Tätigkeitsbericht 2017

Datenschutzbeauftragte des Kantons Zug

Kanton Zug

Gemäss § 19 Abs. 1 Bst. h des Datenschutzgesetzes des Kantons Zug (DSG; BGS 157.1) erstattet die Datenschutzbeauftragte dem Kantonsrat jährlich Bericht über ihre Tätigkeit und vertritt den Bericht im Kantonsrat. Der Bericht wird veröffentlicht.

Der vorliegende Bericht bezieht sich auf das Kalenderjahr 2017.

In Umsetzung des Entlastungsprogramms 2015–2018 wird der Tätigkeitsbericht nur noch als PDF-Dokument über die Website der Datenschutzbeauftragten (www.datenschutz-zug.ch) veröffentlicht.

Zug, im April 2018

Inhaltsverzeichnis

2017 – Haben 30 000 Datenschützer versagt? 4

1. Beispiele aus der Beratungs- und Aufsichtstätigkeit 5

- Beratung bei IT- und Digitalisierungsprojekten 5
- Fall 1: Antolin – Lesehilfe für die Kleinsten 5
- Fall 2: Einwohnerkontrolle – Wann kann eine Datensperre durchbrochen werden? 6
- Fall 3: Darf die Gemeinde Kundengespräche aufzeichnen? 7
- Fall 4: Bekanntgabe von Fahrzeughalterdaten für ein Forschungsprojekt 8
- Weitere Fälle 9

2. Kontrollen 10

3. Spezialgesetzliche Aufgaben 11

4. Schulung und Öffentlichkeitsarbeit 13

5. Mitwirkung an der Gesetzgebung, Vernehmlassungen und Mitberichte 15

6. Zusammenarbeit mit anderen Datenschutzstellen 19

7. Personal, Finanzen und Statistik 20

2017 – Haben 30 000 Datenschützer versagt?

Jüngst verkündete die Stadt Zug, dass mit der Blockchain-basierten digitalen ID «jeder sein eigener Datenschützer» sei. Kurz darauf konnten wir alle den Medien entnehmen: Der Facebook-Skandal und Datenklau durch Cambridge Analytica war grösser als angenommen. Kritiker, die das problematische «Absaugen» von Facebook-Daten längst anprangerten, wurden jahrelang als Schwarzmaler und Wirtschaftsschädlinge hingestellt. Nun wurden auch Daten von rund 30 000 Personen aus der Schweiz missbräuchlich abgesaugt. Haben alle diese Datenschützer versagt?

Vom Facebook-Skandal sind weltweit geschätzt 87 Millionen Nutzerinnen und Nutzer betroffen. Für die Datenschutzbehörden in ganz Europa sind die letzten Enthüllungen um Wahlmanipulationen und Datenmissbrauch eher eine Bestätigung denn eine Offenbarung. Sie weisen seit Jahren darauf hin, dass Nutzerinnen und Nutzer sorgfältiger mit ihrer Privatsphäre umgehen sollten und Internetgiganten einer stärkeren Datenschutzkontrolle zu unterstellen sind.

Hilfe verspricht da auf den ersten Blick die Blockchain-Technologie. Daten sollen in der Herrschaft der Nutzerinnen und Nutzer bleiben. Alles wunderbar, jeder wäre sein eigener Datenschützer. Wirklich? Wer hätte 2004 bei der Gründung von Facebook gedacht, dass es einst Wahlmanipulationen begünstigen kann? Und wie sieht es mit einer Blockchain-basierten digitalen ID aus? Wir wissen es aus heutiger Sicht schlicht und einfach nicht.

Was uns aber bewusst sein sollte: Jedes Streben nach mehr Digitalisierung in unserem (Behörden-)Alltag setzt vertiefte Vorabklärungen von Datenschutzfragen und einen noch sorgfältigeren Umgang mit Personendaten voraus. *Digitalisierung braucht einen wirksamen Datenschutz! Nicht um zu verhindern, sondern um zu lenken.*

Darum:

- Um den Wirtschaftsstandort Schweiz und insbesondere auch den Kanton Zug nachhaltig stark zu halten, braucht es bei Bund und Kantonen griffige und einfache Datenschutzgesetze, die mit den europäischen Vorgaben auch tatsächlich mithalten können.
- Gute und einfache Lösungen sind gefragt. Die Wirtschaft hat die Bedeutung des Datenschutzes erkannt – unzählige Firmen und Anwaltskanzleien suchen nun Datenschutzspezialistinnen und -spezialisten und beginnen die grossen Wissenslücken zu füllen.

Will man Datenschutz richtig umsetzen, braucht es Weitblick und den frühzeitigen Einbezug der Datenschutzbeauftragten – bevor Digitalisierungsprojekte gestartet werden. Der Facebook-Skandal hat gezeigt, wie unwissend und unbedarft die Bevölkerung zum Teil ist. Deshalb ist Datenschutz auch auf kantonaler und Gemeindeebene wichtig, hier liegt die Verantwortung für die Personendaten noch höher. Digitalisierungsprojekte dürfen nicht nur unter dem Aspekt Kostenersparnis und Verfügbarkeit betrachtet werden, sondern müssen auch unter dem Aspekt des Datenschutzes gesteuert werden.

Cloud, Blockchain und Künstliche Intelligenz stellen uns alle vor neue Herausforderungen.

Viele Nutzerinnen und Nutzer haben ihre Accounts bei Facebook mittlerweile gelöscht, weil ihnen das Vertrauen fehlt. Eine solche Wahl haben unsere Bürgerinnen und Bürger beim Staat nicht. Sie verdienen es, dass Datenbearbeitungen sicher und korrekt erfolgen. Dies wird aber nicht erreicht, indem man den Datenschutz schwächt oder die Datenschutzbehörden aussen vor lässt.

Die Herausforderungen der Digitalisierung lassen sich nur gemeinsam meistern.

Dr. iur. Claudia Mund
Datenschutzbeauftragte des Kantons Zug

1. Beispiele aus der Beratungs- und Aufsichtstätigkeit

Beratung bei IT- und Digitalisierungsprojekten

Die Digitalisierung schreitet auch in der kantonalen und gemeindlichen Verwaltung voran. Im Berichtsjahr wurden wir unter anderem bei folgenden IT-Projekten beratend beigezogen:

- Neue Steuersoftware für die Steuerverwaltung
- Neues Personalinformationssystem für Kanton und Gemeinden
- Neue kantonale, zentrale Datenaustauschplattform
- Pilotprojekt zur Einführung eines Predictive-Policing-Tools bei der Zuger Polizei

Zudem erhielten wir diverse Anfragen zum Einsatz von Cloud-Anwendungen in der öffentlichen Verwaltung und bei privaten Institutionen mit Leistungsvereinbarungen.

An folgenden Dokumenten haben wir mitgearbeitet oder eine Stellungnahme abgegeben:

- Charta zur Nutzung von digitalen Medien an den Stadtschulen Zug
- ICT-Strategie gemeindliche Schulen des Kantons Zug (2018–2022)
- IT-Governance des Kantons Zug

Übrigens:
IT- und Digitalisierungsprojekte sind gemäss § 19a DSG der Datenschutzbeauftragten *vorgängig zur Stellungnahme vorzulegen*. Diese sogenannten *Vorabkontrollen* tragen dazu bei, dass Datenschutz und Informationssicherheit bereits in der Projektphase berücksichtigt werden. Dadurch lassen sich Fehlinvestitionen und kostspielige Nachkorrekturen vermeiden. Dieses Instrument des *präventiven Datenschutzes* wird von den verantwortlichen Organen aus Sicht der Datenschutzbeauftragten (noch) zu wenig beachtet.

Fall 1
Antolin – Lesehilfe für die Kleinsten

Antolin verspricht Lesespass für Kinder von der 1. bis zur 10. Klasse. Das aus Deutschland stammende Online-Portal bietet Quizfragen zu Kinder- und Jugendbüchern, erstellt Ranglisten und erteilt Urkunden. Schülerinnen und Schüler können über das Internet Quizfragen beantworten und dabei Punkte sammeln, auch in ihrer Freizeit. Lehrpersonen können die Lesefortschritte online überprüfen. Um Antolin nutzen zu können, muss entweder die Schule (für alle Klassen) oder eine Lehrperson (für eine bestimmte Klasse) eine Lizenz erwerben. Über die Schule oder die Lehrperson werden die Schülerinnen und Schüler angemeldet. Gleichzeitig wird ein eigenes Benutzerkonto für jedes Kind errichtet (inklusive Postbox). Privatpersonen können keine Lizenz erwerben. Auch Zuger Schulen setzen Antolin zur Leseförderung ein.

