

Tätigkeitsbericht 2021

Datenschutzbeauftragte des Kantons 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 vorliegende Bericht bezieht sich auf den Zeitraum vom 1. Januar bis 31. Dezember 2021. Sofern relevant werden bis zur Drucklegung eingetretene Sachverhalte zu erwähnten Themen ebenfalls noch berücksichtigt.

Der Bericht wird auf der Website der Datenschutzstelle (www.datenschutz-zug.ch) veröffentlicht.

Zug, im März 2022

Inhaltsverzeichnis

2021 – Digitale Verwaltung: Rechtsgrundlagen, Vertrauen und Kulturwandel	4
1. Beratungs- und Aufsichtstätigkeiten	5
1.1 Erfahrungen mit der Datenschutz-Folgenabschätzung	
1.2 Projekt Unified Communication und Collaboration (UCC)	
1.3 Weitere IT- und Digitalisierungsprojekte	
1.4 Beratung von Privaten	
2. Gesetzgebung und Vernehmlassungen	9
2.1 Kantonale Vorlagen	
2.2 Kantonsrätliche Vorstösse	
2.3 Bundesvorlagen	
3. Spezialgesetzliche Aufgaben	11
3.1 Verordnung über das Bewilligungsverfahren für den elektronischen Datenaustausch (Online-Verordnung)	
3.2 Videoüberwachungen	
4. Kontrollen	14
5. Schulung und Öffentlichkeitsarbeit	15
6. Zusammenarbeit mit anderen Datenschutzstellen	16
7. Personal und Statistik	18

2021 – Digitale Verwaltung: Rechtsgrundlagen, Vertrauen und Kulturwandel

E-Government und Digitalisierung werden beschleunigt vorangetrieben. Das haben Bund und Kantonsregierungen beschlossen und die Kräfte in einer neuen gemeinsamen Organisation «Digitale Verwaltung Schweiz» gebündelt. Zu den erforderlichen Rahmenbedingungen der digitalen Transformation werden die Rechtsgrundlagen, das Vertrauen der Bevölkerung, der Wirtschaft und der Mitarbeitenden in die digitale Verwaltung sowie ein entsprechender Kulturwandel gezählt.

Auch im Kanton Zug gibt es inzwischen kaum mehr einen Bereich, in dem nicht ein E-Government- oder Digitalisierungsprojekt ansteht. Im Gegensatz zur Privatwirtschaft sind der Verwaltung Schranken gesetzt – nicht nur durch den Datenschutz oder die Datenschutzbehörde(n), sondern insbesondere auch durch Föderalismus, Gesetzmässigkeitsprinzip, Amtsgeheimnis und weitere Geheimhaltungspflichten.

Von entscheidender Bedeutung sind die Rechtsgrundlagen, die dazu beitragen, Rechtssicherheit und Transparenz bei Bürgerinnen, Bürgern sowie Mitarbeitenden der Verwaltung zu schaffen und damit auch Vertrauen in die digitale Verwaltung. Auch die gesetzliche Verpflichtung der verantwortlichen Organe zur Datenschutz-Folgenabschätzung und Vorabkonsultation der unabhängigen Datenschutzstelle dienen letztlich dazu, Vertrauen zu schaffen.

Feststellbar ist, dass in E-Government- und Digitalisierungsprojekten der Verwaltung die Bedürfnisse der Bevölkerung oft (noch) eine untergeordnete Rolle spielen. Dies belegen nicht nur Beispiele aus dem vorliegenden Tätigkeitsbericht, sondern auch eine aktuelle Studie (*Digitaler Staat in der Schweiz*). Für die Bevölkerung stehen danach nicht Dienstleistungen wie Online-Schalter oder E-Voting im Vordergrund, sondern Grund- und Schutzbedürfnisse gegenüber dem Staat (Cybersicherheit und digitale Gewalt) – und damit auch der Schutz ihrer Grund- und Persönlichkeitsrechte.

Das Interesse der Bevölkerung liegt primär in einer rechts- und datenschutzkonformen Datenbearbeitung durch die Verwaltung. Eine konsequente(re) Fokussierung auf die Bedürfnisse der Bevölkerung dürfte auch zum angestrebten Kulturwandel beitragen. Dieser muss sich zudem ebenfalls im Rahmen der eingangs erwähnten Schranken bewegen und/oder sich auch in den Rechtsgrundlagen niederschlagen.

