensicherheit» einzubauen. Die ausgezeichnete Zusammenarbeit mit der kantonalen Informatik [ITL] ermöglichte eine speditive Projektabwicklung, bei der das ITL für den Rahmen, der DSB für den Inhalt des Moduls verantwortlich war.

Der DSB konzipierte das Ausbildungsmodul «Datensicherheit und Datenschutz», das aus Präsentation und Kursunterlagen besteht und schulte die XP-Kursleiter, die im Rahmen ihres Ausbildungsauftrages die Mitarbeitenden der Verwaltung in der Folge auch im Bereich des Datenschutzes ausbildeten. Aus Kapazitätsgründen war es für den DSB ausgeschlossen, diesen Bereich selber zu präsentieren, fanden doch allein im Berichtsjahr mehr als 30 Kurse mit rund 350 Teilnehmenden statt – und im Jahr 2004 werden es noch einige mehr sein.

Fazit: Für den Schutz der Privatsphäre von Bürgerinnen und Bürgern ist es entscheidend, dass sämtlichen Mitarbeitenden der Verwaltung zumindest in den Grundzügen bekannt ist, welche Pflichten sie im Bereich Datenschutz/Datensicherheit zu befolgen haben. Dazu hat das vorliegende Schulungsprogramm einen wichtigen Beitrag geleistet. «Datenschutz? – Nie gehört!» kann man bei den kantonalen Mitarbeitenden der Verwaltung zukünftig nicht mehr gelten lassen …

Weitere Veranstaltungen und Präsentationen

Im Berichtsjahr wünschten einige private Institutionen, die im Rahmen von Leistungsverträgen öffentliche Aufgaben – insbesondere aus dem Sozialbereich – für den Kanton übernommen haben, eine Ausbildung in Sachen Datenschutz durch den DSB. Im Rahmen seiner zeitlichen Möglichkeiten ist der DSB stets gerne bereit, Verwaltungsstellen und auch Auftragsnehmer öffentlicher Aufgaben gezielt auszubilden, zu informieren und mit ihnen bei konkreten Fragestellungen nach Lösungen zu suchen.

Daneben gab es zusätzlich zahlreiche Gelegenheiten, im Rahmen von Referaten, Kurz-Präsentationen oder Sitzungen über Anliegen des Datenschutzes und der Datensicherheit zu informieren.

5.2 Auch der DSB muss sich weiterbilden

Allgemeines

Von Hause aus ist der Datenschutzbeauftragte Jurist, kein IT-Spezialist. Insbesondere im Bereich der Datensicherheit ist ein Minimum an technischem Verständnis und Wissen zwingend erforderlich. Der DSB muss sich deshalb diesbezüglich informieren und weiterbilden.
Im Berichtsjahr besuchte der DSB Veranstaltungen der «Fachgruppe Security» der «Schweizer Informatiker Gesellschaft [SI]» mit Schwerpunkt Informatiksicherheit, daneben solche verschiedener Anbieter zu den Themen Videoüberwachung, IT-Security, Datenschutz und Terrorismusbekämpfung sowie das Zürcher «Symposium on Privacy and Security».

Internationale Konferenzen

Datenschutz und insbesondere Datensicherheit sind Themen, die international diskutiert, entwickelt und entschieden werden. Der DSB muss informiert sein, was in Europa und weltweit passiert. Um einen vertieften Einblick in das aktuelle Geschehen zu erhalten, bieten internationale Treffen ideale Möglichkeiten. Was liegt in der Luft – welche Themen kommen durch internationale Vorgaben bald auch auf die Schweiz zu? Wie können wir uns vorbereiten? Wie machen es die anderen? Was hat sich bereits bewährt, was nicht?

Neben Referaten, Workshops und Diskussionen sind stets auch Gespräche im informellen Rahmen wichtig und wertvoll. Geben diese Kontakte doch viele Anstösse für die tägliche Arbeit und auch die Möglichkeit, bei Bedarf auf ausländisches Fachwissen zurückgreifen zu können.
Die Datenschutzstelle – und damit auch ihre Kunden – können dadurch ganz direkt vom international vorhandenen Know-how profitieren.

[Hinweis: An den folgenden drei internationalen Konferenzen hat der DSB in seiner Freizeit teilgenommen; für Kosten und Spesen kam er selber auf.]