Wir wurden von der Direktion für Bildung und Kultur (DBK) angefragt, was es bei der Anmeldung zu Antolin zu beachten gilt. Insbesondere ging es um die Frage, ob eine Schule oder Lehrperson ohne Information, Einwilligung und Wissen der Eltern ein Mitgliederkonto mit personalisierten Zugangsdaten und Login bei Antolin eröffnen darf.

Wird *schuleigenes Unterrichtsmaterial* zur Erfüllung des gesetzlichen Ausbildungsauftrags eingesetzt und werden dabei Personendaten von Schülerinnen und Schülern *schulintern* bearbeitet, braucht es *keine Einwilligung* der Erziehungsberechtigten. Bei Antolin ist dies nicht der Fall. Hier werden Personendaten von Schülerinnen und Schülern an *einen Dritten ausserhalb der Schule* bekannt gegeben.

Wir haben der DBK geraten, auf die Bekanntgabe von Vorname und Nachname von Schülerinnen und Schülern bei der Eröffnung eines Benutzerkontos *zu verzichten*. Die Datenschutzrichtlinien von Antolin und die AGB der Betreiberfirma, ein Schulbuchverlag, weisen darauf hin, dass Schü-

leranmeldungen auch unter einem Pseudonym oder Spitznamen des Kindes vorgenommen werden können. Werde davon abgesehen und ein Kind mit Name und Vorname angemeldet, so sei *vorgängig die Einwilligung der Erziehungsberechtigten einzuholen*. Dem ist zuzustimmen. Selbst wenn die Anmeldung nur mit Name und Vorname erfolgt, lassen sich über die Schul- oder Klassenlizenzen Rückschlüsse auf das Leseverhalten (und allenfalls Freizeitverhalten der Familie) eines bestimmten Kindes ziehen und von Antolin auf Servern ausserhalb der Schweiz auswerten. Dafür braucht es die Einwilligung der Erziehungsberechtigten.

Zudem haben wir empfohlen, die Erziehungsberechtigten proaktiv und transparent über den Einsatz von Antolin als Leseförderprogramm in der Schule oder Freizeit, inklusive Punkte- und Belohnungssystem, zu informieren. Antolin stellt den Schulen dazu einen Musterbrief zur Verfügung.

Da es sich bei Antolin mutmasslich um eine Cloud-Lösung handelt, haben wir zusätzlich auf die Verantwortung der Schulen zur Gewährleistung des Datenschutzes und der Informationssicherheit bei Auslagerung von Personendaten in eine Cloud hingewiesen (vgl. § 6 DSG).

Übrigens:
Die Datenschutzstelle empfiehlt den Schulen bei externen Plattformen, wenn immer möglich weder die tatsächlichen Namen noch die privaten E-Mail-Adressen von Schülerinnen und Schülern zu verwenden, sondern auf *Pseudonyme oder unpersönliche E-Mails* auszuweichen (zum Beispiel Schüler1@SchuleXY.ch; ProjektXY@SchuleXY.ch). Denn zur Medienkompetenz gehört auch, dass Schülerinnen und Schüler den sorgfältigen Umgang mit ihren eigenen Personendaten lernen und ihre Privatsphäre schützen.

Fall 2
Einwohnerkontrolle – Wann kann eine Datensperre durchbrochen werden?

Wer nicht will, dass seine persönlichen Angaben (insbesondere die Adresse), über welche die Gemeinde verfügt, an Privatpersonen bekannt gegeben werden, kann seine Daten bei der Einwohnerkontrolle kostenlos und ohne Begründung sperren lassen (§ 9 Abs. 1 DSG). Die Datensperre wirkt nur gegenüber *Anfragen privater Personen (auch Firmen)*. Verwaltungsstellen, die für die Erfüllung ihrer gesetzlichen Aufgaben auf diese Daten angewiesen sind, erhalten auch gesperrte Daten.

Mit einer Datensperre lässt sich zum Beispiel unterbinden, dass eine private Person bei der Einwohnerkontrolle voraussetzungslos die aktuelle Adresse, bei Wegzug auch das Wegzugsdatum und den Wegzugsort, erfragen kann. Bei Glaubhaftmachung eines Interesses kann über die Einwohnerkontrolle auch der Zuzugsort in Erfahrung gebracht werden (vgl. § 8 Abs. 2 Bst. a und b DSG). Besteht eine Datensperre, werden auch dann keine Auskünfte erteilt, wenn die Bekanntgabe im Sinne der nachgefragten Person sein könnte (wie Adressanfragen für Klassenzusammenkünfte; zur Kontaktaufnahme früherer Bekannter).

Immer wieder wenden sich Gemeinden an uns, wenn nahe Verwandte, Angehörige oder andere private Personen (wie Schuldner oder Inkassobüros) eine Adressauskunft trotz Datensperre bei der Einwohnerkontrolle erfragen. Was ist zu tun?

Eine Datensperre gestützt auf § 9 DSG *gilt nicht absolut*: Sie kann unter bestimmten Voraussetzungen durchbrochen werden, namentlich wenn die gesuchstellende Person glaubhaft macht, dass sie dadurch behindert wird, schutzwürdige Ansprüche gegenüber der betroffenen Person geltend zu machen. Schutzwürdige Rechtsansprüche können etwa dort vorliegen, wo ein Schuldner weggezogen ist und noch offene For-

derungen bestehen und/oder beim zuständigen Betreibungsamt eine Betreibung eingereicht werden soll. Der Gedanke dahinter: Das Sperrrecht soll nicht dazu missbraucht werden können, dass sich etwa ein Schuldner seinen Gläubigern entzieht oder bestehende Rechtsansprüche vereitelt werden. *Der Rechtsmissbrauch wird nicht geschützt*.

Keine schutzwürdigen Rechtsansprüche liegen in der Regel vor, wenn nahe Verwandte oder Angehörige in Sorge um die betroffene Person nach dem aktuellen Aufenthaltsort fragen. Dafür stehen andere rechtliche Möglichkeiten (wie der Beizug der Kindes- und Erwachsenenschutzbehörde) zur Verfügung. Auch reicht es nicht aus, wenn der geltend gemachte Rechtsanspruch erst in Aussicht steht.

Die geltend gemachten Rechtsansprüche sind mittels eines Vertrags, eines Urteils oder einer Rechnung zu belegen. Kommt die Einwohnerkontrolle zum Schluss, dass schutzwürdige Ansprüche glaubhaft geltend gemacht werden konnten, und beabsichtigt sie, die Datensperre zu durchbrechen, so ist der betroffenen Person die Möglichkeit zu geben, sich zur Aufhebung der Datensperre zu äussern (vgl. § 9 Abs. 3 Bst. b DSG; *Anspruch auf rechtliches Gehör*). Dies geschieht unter Ansetzung einer Frist. Ist die betroffene Person nicht mit der Aufhebung der Datensperre einverstanden, so hat sie dies zu begründen. Nach Erhalt der Antwort nimmt die angefragte Stelle *eine Interessenabwägung* vor und erlässt einen begründeten Entscheid in Form einer anfechtbaren Verfügung. Bis zum Ablauf der Rechtsmittelfrist dürfen keine Daten bekannt gegeben werden.

Wird die Datensperre geschützt, darf die gesuchstellende Person aufgrund der Begründung nicht erkennen, wo die nachgefragte Person zum Beispiel ihren aktuellen Wohnsitz hat. Die Ablehnung des Gesuchs darf nicht dazu führen, dass die Einwohnerkontrolle der gesuchstellenden Person die erfragte Information indirekt bekannt gibt, was etwa mit der unglücklichen Formulierung «Die gesuchte Person hat in unserer Gemeinde eine Datensperre errichten lassen, weshalb wir Ihnen keine Auskunft geben können» der Fall sein könnte.

Fall 3
Darf die Gemeinde Kundengespräche aufzeichnen?

Eine Gemeindeverwaltung wollte von uns wissen, ob sie Gespräche mit Kundinnen und Kunden unter gewissen Bedingungen am Telefon oder an Sitzungen vor Ort aufzeichnen dürfe. Da es immer wieder schwierige Kundengespräche gäbe, wolle man die Aufzeichnungen nur in ganz spezifischen Situationen zu Beweiszwecken oder zur nachweislich korrekten Protokollierung von Sitzungen einsetzen.

Die Aufzeichnung von Gesprächen stellt ein Bearbeiten von Personendaten dar. Gemäss § 5 DSG sind solche Aufzeichnungen nur dann rechtmässig, wenn eine gesetzliche Grundlage die Aufzeichnung erlaubt oder – ausnahmsweise – die betroffene Person ausdrücklich und freiwillig ihre Einwilligung erteilt hat, nachdem sie vorgängig hinreichend über die Datenbearbeitung aufgeklärt wurde.