E-Government- und Digitalisierungsprojekte sind anspruchsvoll, die anstehenden Herausforderungen erfordern Koordination und Zusammenwirken, nicht nur kantonsübergreifend, sondern primär kantons- und verwaltungsintern. Die Datenschutzstelle legt als unabhängige Stelle, die in einem interdisziplinären Umfeld zu Hause ist, den Fokus auf die Grund- und Persönlichkeitsrechte der Bürgerinnen und Bürger – und kann damit einen wesentlichen Beitrag zu Rechtsetzung, Vertrauen und Kulturwandel, d.h. zu den Rahmenbedingungen der digitalen Transformation in der Verwaltung leisten.

Dr. iur. Yvonne Jöhri
Datenschutzbeauftragte des Kantons Zug

1. Beratungs- und Aufsichtstätigkeiten

Ein Schwerpunkt der Tätigkeit der Datenschutzstelle liegt in der Beratung von kantonalen und kommunalen Behörden und Dienststellen sowie von natürlichen und juristischen Personen, soweit ihnen öffentliche Aufgaben übertragen sind. Beratung lässt sich auch als eine Form der präventiven Aufsicht verstehen und entsprechend hoch ist ihr Stellenwert.

Im Berichtsjahr lag der Schwerpunkt der Beratungs- und Aufsichtstätigkeit erneut auf IT- und Digitalisierungsprojekten. Zentrales Thema waren weiterhin Fragestellungen rund um den Einsatz von Cloud-Lösungen; der Trend geht unaufhaltsam in diese Richtung. Gleichzeitig bestehen für Verwaltungen, insbesondere was Cloud-Lösungen der US-Anbieter betrifft, grosse, komplexe Herausforderungen und teilweise (noch nicht) hinreichende Lösungsansätze.

Zudem konnten im Berichtsjahr sowohl die Datenschutzstelle als auch die verantwortlichen Organe erste Erfahrungen mit der Umsetzung des am 1. September 2020 in Kraft getretenen revidierten Datenschutzgesetzes machen.

1.1 Erfahrungen mit der Datenschutz-Folgenabschätzung

Mit dem Inkrafttreten des revidierten Datenschutzgesetzes wurde die bisherige Regelung der Vorabkontrolle durch Bestimmungen zur Datenschutz-Folgenabschätzung (DSFA) und zur Vorabkonsultation konkretisiert.

Das revidierte Datenschutzgesetz verpflichtet die verantwortlichen Organe ausdrücklich, den mit der Digitalisierung einhergehenden erhöhten Risiken für die Grundrechte der betroffenen Personen im Vorfeld einer Datenbearbeitung Rechnung zu tragen. Die Datenschutzstelle hat zur Unterstützung der Organe deshalb Informationen, Vorlagen und Checklisten für die Datenschutz-Folgenabschätzung – sowie für ein allenfalls erforderliches Datenschutz- und Informationssicherheitskonzept (ISDS-Konzept) und eine Vorabkonsultation – erarbeitet und zur Verfügung gestellt.

Diese Hilfsmittel sollen den verantwortlichen Organen ermöglichen, eigenständig eine Datenschutz-Folgenabschätzung durchzuführen. Diese umfasst neben der erforderlichen Rechtsgrundlagenanalyse eine Risikoanalyse und -bewertung, d.h. die Risiken einer (geplanten oder wesentlich geänderten) Datenbearbeitung für die Grundrechte der betroffenen Personen sind zu identifizieren, zu bewerten und mit geeigneten Massnahmen zu eliminieren oder mindestens auf ein tragbares Mass zu minimieren. Je nach Einschätzung der Risiken sind auch ein ISDS-Konzept und eine Vorabkonsultation der Datenschutzstelle erforderlich.

Im Berichtsjahr wurden die zur Verfügung gestellten Hilfsmittel rege genutzt, und die Datenschutzstelle wurde – auch wenn sie nur im Fall einer Vorabkonsultation zwingend zu involvieren ist – aufgrund der mit dem revidierten Datenschutzgesetz einhergehenden verschiedenen Neuerungen vermehrt kontaktiert.