Konferenz der europäischen Datenschutzbeauftragten

Die Konferenz fand am 3. und 4. April in Sevilla statt. Es haben rund 90 Personen teilgenommen, die Datenschutzstellen aus 25 europäischen Staaten, die Europäische Kommission, den Rat der EU, das Europäische Parlament und den Europarat vertreten haben. Neben dem Eidg. Datenschutzbeauftragten waren aus der Schweiz die Datenschutzstellen der Kantone Basel-Landschaft, Freiburg, Zürich und Zug vertreten.
Die Schwerpunkte:
- Zur Rolle der Datenschutzstellen
- Stand der Umsetzung der Richtlinie 95/46/EG
- Datenschutz in den neuen EU-Mitgliedsstaaten
- Grenzüberschreitender Datenverkehr
- Datenschutz im Telekommunikations-Sektor
- Zur Unabhängigkeit beim Umgang mit Beschwerden gegen Politiker

International Working Group on Data Protection in Telecommunications

Auf Einladung des Organisators, des Berliner Beauftragten für Datenschutz und Informationsfreiheit, nahm der DSB erstmals an der Frühjahrestagung dieser Arbeitsgruppe vom 17./18. März 2003 in Zürich sowie an der Herbsttagung vom 2./3. September 2003 in Berlin teil. Rund 40 Teilnehmende vertraten gegen 20 europäische Staaten, die EU-Kommission sowie weitere Organisationen oder Stellen [US-FTC, EPIC].
Die Themen:
- Aktuelles aus der Gesetzgebung der Staaten im Bereich Telekommunikation, Internet und E-Government
- Datenschutz und Strafverfolgung
- Wireless-LAN und Datenschutz
- Rechtsentwicklungen bezüglich Spam
- Datenschutz bei mobiler Telekommunikation
- RFID-Resolution

Symposium «Informationsfreiheit und Datenschutz im Internet»

Im Sinne eines Vorprogramms zur Herbsttagung fand am 1. September 2003 in Berlin im Rahmen der Internationalen Funkausstellung das Symposium «Informationsfreiheit und Datenschutz im Internet» statt. Diskutiert wurden folgende Themen:
- Informationsfreiheit und Datenschutz – Gegensatz oder Ergänzung?
- Informationsfreiheit und das Internet
- Informationsfreiheit und Datenschutz – im Zweifel für den Datenschutz?
- Electronic Freedom of Information in the US
- Kommerzialisierung öffentlicher Informationen im Internet

6. Zusammenarbeit mit dem Eidgenössischen und mit den kantonalen Datenschutzbeauftragten

Allgemeines

Die Datenschutzbeauftragten sämtlicher Kantone und der Eidgenössische Datenschutzbeauftragte [EDSB] sind im Verein «DSB + CPD.CH» zusammengeschlossen.[139] So können die – meist sehr beschränkt – vorhandenen Ressourcen besser genützt werden: Gemeinsames Auftreten gegenüber den Medien, Verfassen von Vernehmlassungen, Organisation von Weiterbildungsveranstaltungen, Informationsaustausch usw. Ein Teil dieser Arbeit wird von Arbeitsgruppen geleistet.[140]
Der im Jahre 2002 neu eingesetzte DSB des Fürstentums Liechtenstein und der DSB der Stadt Zürich sind dem Verein mit Beobachterstatus beigetreten.

«Arbeitsgruppe innere Sicherheit»

Der DSB leitete seit Sommer 2000 die «Arbeitsgruppe innere Sicherheit [AGIS]». Aus Gründen der Arbeitsüberlastung musste er per Ende 2002 Leitung und Mitarbeit in dieser Arbeitsgruppe leider aufgeben.

Zusammenarbeit mit dem DSB Luzern

Für den Zuger DSB ist die Zusammenarbeit mit Luzern nahe liegend, da in der Zentralschweiz nur dort eine eigenständige Datenschutzstelle vorhanden ist.[141] Es besteht seit Jahren eine lockere, aber regelmässige Kooperation. Im Berichtsjahr wurde beschlossen, im Jahr 2004 gemeinsam Weiterbildungsveranstaltungen im Bereich Datenschutz für die Zentralschweizer Mitarbeitenden der Verwaltung zu konzipieren und anzubieten.
Es wäre sinnvoll, vermehrt gemeinsame Projekte kantonsübergreifend anzugehen. Langfristiges Ziel wäre ein effizienterer Einsatz von personellen und finanziellen Ressourcen bei den einzelnen Datenschutzstellen. Leider verfügen die jeweiligen Datenschutzstellen jedoch über derart knappe Mittel, dass nicht einmal der Anfangsinput in solche Projekte erbracht werden kann.