Im Kanton Zug gibt es nur wenige Rechtsgrundlagen, die den Einsatz von Aufzeichnungsgeräten ausdrücklich regeln. Einige davon betreffen die Protokollführung. Dazu gehören etwa § 20 Abs. 3 der Geschäftsordnung für die Schätzungskommission (BGS 162.32), § 24 Abs. 2 der Geschäftsordnung des Verwaltungsgerichtes (BGS 162.11) oder § 12 Abs. 4 der Geschäftsordnung des Kantonsrats (BGS 141.1). In der fraglichen Gemeinde sind keine entsprechenden Rechtsgrundlagen bekannt, deshalb kommt nur die *Einwilligung der Betroffenen im Einzelfall* in Betracht. Dabei ist Folgendes zu beachten:

- Angekündigte Aufnahmen von Gesprächen an Sitzungen oder von Telefongesprächen sind *nur ausnahmsweise und im Einzelfall* zulässig. Die betroffene Person ist vorgängig über den Verwendungszweck, die Zugriffsberechtigun-

gen und Löschvorschriften aufzuklären. Gestützt darauf entscheidet die betroffene Person selbst, ob sie dem zustimmen will oder nicht. Zu beachten ist, dass eine allfällige Aufnahme zu den Akten gehört und der betroffenen Person gestützt auf § 13 DSG ein Auskunftsrecht bezüglich der Aufnahmen zusteht.
- Die Gesprächsbeteiligten können die Aufnahmen *jederzeit ablehnen*. Die Einwilligung muss freiwillig sein und darf nicht unter Zwang oder unter Androhung von Nachteilen (z.B. Gesprächsverweigerung) erfolgen.
- Die Löschfristen sind *so früh wie möglich* anzusetzen (vgl. § 4 Abs. 1 Bst. d DSG; Verhältnismässigkeit). Es gilt: Aufbewahrung nur so lange, wie zwingend nötig. Bei Sitzungsprotokollen beispielsweise sind die Aufzeichnungen zu löschen, sobald das Protokoll von beiden Seiten abgesegnet ist.

Fazit:
Die Aufzeichnung von Gesprächen mit Kundinnen und Kunden durch Gemeindemitarbeitende ohne ausreichende gesetzliche Grundlage oder ohne ausdrückliche Einwilligung der betroffenen Personen ist unzulässig. Zu beachten ist auch, dass Art. 179ter Strafgesetzbuch (StGB; SR 311.0) ein solches Verhalten auf Anzeige hin unter Strafe stellt. Angekündigte Aufnahmen von Gesprächen an Sitzungen oder von Telefongesprächen sind *nur ausnahmsweise und im Einzelfall zulässig*. Die Einwilligung muss freiwillig sein und darf nicht unter Zwang oder Androhung von Nachteilen erteilt werden. Vorgängig ist die betroffene Person hinreichend über die Datenbearbeitung aufzuklären. Die Aufzeichnungen gehören zu den Akten, und der betroffenen Person steht ein Auskunftsrecht zu.

Fall 4
Bekanntgabe von Fahrzeughalterdaten für ein Forschungsprojekt

Ein Forschungsinstitut einer schweizerischen Universität erfragte vom Strassenverkehrsamt eine Zufallsstichprobe von 5 000 Adressdatenstämmen von Fahrzeughalterinnen und -haltern des Kantons Zug. Das Institut beabsichtigte, mit den erhaltenen Adressen eine Direktbefragung bei den Halterinnen und -haltern über ihr Mobilitätsverhalten und ihre Einstellung zu energieeffizienten Autos durchzuführen. In einem zweiten Schritt sollte ermittelt werden, ob sich die Einstellung der Befragten nach Erhalt weiterer Informationen und der Möglichkeit von Probefahrten allenfalls verändert hat. Das Strassenverkehrsamt erkundigte sich bei uns über die Zulässigkeit und die Modalitäten der Datenbekanntgabe, unter Hinweis darauf, dass Art. 125 und 126 Verkehrszulassungsverordnung (VZV; SR 741.51) eine solche Datenbekanntgabe eigentlich nicht vorsehe.

Das Datenschutzgesetz «privilegiert» die Datenbearbeitung zu einem sogenannten *nichtpersonenbezogenen* Zweck und lässt eine Zweckänderung von erhobenen Personendaten unter gewissen Auflagen zu. So dürfen Personendaten für Forschung, Planung und Statistik bearbeitet werden, wenn sie anonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt, wenn sie nicht weitergeben werden und wenn die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind (§ 4 Abs. 1 Bst. e DSG). Eine Pflicht zur Datenbekanntgabe besteht für die angefragte Verwaltungsstelle nicht. Sie muss aber eine rechtsgleiche Behandlung der eingegangenen Gesuche sicherstellen. Im vorliegenden Fall standen somit Art. 125 und 126 VZV einer Datenbekanntgabe zu Forschungszwecken grundsätzlich nicht entgegen (Ausnahme: gesperrte Halteradressen, siehe weiter unten).

Im besagten Forschungsprojekt ging es nicht darum, dass das Forschungsinstitut bereits erhobene Daten oder Unterlagen vom Strassen-

verkehrsamt erhalten und diese zu einem nichtpersonenbezogenen Zweck wissenschaftlich auswerten wollte. Vielmehr erfragte das Institut eine Stichprobenziehung von Adressdatenstämmen von Fahrzeughalterinnen und -haltern, um bei diesen Personen eine Direktbefragung durchführen und somit *selbst neue Daten zur wissenschaftlichen Auswertung erheben zu können*. Auch wenn somit die Stichprobenziehung klar zu einem personenbezogenen Zweck (persönliches Anschreiben und Versand von Umfrageunterlagen) erfolgt, ist dies unter Einhaltung gewisser Bedingungen und Auflagen möglich. Wir haben dem Strassenverkehrsamt zu folgendem Vorgehen geraten:

- Die Stichprobenziehung erfolgt durch das Strassenverkehrsamt.
- Gesperrte Halterdaten dürfen für die Stichprobenziehung nicht verwendet werden.
- Vorzugsweise erfolgt der Versand der Umfrageunterlagen durch das Strassenverkehrsamt (unter allfälliger Kostenfolge für das Forschungsinstitut).
- Alternativ kann der Versand der Umfrageunterlagen für das vorliegende Forschungsprojekt auch direkt durch das Institut erfolgen, da es sich hier «nur» um die Bekanntgabe von Adressdaten und um keinen «sensiblen» Forschungsbereich handelt (anders zu beurteilen wäre die Situation beispielsweise bei einem Forschungsprojekt, das die Lebensumstände von Pflegekindern bei ihren Pflegeeltern mittels eines Fragebogens oder einer Direktbefragung untersuchen wollte; hier sollte die Verwaltungsstelle die betroffenen Personen zuerst fragen, ob sie am Projekt überhaupt teilnehmen wollen oder nicht und ob sie mit der Bekanntgabe ihrer Adressen zwecks Kontaktaufnahme durch das Forscherteam einverstanden sind oder nicht).
- Die Adressen sind verschlüsselt oder auf dem Postweg zu übermitteln.
- Jede Person, die im Rahmen des Forschungsprojektes die Adressen bearbeitet, muss zuhanden des Strassenverkehrsamtes eine *Verpflichtungserklärung* zur Einhaltung des Datenschutzes und zur Beachtung der datenschutzrechtlichen Auflagen ausfüllen und unterzeichnen (die Datenschutzstelle stellt dafür Muster zur Verfügung).

Das Strassenverkehrsamt entschied sich für die alternative Variante und somit für den Versand der Umfrageunterlagen durch das Forschungsinstitut.

Weitere Fälle

Aus Ressourcengründen musste die Datenschutzbeauftragte erstmalig auf die Einreichung von Beiträgen in der «Gerichts- und Verwaltungspraxis (GVP) des Kantons» verzichten. Für das Jahr 2017 konnten keine Fälle zur Publikation aufbereitet werden.

Bei den GVP-Beiträgen handelt es sich um umfangreichere Stellungnahmen der Datenschutzbeauftragten. Sie sind unter www.zg.ch auf der Seite der Staatskanzlei aufgeschaltet – reinschauen lohnt sich!

2. Kontrollen

Es gehört zu den gesetzlichen Aufgaben der Datenschutzbeauftragten, dass sie bei den Organen die Einhaltung der Datenschutzvorschriften in rechtlicher, technischer und organisatorischer Hinsicht kontrolliert.