Eine erste Zwischenbilanz zeigt, dass dort, wo man mit den aus der Projektmanagement-Methode HERMES bekannten Vorgaben einer Rechtsgrundlagenanalyse sowie Risikoanalyse und -beurteilung bereits vertraut ist, die Vorgaben der Datenschutz-Folgenabschätzung weniger Mühe bereiten. Eines der Ziele der Datenschutzstelle war es denn auch, die Datenschutz-Folgenabschätzung in bereits bestehende Abläufe einzubetten (siehe Tätigkeitsbericht 2020, S. 7). Im Sinne einer Zwischenbilanz lassen sich folgende Feststellungen zusammenfassen:

- Rechtsgrundlagenanalyse: Personendaten dürfen nur bearbeitet werden, wenn dafür eine genügende gesetzliche Grundlage vorliegt (Legalitäts-/Gesetzmassigkeitsprinzip). Mangels klarer (unmittelbarer) gesetzlicher Grundlagen ist oftmals bereits die Rechtsgrundlagenanalyse aufwendig. Für die Rechtsgrundlagenanalyse ist daher grundsätzlich auch der zuständige Rechtsdienst des Fach-/Sachbereichs beizuziehen. Ziel der Datenschutzstelle ist es, auch die Bewilligungsverfahren im Bereich Videoüberwachung und Online-Zugriffe mit dem

DSFA-Prozess zu koordinieren. Dies erweist sich allerdings insbesondere beim Online-Bewilligungsverfahren nicht immer als einfach.

- Der Fokus bei der datenschutzrechtlichen Risikoanalyse und -beurteilung, die im Rahmen der Datenschutz-Folgenabschätzung vorzunehmen ist, liegt auf den Grund- und Persönlichkeitsrechten der von einer Datenbearbeitung betroffenen Personen und nicht auf den Risiken für die öffentliche Verwaltung. Bei den von behördlichen Datenbearbeitungen betroffenen Personen handelt es sich primär um Bürgerinnen und Bürger, aber auch um Mitarbeitende. Die Datenschutz-Folgenabschätzung trägt damit einem bzw. dem zentralen Anliegen jeder Digitalisierungsstrategie Rechnung: Sie orientiert sich am Kundenbedürfnis, d.h. den Interessen der Bürgerinnen und Bürger, der Nutzerinnen und Nutzer, der (End-)Kundinnen und -Kunden. Deren Interesse gegenüber der Verwaltung ist eine rechts- und datenschutzkonforme Datenbearbeitung, die ihren Grund- und Persönlichkeitsrechten Rechnung trägt.
- Die Datenschutzstelle stellt oftmals fest, dass im Rahmen der datenschutzrechtlichen Risikoanalyse und -beurteilung mögliche Massnahmen zwar aufgezählt werden, ohne dass damit aber gemeint ist, dass diese auch zur Risikominimierung umgesetzt werden. Dabei ist im Rahmen einer Datenschutz-Folgenabschätzung selbstverständlich darzulegen, welche Massnahmen konkret getroffen und umgesetzt werden, um bestehende Risiken für die betroffenen Personen effektiv zu eliminieren – oder mindestens zu minimieren –, und es sind nicht nur mögliche Massnahmen aufzuzählen. Nur so ist letztlich eine Aussage über die Restrisiken möglich.
- Verbesserungspotenzial besteht betreffend die systematische, konsequente Einbindung und Integration von Datenschutz und Informationssicherheit in die organisatorischen Prozessabläufe der Verwaltungseinheiten (Direktionen/Ämter). Die Datenschutzstelle hatte auf diese Massnahme im Rahmen ihres Mitberichts zur Interpellation betreffend Datensicherheit und

Datenschutz beim Zuger Impfzentrum hingewiesen (siehe S. 9, 2.2 Kantonsrätliche Vorstösse), gleichzeitig aber auch festgehalten, dass die (bestehenden) gesetzlichen Vorgaben und Prozesse nicht nur in die Prozessabläufe der Direktionen und Verwaltungseinheiten einzubinden sind, sondern die Einhaltung (durch Kontrollen/Audits) auch überprüft und durchgesetzt werden müssen. In der Praxis zeigt sich, dass Datenschutz und Informationssicherheit (noch) nicht systematisch und konsequent in die organisatorischen Prozessabläufe der kantonalen Direktionen und Ämter eingebunden und integriert sind und u.a. auch bei grossen Digitalisierungsvorhaben nicht immer die erforderliche Datenschutz-Folgenabschätzung durchgeführt wird (inkl. allfälliger Erstellung eines ISDS-Konzepts und Vorabkonsultation der Datenschutzstelle). Noch wenig(er) thematisiert ist der Stand betreffend die Integration von Datenschutz und Informationssicherheit in die Prozessabläufe bei den Gemeinden.