Jahreskonferenz der schweizerischen Datenschutzbeauftragten

Nachdem im Vorjahr der Zuger DSB die Jahreskonferenz durchgeführt hatte, lud im Berichtsjahr die Genfer «Commission de contrôle de l'informatique de l'Etat» auf den 19./20. November 2003 nach Genf ein. Neben der Erledigung der vereinsinternen Geschäfte stand das Thema «Spam»[142] im Zentrum von Referaten und Diskussion. Wertvoll waren auch die Gelegenheiten zu informellem Gedankenaustausch mit Kolleginnen und Kollegen.

Kooperation mit dem Datenschutzbeauftragten der Stadt Zürich

Seit Dezember 2000 ist der DSB vom Gemeinderat der Stadt Zürich[143] gewählter Stellvertreter des Datenschutzbeauftragten der Stadt Zürich. Es handelt sich dabei um ein Nebenamt, das im Berichtsjahr etwa einem 1%-Pensum entsprach. Durch diese Zusammenarbeit ergeben sich wertvolle Synergien für die Datenschutzstelle im Kanton Zug.
[Hinweis: Der DSB übt diese Tätigkeit ausserhalb seines 60%-Pensums aus.]

7. Wir über uns

Allgemeines

Das Arbeitspensum des DSB betrug im Berichtsjahr von Januar bis Juli 75%, seit August 60%. Rechtsanwältin Dr. iur. Yvonne Artho hat die Datenschutzstelle auf Ende Juni verlassen. Als neuer Mitarbeiter konnte Rechtsanwalt lic. iur. Carl-Rudolf Meier gewonnen werden. Er ist seit August mit einem Pensum von 60%[144] im Einsatz. Durch seine frühere Tätigkeit als Leiter des Justizamtes des Kantons Obwalden, wo er sich auch mit Fragen des Datenschutzes befasste, ist er mit Struktur, Aufgaben und Dienstleistungen einer kantonalen Verwaltung bestens vertraut, so dass er innerhalb kurzer Zeit eingearbeitet war. Durch diese Änderung hat sich das Dienstleistungsangebot der Datenschutzstelle wesentlich verbessert, ist doch nun auch bei Abwesenheit des DSB für Konstanz gesorgt.
Das DSB-Sekretariat wird nun bereits seit fünf Jahren von Hildegard Steiner von der Staatskanzlei betreut. An sie – wie auch an alle Mitarbeitenden der Staatskanzlei, die den DSB im Administrativen unterstützen – geht an dieser Stelle ein sehr herzliches Dankeschön!
Der Stellvertreter des DSB war wie bis anhin Landschreiber Dr. Tino Jorio.

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

140 Folgende Arbeitsgruppen sind zurzeit aktiv: «AG Informationstechnologie», «AG Gesundheit», «AG Statistik» sowie «AG Innere Sicherheit».

141 Schwyz hat eine Datenschutzkommission, Uri einen externen Anwalt und in Obwalden und Nidwalden befassen sich Verwaltungsmitarbeitende im Nebenamt mit Datenschutz.

142 Diese Bezeichnung umschreibt das Problem der unerwünschten elektronischen Post.

143 Legislative.

144 Bei einem Teil des Pensums handelt es sich um eine befristete Aushilfsstelle.

Übersicht des Aufwandes für die verschiedenen Tätigkeitsbereiche

Wofür hat der Datenschutzbeauftragte[145] im Berichtsjahr seine Arbeitszeit eingesetzt? Statistische Angaben wie Anzahl der Anfragen, der geführten Telefongespräche, der verfassten Stellungnahmen usw. sind nur beschränkt aussagekräftig. Der Arbeitsaufwand für ein einzelnes Geschäft kann je nach Komplexität zwischen 20 Minuten und 20 Stunden betragen. Im Folgenden deshalb eine Aufstellung der aufgewendeten Arbeitszeit nach thematischen Schwerpunkten:

Bereich	2003*	[2002]	[2001]	Hinweise				
Beratung/Auskunft/Information	48%	[40%]	[49%]	aufgeteilt nach:	kantonale Verwaltung	35%	[31%]	[40%]
					Gemeinden	7%	[4%]	[5%]
					Private	6%	[5%]	[4%]
Ausbildungsangebote	6%	[3%]	[4%]	Für kantonale und gemeindliche Verwaltungen [Schulung im Rahmen der XP-Umstellung; Referate/Präsentationen usw.]				
Betreuung grösserer Projekte	13%	[13%]	[21%]	Register Datensammlungen, Tätigkeitsbericht 2002, Rechenschaftsbericht und Beitrag GVP				
Begleitung Datenschutzgesetz	1%	[1%]	[1%]	Verfassen von Merkblättern				
Öffentlichkeitsarbeit	11%	[11%]	[8%]	Internet-Auftritt, Medienarbeit, Mailing-Liste				
Zusammenarbeit mit Eidg. DSB und kantonalen DSB	3%**	[14%**]	[5%]	Informationsaustausch, Teilnahme an den Veranstaltungen des Vereins «DSB+CPD.CH»				
Weiterbildung	3%	[4%]	[1%]	Tagungsbesuche [insbesondere im Bereich der IT-Security]				
Diverses	15%	[14%]	[11%]	Korrespondenz, Rechnungswesen, Betreuung der eigenen EDV-Infrastruktur, Bibliothek, Besprechungen – soweit nicht direkt einzelnen Projekten zuweisbar				
Total	100%	[100%]	[100%]					

*** In % der Arbeitszeit [Pensum: Januar bis Juli 75%, seit August 60%]**

** Zur starken Abweichung in diesem Bereich: Im Jahr 2002 organisierte der DSB die Jahreskonferenz der schweizerischen Datenschutzbeauftragten und war zudem Leiter der «Arbeitsgruppe Sicherheit» [aufgegeben per 31. Dezember 2002]. Die im Berichtsjahr frei gewordenen Kapazitäten wurden in die Bereiche «Beratung» und «Ausbildung» investiert.

145 Unter Ausschluss der Projektleitung «Register der Datensammlung» [20%-Pensum].

Dank!

Nicht der Datenschutzbeauftragte setzt den Datenschutz um – vielmehr machen dies die Mitarbeitenden der Verwaltungen bei ihrer täglichen Arbeit. Der Datenschutzbeauftragte bietet Dienstleistungen an, damit die Datenschutzvorschriften durch die Mitarbeitenden korrekt umgesetzt werden und dadurch die Privatsphäre der Zuger Bürgerinnen und Bürger respektiert wird.

Stellen sich Probleme, muss gemeinsam nach einer Lösung gesucht werden. Es hat sich in den letzten fünf Jahren gezeigt, dass dies nicht immer ganz einfach ist. Werden für die Mitarbeitenden der Verwaltung durch die Vorgaben des Datenschutzes gewisse Arbeitsabläufe erschwert, so darf nicht vergessen werden, dass die Verwaltung die Daten der Zuger Bevölkerung nur zu treuhänderischer Verwaltung übertragen erhält. Die Datenherrschaft bleibt jedoch grundsätzlich bei der Bevölkerung. Mit den Daten in jeder Beziehung rechtmässig und sorgfältig umzugehen und den Schutz der Privatsphäre von Bürgerinnen und Bürgern zu gewährleisten, muss deshalb für die Verwaltung *zentrales Anliegen* sein.

Die Arbeit als Datenschutzbeauftragter wäre ohne die angenehme, interessierte und kooperative Zusammenarbeit kantonaler und gemeindlicher Stellen aller Stufen nicht möglich. Es ist mir deshalb ein grosses Bedürfnis, allen Personen für diese Zusammenarbeit in den letzten Jahren sehr herzlich zu danken!

Mein Dank geht auch an sämtliche Mitarbeitende der Staatskanzlei, wo die Datenschutzstelle «Kost und Logis» hat, für die in jeder Beziehung äusserst angenehme und kollegiale Zusammenarbeit. Insbesondere natürlich geht mein Dank an Hildegard Steiner, welche das DSB-Sekretariat im Jahr 2003 kompetent betreute.

Auch in diesem Jahr arbeiteten bei der Datenschutzstelle mit sehr viel Engagement und Erfolg Yvonne Artho [bis Juni], Christine Andres [bis März] und Carl-Rudolf Meier [ab August] am Abschluss des wichtigen Projekts des Registers der Datensammlungen. Ihnen sei dafür – und für alle weiteren tatkräftigen Unterstützungen – ganz herzlich gedankt.

Abschliessend geht ein grosses Dankeschön an Landschreiber Dr. Tino Jorio: Er stand im Berichtsjahr nicht nur als Stellvertreter des Datenschutzbeauftragten zur Verfügung, sondern war vielmehr auch ein stets interessierter, engagierter und nicht zuletzt kritischer Gesprächspartner in Sachen Datenschutz.

Sachregister

www.datenschutz-zug.ch

Gestaltung:
Christen Visuelle Gestaltung, Zug

Auflage: 3'000 Expl.

Druck: Speck Print AG, Zug

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