Im Berichtsjahr hat die Datenschutzbeauftragte bei der Zuger Polizei eine Kontrolle der Zugriffe auf das Schengener Informationssystem (SIS), eine sogenannte *Schengen-Kontrolle*, an die Hand genommen. Die erste und zugleich letzte Schengen-Kontrolle fand in den Jahren 2009/10 statt. Eigentlich wären die Datenschutzstellen der Kantone und des Bundes verpflichtet, solche Kontrollen bei denjenigen Organen respektive Verwaltungsstellen, die auf das SIS Zugriff haben, jährlich durchzuführen. Die Kontrolle war somit mehr als überfällig.

Wir beauftragten das gleiche Unternehmen, das bereits die erste Schengen-Kontrolle in den Jahren 2009/10 bei der Zuger Polizei durchgeführt hatte. Das externe Unternehmen verfügte bei dieser Kontrolle nicht nur über ein wertvolles Vorwissen, sondern auch über fundiertes Wissen im Bereich Datenschutz-Audits. Zahlreiche kantonale Datenschutzbeauftragte arbeiten seit mehreren Jahren mit besagtem Unternehmen zusammen.

Da die Endergebnisse der Schengen-Kontrolle Ende des Berichtsjahres noch nicht vollständig ausgewertet waren, werden wir im nächsten Tätigkeitsbericht ausführlicher darüber berichten.

3. Spezialgesetzliche Aufgaben

Online-Zugriffe

Der elektronische Zugriff auf Personendaten im Abrufverfahren (auch *Online-Zugriff* genannt) ist in der Verordnung über das Bewilligungsverfahren für den elektronischen Datenaustausch (Online-Verordnung; BGS 157.22) geregelt.

Damit eine Verwaltungsstelle im Abrufverfahren auf Personendaten einer anderen Verwaltungsstelle zugreifen darf – und sich so quasi mit «fremden» Daten bei der anderen Stelle «bedienen» kann – braucht es entweder eine ausdrückliche gesetzliche Grundlage oder eine Bewilligung von der zuständigen Instanz (je nach Datensammlung: oberste Exekutiv- oder Gerichtsbehörde). Das Bewilligungsverfahren folgt einem gesetzlich vorgegebenen Ablauf. Gesuchsformular und Ablaufschema sind auf unserer Website abrufbar (www.datenschutz-zug.ch, Rubrik «Services»).

Als elektronische Zugriffe im Abrufverfahren gelten zum einen Online-Zugriffe über *eine Benutzeroberfläche beziehungsweise ein Webportal* (Mensch-zu-Maschine-Interaktion). Sie erlauben einer oder mehreren berechtigten Personen den direkten Zugriff auf einen Datenbestand einer anderen Verwaltungsstelle. Anderseits gehören zu den Abrufverfahren auch sogenannte *Webservices*, bei denen Schnittstellen so eingerichtet werden, dass die Daten aus einem System einem anderen System in einem lesbaren Format zur Verfügung gestellt werden (Maschine-zu-Maschine-Interaktion). Und schliesslich handelt es sich auch bei der *periodischen und automatisierten Zurverfügungstellung von Listen* um einen elektronischen Zugriff im Abrufverfahren, wofür eine Online-Bewilligung einzuholen ist. Auch hier erfolgt der Datenzugriff ohne Zutun des für die Datensammlung verantwortlichen Organs.

Online-Gesuche sind der Datenschutzstelle vorgängig zur Stellungnahme vorzulegen. Im Berichtsjahr hatte die Datenschutzbeauftragte einen markanten Anstieg an Beratungsaufwand rund um Online-Zugriffe zu verzeichnen: Die Einführung der neuen Einwohnerkontrollsoftware (NEST) und die anstehende Ablösung der zentralen Personenkoordination (ISOV ZPK) durch eine neue kantonale, zentrale Datenaustauschplattform (GERES) hat zahlreiche datenschutzrechtliche Fragen betreffend Online-Zugriffe und Bewilligungen aufgeworfen. Diverse Verwaltungsstellen haben sich bei der Datenschutzbeauftragten gemeldet und nach Antworten verlangt. Gemeinsam mit den verantwortlichen Organen und den Informatikdienstleistungserbringern haben wir Antworten und gangbare Lösungen gesucht.

Videoüberwachung

Seit Inkrafttreten der Videoüberwachungsverordnung (VideoV; BGS 159.11) ist der Einbezug der Datenschutzstelle bei Gesuchen um Bewilligung einer Videoüberwachungsanlage von kantonalen oder gemeindlichen Organen ausdrücklich vorgeschrieben (§ 1 Abs. 2 VideoV). Der Einbezug erfolgt einerseits durch Beratungen bei der Planung von Videoüberwachungen und andererseits durch eine schriftliche Stellungnahme der Datenschutzbeauftragten zu einem konkreten Gesuch, bevor dieses der zuständigen Instanz zur Bewilligung vorgelegt wird (vgl. auch § 19a DSG; Vorabkontrolle).

Im Berichtsjahr haben wir zu zwei Videoüberwachungsgesuchen eine ausführliche Stellungnahme abgegeben. Eine davon betraf die Videoüberwachung der Zuger Polizei im Bereich Bahnhof und Bossard Arena (Fanmeile). Unsere Kritik bezüglich der Verhältnismässigkeit der geplanten Videoüberwachung blieb weitgehend unberücksichtigt. Gegen die vom Regierungsrat erteilte Bewilligung wurde vor Verwaltungsgericht Beschwerde erhoben. Der aktuelle Verfahrensstand ist uns nicht bekannt. Das zweite Videoüberwachungsgesuch betraf das Parkhaus der Zentrumsüberbauung Dreiklang in Steinhausen. Der Gemeinderat hat die Videoüberwachungsanlage zwischenzeitlich bewilligt; der Entscheid ist rechtskräftig. Die Stellungnahme beziehungsweise die Empfehlungen der Datenschutzbeauftragten wurden vom Gemeinderat vollumfänglich berücksichtigt.

Im Fall einer bereits seit mehreren Jahren in Betrieb stehenden Videoüberwachungsanlage haben wir aus Ressourcengründen auf eine Stel-

lungnahme verzichtet. In drei weiteren Fällen haben wir die Gesuchsteller in der Planungsphase beraten.

Übrigens:
Auf der Website der Datenschutzbeauftragten sind alle rechtskräftig erteilten Bewilligungen für Videoüberwachungsanlagen des Kantons und der Gemeinden aufgeschaltet, einschliesslich der Angaben zu den Aufnahmebereichen (www.datenschutz-zug.ch, Rubrik «Services»).

4. Schulung und Öffentlichkeitsarbeit

Schulungen

Die Datenschutzbeauftragte hat im Berichtsjahr 5 Schulungen (2016: 4) von unterschiedlicher zeitlicher Intensität für die kantonale Verwaltung und die Gemeinden durchgeführt:

- «Die Verwaltung kennen lernen»: An zwei Nachmittagen auf das Jahr verteilt durfte die Datenschutzbeauftragte ihre Arbeit und die Grundprinzipien des Datenschutzrechts neuen Mitarbeitenden in der Verwaltung näherbringen. Die 40-minütige Präsentation baut auf konkreten Praxisbeispielen aus dem Behördenalltag auf.
- «Open Data – Big Data»: Auf Anfrage des Amtes für Informatik- und Organisation (AIO) hat die Datenschutzbeauftragte im Rahmen der internen Veranstaltungsreihe «StayUp2Date» interessierten Mitarbeitenden des Amtes die Chancen und Herausforderungen der zunehmenden Digitalisierung in der öffentlichen Verwaltung aufgezeigt. Die anschliessende Diskussion zeigte, dass datenschutzrechtliche Fragestellungen rund um die Digitalisierung auch bei Mitarbeitenden aus Informatik und Technik auf grosses Interesse stossen.
- «Schule & Recht – Umgang mit dem Datenschutz»: Auf Anfrage der Schulleitung Kirchmatt wurde die Datenschutzbeauftragte eingeladen, im Rahmen des Präsenznachmittags den anwesenden Lehrpersonen die Dos und Don'ts im Umgang mit Schülerdaten näherzubringen. Unterstützt wurde die Datenschutzbeauftragte vom Leiter Schulaufsicht des Amtes für gemeindliche Schulen. Die Rückmeldung der Schulleitung Kirchmatt war durchwegs positiv: Der Nachmittag habe viel Klarheit und Sicherheit in den Schulalltag gebracht.
- «Schule & Recht – Datenschutz-Leitfaden für die gemeindlichen Schulen»: Im Nachgang zur Neuauflage des Datenschutz-Leitfadens für die Schulen (wir berichteten darüber bereits im Tätigkeitsbericht 2016, S. 11), wurden wir von der Schule Oberägeri eingeladen, den Leitfaden direkt an der Gesamtkonferenz den Lehrpersonen vorzustellen. Da der Leitfaden als Sensibilisierungstool gedacht ist und nicht auf alle Fragen im Schulalltag eine Antwort liefern kann, wurden die brennendsten Fragen der Lehrpersonen vorgängig gesammelt. Das Referat der stellvertretenden Datenschutzbeauftragten und die integrierten Beispiele aus dem Schulalltag waren gemäss Rückmeldung noch lange Gesprächsthema und wirkten positiv nach.

Die Kaderweiterbildung «Datenschutz und Datensicherheit – Datenschutzkompetenz direktionsspezifisch auf den Punkt gebracht!» fand auch in diesem Berichtsjahr keine Fortsetzung. Sobald es die Ressourcensituation in den Direktionen wieder erlaubt, wird die Datenschutzbeauftragte die Fortsetzung des Kurses an die Hand nehmen.

Zusätzlich zu obigen verwaltungsinternen Schulungen hat die Datenschutzbeauftragte im Berichtsjahr an 3 externen Veranstaltungen teilgenommen, die sich den Chancen und Herausforderungen der Digitalisierung widmeten:

- «Big Data – Segen oder Fluch?»: Podiumsdiskussion auf Einladung der Schweizerischen Akademie der Technischen Wissenschaften (SATW) im Rahmen des «Digital Festivals Zürich 2017».
- «Open Data, Big Data: Big Problem?»: Referat mit anschliessender Diskussion auf Einladung des Efficiency Clubs Zug.
- «Big Data – Arbeit – Leadership: Welche digitale Zukunft wollen wir?»: Podiumsdiskussion am Herbst-Symposium des Lassalle-Instituts, Bad Schönbrunn, in Edlibach.

Medienkontakte

Im Berichtsjahr erhielt die Datenschutzbeauftragte insgesamt 11 Anfragen (2016: 12) von Zeitungen, Onlinemagazinen und Radiostationen, unter anderem zu folgenden Themen:

- Einsatz von Drohnen zur Aufdeckung von illegalen Bauten sowie zu Verkehrserhebungen aus der Luft
- Videoüberwachung im Kanton Zug
- Einsatz der Software «Ra-Prof» (*Ra*dicalisation *Pro*filing) im schulischen Umfeld

– Fragen zur Passwortsicherheit
– Revision des Datenschutzgesetzes des Bundes

Publikationen

Im Berichtsjahr haben wir an den folgenden 4 Publikationen (2016: 3) mitgewirkt:

– Personalziitig: Beitrag zum Thema «Neue Medien und Datenschutz». Das Thema wurde aufgrund des übergeordneten Themas «Alte und Neue Medien» der entsprechenden Ausgabe ausgewählt. Der Beitrag beleuchtet Fragen rund um das Recht am eigenen Bild (insbesondere auch von Minderjährigen) und Veröffentlichung von Fotografien via Facebook, Twitter und Co.
– Fachzeitschrift Spielgruppe: Beitrag über «Datenschutz und Soziale Medien» im Umfeld von Spielgruppen.
– Gerichts- und Verwaltungspraxis des Kantons Zug (GVP): Für die GVP 2016 haben wir im Berichtsjahr 2 Stellungnahmen (2016: 4) aus unserer Beratungspraxis publiziert.
– Schulinfo: Informationsbeitrag zum neuen «Datenschutz-Leitfaden für die gemeindlichen Schulen».

Übrigens:
Der neue «Datenschutz-Leitfaden für die gemeindlichen Schulen» steht nun allen Lehrpersonen als Druckbroschüre (Bestellung über die Lehrmittelzentrale des Kantons Zug) oder als PDF-Download unter www.datenschutz-zug.ch (Rubrik «Services») zur Verfügung.

5. Mitwirkung an der Gesetzgebung, Vernehmlassungen und Mitberichte

Im Rahmen ihres gesetzlichen Auftrags nimmt die Datenschutzbeauftragte aus datenschutzrechtlicher Sicht Stellung zu kantonalen und gemeindlichen Vorlagen und Vorlagen des Bundes.

Nach wie vor sehr erfreulich ist die frühzeitige Einbindung der Datenschutzbeauftragten in die Gesetzgebungsarbeiten sowie die gute Zusammenarbeit mit den Juristinnen und Juristen in den Direktionen und Ämtern. Bei Vorlagen mit einer hohen Datenschutzrelevanz erfolgte der Einbezug der Datenschutzbeauftragten, wie schon in den vergangenen beiden Jahren, bereits vor dem internen Mitberichtsverfahren. Stellvertretend für die gute Zusammenarbeit seien die folgenden Beispiele herausgegriffen:

- Bei der Ausarbeitung der neuen *Justizvollzugsverordnung (JVV)* wurde die Datenschutzstelle bereits vor dem Mitberichtsverfahren vom Amt für Justizvollzug begrüsst. Dem Amt war es so möglich, die notwendigen datenschutzrechtlichen Fragen bei der Ausarbeitung der neuen Verordnung frühzeitig anzugehen. Im Mitberichtsverfahren konnte die Vorlage in Zusammenarbeit mit der federführenden Sicherheitsdirektion und dem Amt für Justizvollzug bereinigt werden. Der Regierungsrat konnte die Verordnung ohne Antragstellung der Datenschutzbeauftragten verabschieden. Die JVV ist am 24. März 2018 in Kraft getreten.
- Die Ablösung der zentralen Personenkoordination (ISOV ZPK) durch eine neue kantonale, zentrale Datenaustauschplattform (GERES) bedingt gesetzliche Anpassungen des *Einführungsgesetzes zum Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister (EG RHG)* und der zugehörigen Verordnung. Diese gesetzlichen Anpassungen sind Gegenstand des Teilprojekts Recht im Gesamtprojekt PARIS. Am Teilprojekt Recht beteiligen sich Vertreterinnen und Vertreter des Kantons und der Gemeinden. Die stellvertretende Datenschutzbeauftragte ist Mitglied dieser Arbeitsgruppe. Sie engagiert sich dort für die datenschutzkonforme Ausgestaltung der notwendigen gesetzlichen Anpassungen.
- In enger Zusammenarbeit mit der federführenden Sicherheitsdirektion hat die Datenschutzbeauftragte die Revision des *Datenschutzgesetzes des Kantons Zug (DSG)* an die Hand genommen. Die Revision erfolgt in Umsetzung der revidierten Datenschutzkonvention SEV 108 des Europarates und der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung (siehe dazu ausführlicher auf S. 16 f).

Die Datenschutzbeauftragte sieht in der Mitwirkung in der Gesetzgebung eine Schwerpunktarbeit, werden doch hier die Weichen für Datenbearbeitungen einer Vielzahl von Personen gestellt. Entsprechend viel Zeit fliesst in die Mitarbeit an der Gesetzgebung. Sofern es aus Ressourcengründen möglich ist, nehmen wir auch zu Bundesvorlagen Stellung.

Kantonale Vorlagen sowie parlamentarische Vorstösse

Im Berichtsjahr nahmen wir zu 10 kantonalen Vorlagen (2016: 12) Stellung:

- Änderung des Gesetzes über Denkmalpflege, Archäologie und Kulturgüterschutz (Denkmalschutzgesetz)
- Änderung des Polizeigesetzes (Verstärkung der Gewaltprävention)
- Teilrevision der Kantonsverfassung sowie des Verantwortlichkeitsgesetzes (Einführung eines Amtsenthebungsverfahrens)
- Teilrevision des Personalgesetzes (Umsetzung Postulat Thomas Werner; Anstellung nur mit Strafregisterauszug)
- Teilrevision des Kantonsratsbeschlusses über die Gebühren in Verwaltungs- und Zivilsachen (Verwaltungsgebührentarif)
- Revision des Datenschutzgesetzes (Umsetzung der revidierten Datenschutzkonvention SEV 108 des Europarates und der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung)
- Finanzhaushaltverordnung (FHV)
- Teilrevision der Kantonsverfassung sowie des Wahl- und Abstimmungsgesetzes (Umsetzung Motion Laura Dittli; Einführung einer Abstim-

mungshilfe für junge Erwachsene)
- Justizvollzugsverordnung (JVV)
- Teilrevision des Geoinformationsgesetzes (GeoIG-ZG)

Die Anträge der Datenschutzbeauftragten wurden grösstenteils berücksichtigt. Häufig bezogen sich unsere Anträge auf Fragen der Normstufe (Gesetz oder Verordnung) und Verhältnismässigkeit einer Datenbearbeitung sowie auf die Verbesserung der Transparenz für die betroffenen Personen.

Hinzu kam ein parlamentarischer Vorstoss (2016: 3):

- Kleine Anfrage von Philip C. Brunner – Was ist eigentlich jetzt wieder mit der Direktion des Innern los?

Revision Datenschutzgesetz

Die Datenschutzgesetze von Bund und Kantonen basieren auf Grundprinzipien, die in den 70er Jahren entwickelt wurden. Dass sich damit die heutigen Herausforderungen der Digitalisierung bei Weitem nicht mehr bewältigen lassen, hat die europäischen Staaten zu Reformen veranlasst. Die Schweiz ist als Mitglied des Europarats und als Schengen-Mitglied verpflichtet, diese *Reformen in ihr nationales Recht zu übernehmen*. Der Bundesrat hat die entsprechende Botschaft zur Totalrevision des Datenschutzgesetzes des Bundes am 15. September 2017 verabschiedet. Die Revision soll dem Bund erlauben, die revidierte Datenschutzkonvention SEV 108 des Europarates zu ratifizieren sowie die Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung zu übernehmen, wozu die Schweiz als Schengen-Mitglied verpflichtet ist.

Die Kantone müssen ihre Datenschutzgesetzgebung ebenfalls an die beiden Rechtsakte anpassen. Dazu hat die Konferenz der Kantonsregierungen (KdK) im Februar 2017 einen Leitfaden zuhanden der Kantonsregierungen erlassen. Er zeigt auf, *in welchem Umfang die Kantone ihre Datenschutzgesetze anpassen müssen*. Der KdK-Leitfaden enthält dazu vorformulierte Lösungsvorschläge.

Anpassungsbedarf besteht gemäss KdK-Leitfaden in den Kantonen insbesondere in folgenden Bereichen:

- Geltungsbereich: Grundsätzlich dürfen keine Ausnahmen mehr vom Geltungsbereich der Datenschutzgesetze vorgesehen werden. Für die Justiz und die Strafverfolgung sind spezielle Vorkehrungen zur Wahrung der Unabhängigkeit und zur Vermeidung von Kollisionen zwischen Datenschutzrecht und Verfahrens- oder Prozessrecht vorzusehen.
- Schutz für natürliche Personen: Der Schutz juristischer Personen soll wegfallen, da diese durch andere Erlasse ausreichend geschützt sind.
- Genetische und biometrische Daten: Sie sollen als neue Kategorien besonders schützenswerter Personendaten in die Datenschutzgesetze aufgenommen werden.
- Profiling: Der Begriff Profiling soll neu als besonders gefährliche Art der Bearbeitung von Personendaten in die Datenschutzgesetze aufgenommen werden. Ein Profiling unterliegt den gleich strengen Anforderungen wie das Bearbeiten von besonders schützenswerten Personendaten.
- Nachweis der Compliance: Die Verantwortung der Organe soll stärker betont werden. Auch müssen die Organe in Zukunft nachweisen können, dass sie die Datenschutzbestimmungen einhalten.
- Auftragsdatenbearbeitung: Die Voraussetzungen für die Auslagerung von Datenbearbeitungen an Dritte (beispielsweise in eine Cloud) sind klarer zu regeln. An die Auswahl des Dritten werden strengere Anforderungen gestellt.
- Datenschutz-Folgenabschätzung und Vorabkonsultation: Die europäischen Rechtsgrundlagen verlangen vom verantwortlichen Organ eine Datenschutz-Folgenabschätzung. Dadurch sollen die Risiken identifiziert und bewertet werden, die mit einer geplanten Datenbearbeitung einhergehen. Das ist nichts Neues. Schon heute müssen die Organe eine Risikoanalyse

vornehmen und Datenbearbeitungen, die mit besonderen Risiken für die Grundrechte der Betroffenen verbunden sind, der Datenschutzstelle zur Vorabkontrolle vorlegen (vgl. § 19a DSG; siehe dazu auch S. 5). Die Pflicht zur Vorabkontrolle bleibt bestehen (neu: Vorabkonsultation, was den beratenden Charakter besser zum Ausdruck bringt).
- Meldepflicht bei Datenschutzverletzungen: Neu sind die verantwortlichen Organe zu verpflichten, unbefugte Datenbearbeitungen oder Verluste von Personendaten unverzüglich ihren Datenschutzbeauftragten zu melden.
- Privacy by Design und Privacy by Default: Datenbearbeitungen sind so zu gestalten, dass die Prinzipien Privacy by Design (Datenschutz durch Technikgestaltung) und Privacy by Default (Datenschutz durch datenschutzfreundliche Voreinstellungen) eingehalten werden. Beide Prinzipien sind in die Datenschutzgesetze einzuführen.
- Erlass verbindlicher Anordnungen: Die europäischen Vorgaben verlangen, dass die Datenschutzbeauftragten bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen in Form einer Verfügung gegenüber den verantwortlichen Organen treffen können. Die Anordnungen sind anfechtbar.

Gemeinsam mit der federführenden Sicherheitsdirektion haben wir die Arbeiten zur Umsetzung der europäischen Vorgaben an die Hand genommen. An mehreren gemeinsamen Sitzungen haben wir mit der Sicherheitsdirektion den Revisionsbedarf definiert und erste Entwürfe verfasst. Die Revision bietet zudem die Gelegenheit, Datenschutzbestimmungen, die sich in der Praxis schlecht bewährt haben, neu zu gestalten.

Ausblick:
Die Schengen-Mitgliedsstaaten sind verpflichtet, ihre Gesetzgebung bis *1. August 2018* den neuen europäischen Vorgaben anzupassen. Diesen Zeitplan werden voraussichtlich nur wenige Kantone einhalten können. Wollen die Kantone nicht riskieren, den Zugriff auf die europäische Polizeidatenbank, das Schengener Informationssystem (SIS), zu verlieren, müssen sie die Datenschutzrevisionen gemäss den Schengen-Vorgaben voranzutreiben. Im Kanton Zug soll die Revision 2020 umgesetzt sein. Der Kanton Zug geht insofern mit gutem Beispiel voran, als mit Stichtag 1. August 2018 die Gesetzgebungsarbeiten zumindest auf Stufe Regierungsrat relativ weit fortgeschritten sein sollten. Wir werden weiterhin berichten.

Bundesvorlagen

Auf Bundesebene haben wir uns zu 8 Vorlagen (2016: 6) geäussert:

- Totalrevision des Datenschutzgesetzes – Übernahme der Richtlinie (EU) 2016/680 und des Änderungsprotokolls zur Europaratskonvention SEV 108
- Verordnung über den Nachrichtendienst und Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes
- Umsetzung des ersten Massnahmenpakets zur Energiestrategie 2050: Vernehmlassung zu Änderungen auf Verordnungsstufe (unter anderem Smart Meter)
- Revision des Bundesgesetzes über den allgemeinen Teil des Sozialversicherungsrechts (ATSG) – Missbrauchsbekämpfung, insbesondere Durchführung von Observationen
- Ausführungsrecht zum Krebsregistrierungsgesetz
- Vernehmlassung zur Änderung der Verordnung über die Krankenversicherung (KVV)
- Informationssicherheitsgesetz (ISG) – Grobeinschätzung des personellen und finanziellen Aufwands der Kantone zuhanden der Regierungskonferenz Militär, Zivilschutz und Feuerwehr
- Beurkundung des Personenstands und Grundbuch – Vernehmlassung der Rechtskommission des Nationalrats zur Verwendung eines sektoriellen Personenidentifikators oder der AHV-Versichertennummer im Grundbuch

Die datenschutzrechtlichen Hinweise der Datenschutzbeauftragten wurden weitestgehend in den Stellungnahmen des Kantons Zug zuhanden des Bundes berücksichtigt. Aus Ressourcengründen

verzichteten wir auf eine Stellungnahme zum Vorentwurf des Bundesgesetzes über die Bearbeitung von Personendaten im EDA, zur Revision der Verordnung des EDI über das elektronische Patientendossier, zur Totalrevision des Nationalstrassenabgabegesetzes (E-Vignette) sowie zur Verordnung über die Aufsicht über die nachrichtendienstlichen Tätigkeiten.

Übrigens
Die Datenschutzbeauftragte stellt auf ihrer Website ausgewählte Vernehmlassungsantworten oder Stellungnahmen zu kantonalen Vorlagen oder Bundesvorlagen der interessierten Öffentlichkeit zur Verfügung (www.datenschutz-zug.ch, Rubrik «Über uns»).

6. Zusammenarbeit mit anderen Datenschutzstellen

Privatim

Die Datenschutzbeauftragte des Kantons Zug ist Mitglied von «privatim», der Konferenz der schweizerischen Datenschutzbeauftragten (www.privatim.ch). Privatim gehören Datenschutzbehörden aus 23 Kantonen und 7 Städten sowie der Datenschutzbeauftragte des Fürstentums Liechtenstein an. Seit 2017 ist auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) wieder aktiv als assoziiertes Mitglied bei privatim dabei.

Seit Mai 2016 ist die Datenschutzbeauftragte gewähltes Mitglied im Vorstand von privatim und gehört dem vorberatenden Ausschuss des Vorstands an. In dieser Funktion durfte die Datenschutzbeauftragte im November 2017 auf Einladung der Staatspolitischen Kommission des Nationalrats gemeinsam mit dem Präsidenten von privatim eine Stellungnahme zum Revisionsentwurf des Datenschutzgesetzes des Bundes abgeben. Als Vorstandsmitglied leitet die Datenschutzbeauftragte auch die «Arbeitsgruppe Sicherheit», die sich mit kantonsübergreifenden (Sicherheits-)Themen im Polizei- und Migrationsbereich beschäftigt.

Dank dem Engagement bei privatim können kantonsübergreifende Datenschutzthemen koordiniert und mit Unterstützung anderer kantonaler Datenschutzbehörden und des EDÖB angegangen werden. So sind die Mitglieder von privatim an ihre Kantonsregierungen getreten und haben den *Verzicht auf die Verwendung der AHV-Versichertennummer als universellen Personenidentifikator gefordert*. Ein Gutachten der Eidgenössischen Technischen Hochschule (ETH) hatte vorgängig nach einer umfassenden Risikoanalyse die damit verbundenen Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger bestätigt.

An der zweitägigen Frühjahreskonferenz in Schaffhausen leitet die Datenschutzbeauftragte eine öffentliche Podiumsdiskussion zum Thema «Outsourcing und medizinisches Berufsgeheimnis». Immer öfter werden Kliniken, Krankenkassen und Arztpraxen Opfer von Cyberangriffen. Es stellte sich die Frage, ob die Auslagerung von Patientendaten in eine Cloud überhaupt mit dem Datenschutz vereinbar ist. Privatim setzt sich hier für eine pragmatische Lösung ein, die den Einsatz von Cloud-Lösungen unter Gewährleistung des Patientengeheimnisses ermöglicht. Das Herbstplenum fand in Altdorf statt. Es widmete sich den datenschutzrechtlichen Fragen rund um Cloud-Anwendungen in Schulen. Die diesbezüglichen Schlussfolgerungen wurden an einem anschliessenden Workshop besprochen. Ein weiterer Workshop fand auf Einladung des Vorstands zum Thema «Pflichtenheft und Ressourcen der Datenschutzbehörden» statt.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Die Zusammenarbeit des EDÖB (www.edoeb.admin.ch) mit den kantonalen Datenschutzbeauftragten ist aufgrund der Schengen-Assoziierungsabkommen gesetzlich vorgeschrieben. Der EDÖB und die kantonalen Datenschutzbehörden sind verpflichtet, bei der Beaufsichtigung der Datenbearbeitungen, die in Anwendung der Assoziierungsabkommen erfolgen, aktiv zusammenzuarbeiten. Die Zusammenarbeit erfolgt über die «Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Schengen-Assoziierungsabkommen», an deren Sitzungen auch die Datenschutzbeauftragte jeweils teilnimmt.

Die Koordinationsgruppe traf sich 2017 auf Einladung des EDÖB zu einer Sitzung in Bern: An dieser Sitzung konnte der Leitfaden für koordinierte Kontrollen des Schengener Informationssystems (SIS) verabschiedet werden. Die Datenschutzbeauftragte war Mitglied der Arbeitsgruppe, die den Leitfaden erarbeitet hatte. Mit dem Leitfaden steht den kantonalen Datenschutzbeauftragten und dem EDÖB nun ein praxistaugliches Instrument zur koordinierten Durchführung von Schengen-Kontrollen zur Verfügung.

7. Personal, Finanzen und Statistik

Die Datenschutzstelle verfügt über 160 Stellenprozente, verteilt auf die Datenschutzbeauftragte Dr. iur. Claudia Mund (80 %) und ihre Stellvertreterin, Fürsprecherin Christine Andres (80 %).

Während das Budget der Datenschutzstelle von 2015 bis 2017 empfindliche Kürzungen erfahren hatte (siehe Tätigkeitsbericht 2016, S. 15), wurden im Budget 2018 keine weiteren Kürzungen im Rahmen des Projektes «Finanzen 2019» eingestellt. Die Rechnung 2017 schloss gemäss Budgetvorgaben ab.

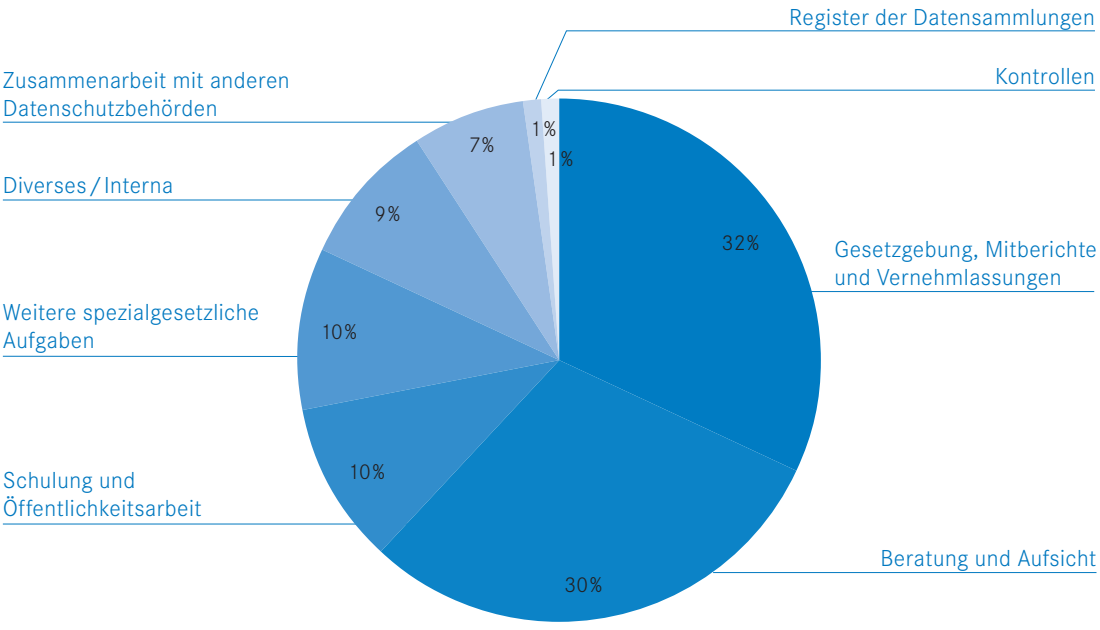
Die Datenschutzbeauftragte hofft, dass der Datenschutzstelle in Zukunft wieder deutlich mehr Ressourcen zugestanden werden, da die Digitalisierung einen wirksamen Datenschutz braucht, um die notwendige Beratung und Lenkung wahrnehmen zu können.

Statistik

Die folgende Aufstellung gibt einen Einblick in unsere Tätigkeiten und darüber, in welchem Umfang wir unsere gesetzlichen Aufgaben wahrnehmen beziehungsweise wahrnehmen können:

Im Berichtsjahr lag der Schwerpunkt unserer Arbeit neu in der Mitarbeit in der Gesetzgebung. Diese nahm im Vergleich zum Vorjahr um 22 % zu. Grund dafür war die zeitintensive Begleitung der Vorarbeiten zur Revision des Datenschutzgesetzes (vgl. ausführlicher S. 16 f) sowie zur Revision des Einführungsgesetzes zum Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister (siehe S. 15).

Eine weitere Verschiebung ist bei den spezialgesetzlichen Aufgaben zu verzeichnen. Diese haben um 7 % zugenommen. Hier fielen einerseits die Stellungnahmen der Datenschutzbeauftragten zu Videoüberwachungsgesuchen ins Gewicht, die gemäss der neuen Videoüberwachungsverordnung vorgängig bei der Datenschutzstelle einzuholen sind. Anderseits stieg auch die Anzahl der Gesuche für den elektronischen Zugriff auf Daten im Abrufverfahren zwischen Behörden, sogenannte Online-Gesuche, die der Datenschutzbeauftragten vorgängig zur Stellungnahme vorzulegen sind (zu diesen spezialgesetzlichen Aufgaben siehe S. 11 f).



Erstmals haben wir unsere Kontrolltätigkeit wahrnehmen können. Diese liegt bei 1 % und fällt auf den ersten Blick kaum ins Gewicht. Diese Interpretation wäre aber falsch. Die Datenschutzbeauftragte liess sich mangels internem Know-how bei der Kontrolle der Zugriffe auf das Schengener Informationssystem (SIS) von einem externen Unternehmen unterstützen.

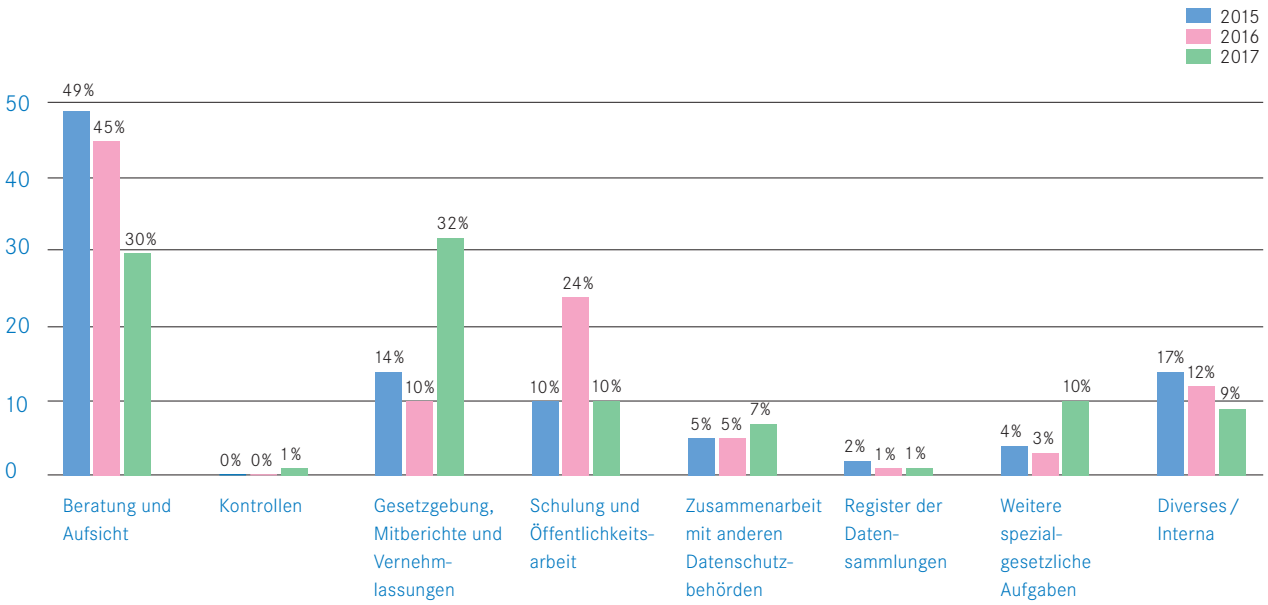
Nach wie vor viel Zeit investieren wir in die Beratung und Aufsicht. Im Berichtsjahr mussten wir unsere Beratungs- und Aufsichtstätigkeit zugunsten anderer gesetzlicher Aufgaben um 15 % reduzieren. Sie setzt sich neu wie folgt zusammen: Beratung und Aufsicht der kantonalen Verwaltung (21 %) und der Gemeinden (6 %) sowie Beratung von Privaten (3 %).

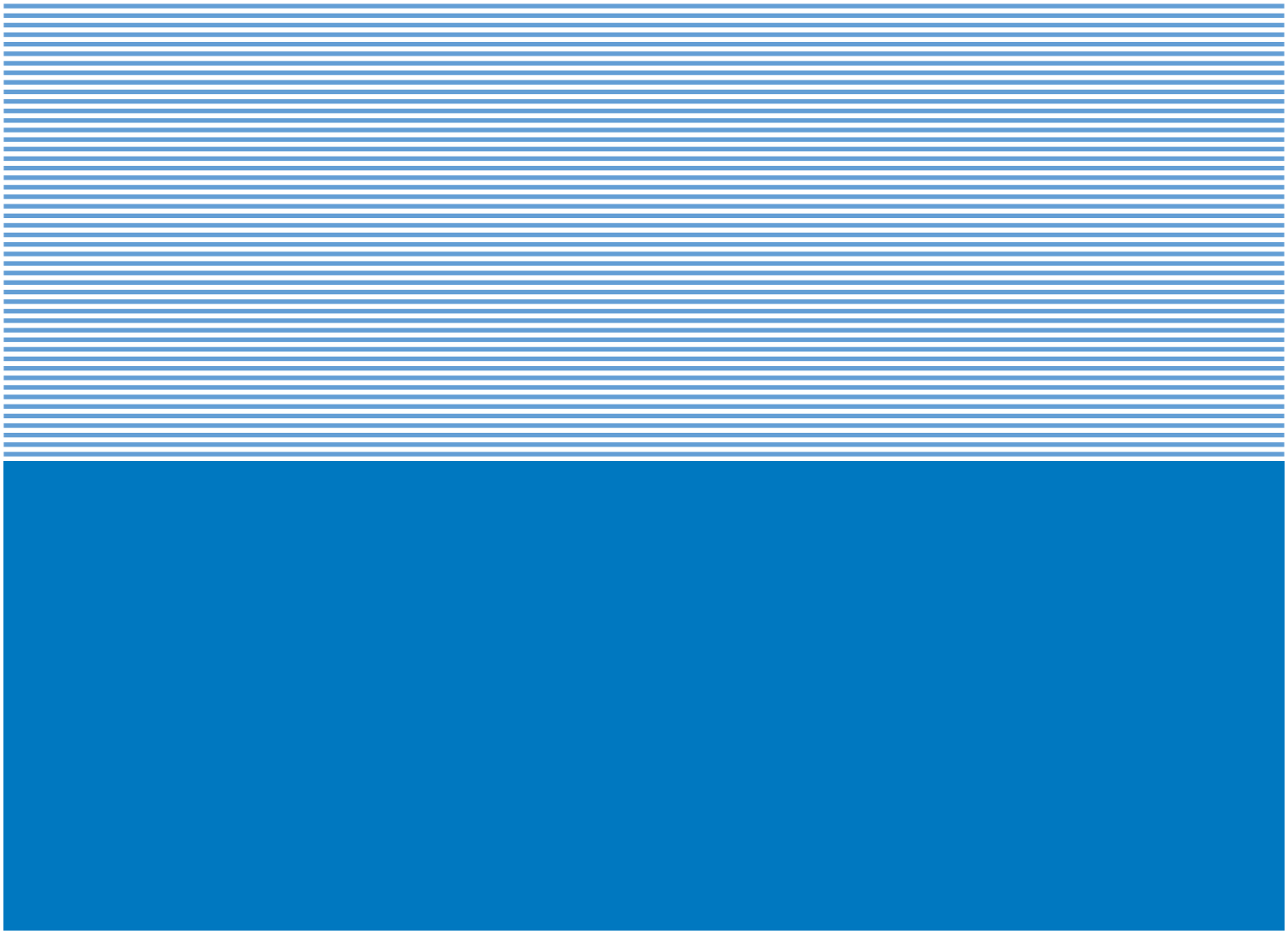
Unsere Aktivitäten im Bereich Schulung und Öffentlichkeitsarbeit mussten wir ebenfalls zugunsten anderer gesetzlicher Aufgaben stark reduzieren (um 14 %).

Ein Rückgang ist auch bei Diverses/Interna zu verzeichnen. Hier verbuchen wir alles, was interne Arbeiten anbelangt und nicht den anderen Aufgaben zugeordnet werden kann (Personalangelegenheiten, eigene Weiterbildung, Rechnungswesen/Budget, Administration, Archivierung usw.). Dank Umstellung auf ein neues Dokumentverwaltungssystem konnten wir unseren administrativen Aufwand um gute 3 % senken.

Ein Rückblick über die vergangenen drei Jahre kann der untenstehenden Grafik entnommen werden.

Die Auflistung zeigt, dass die gesetzliche Aufgabenerfüllung der Datenschutzstelle starken Schwankungen unterliegt. Dies ist nicht zuletzt ein Ausdruck davon, dass wir insbesondere in diesem Jahr mit den uns zur Verfügung stehenden Mitteln nicht allen Bedürfnissen, die aus der fortschreitenden Digitalisierung erwachsen, im verlangten Ausmass nachkommen konnten.





Herausgeberin
Datenschutzbeauftragte des Kantons Zug
Regierungsgebäude am Postplatz
Postfach
6301 Zug
T 041 728 31 87

Gestaltung
Christen Visuelle Gestaltung, Zug

Bezug
Der Tätigkeitsbericht 2017 ist online unter
www.datenschutz-zug.ch abrufbar.