Die Datenschutzstelle hat im Berichtsjahr bereits Informationsanlässe geplant, um sich verwaltungsintern mit verantwortlichen Organen über die Erfahrungen auszutauschen und um Anpassungen und Verbesserungspotenzial beim Datenschutz-Folgenabschätzung-Prozess und bei den von der Datenschutzstelle bereitgestellten Hilfsmitteln/Vorlagen gemeinsam zu diskutieren.

1.2 Projekt Unified Communication und Collaboration (UCC)

Im Berichtsjahr wurde die Datenschutzstelle eingeladen, das Projekt Unified Communication and Collaboration (UCC) zu begleiten. Bei dem Projekt geht es letztlich um die verwaltungsweite Einführung sämtlicher Funktionalitäten von Microsoft Teams und Office 365 (Telefonie, Videokonferenzen, E-Mail, Kalender, Instant Messaging, Office-Programme, Dokumentenablage etc.).

Die Datenschutzstelle konnte im Rahmen der Arbeitsgruppe frühzeitig die datenschutzrechtlichen Risiken in die Diskussion einbringen, die

mit einem verwaltungsweiten Einsatz von Microsoft Teams und der Cloud-Lösung eines US-Anbieters verbunden sind und auf zu treffende Massnahmen (Datenklassifizierung, effektive Verschlüsselung, weitere technische Lösungen etc.) hinweisen. Die Risiken lassen sich wie folgt umschreiben: zu späte Erkennung der konkreten Anforderungen an die Informationssicherheit; Rechtsrisiken, da ein verlässliches Vertragsverhältnis fehlt; Ausland-Datenbearbeitung und US-Zugriffsmöglichkeiten; Zweckentfremdung der Daten durch Microsoft; Verlust von Transparenz und Kontrollmöglichkeiten über Daten und Applikationen; Komplexität überfordert Mitarbeitende und gefährdet damit die Informationssicherheit. Sie entsprechen inhaltlich jenen gemäss [«Merkblatt Cloud-spezifische Risiken und Massnahmen»](#) von privativim. Neben den Risiken aus datenschutzrechtlicher Sicht gibt es weitere Risiken, die ebenfalls in eine Risikoanalyse und -beurteilung einfließen sollten (bspw. digitale Souveränität).

1.3 Weitere IT- und Digitalisierungsprojekte

Nachfolgend eine nicht abschliessende Auflistung von weiteren IT-Projekten, bei denen die Datenschutzstelle beratend mitwirkte oder eine Stellungnahme verfasste:

- Ausschreibung neue IT-Service-Management-Lösung beneFIT
- Cloud-Projekt Identity Management beim AIO (Azure Active Directory)
- Neuer Internetauftritt der kantonalen Verwaltung (Projekt NIA)
- Neue Fachanwendung Fondsverwaltung (Beantragungs- und Entscheidungsprozesse für Beiträge aus dem Lotteriefonds)
- Digitale Dossierführung im Amt für Migration
- Strategie und Machbarkeitsstudie bezüglich des neu geplanten Security Operations Center (SOC)
- Web-Gesundheitskampagne Hey-Zug.ch
- Corona-Reihentests an Schulen mit Easytesting
- Bussen mit QR-Code

Aufgrund der andauernden Corona-Pandemie war die Datenschutzstelle im letzten Jahr auch

regelmässig involviert, wenn es um Plattformen für digitale Zusammenarbeit ging, und bot verschiedenen Stellen Unterstützung im Bereich Videokonferenz-Tools.

1.4 Beratung von Privaten

Im Berichtsjahr sind rund 60 Privatpersonen mit Anfragen an die Datenschutzstelle gelangt. Darunter fallen sowohl einfache Anfragen, die bereits im Rahmen eines Telefongesprächs oder mit einer kurzen E-Mail geklärt werden konnten, als auch Anfragen, die mit grösserem Aufwand verbunden waren. Unter Letztere fallen u.a. Sachverhalte, für deren materielle Beurteilung vertiefte Abklärungen erforderlich sind, oder aber auch Fälle, die für die Datenschutzstelle mit einigen Mühen verbunden sind, um die gewünschten Informationen für eine Beurteilung zu erhalten.

Parkuhren mit Kontrollschildeingabe

Die Datenschutzstelle war von der Stadt Zug im Zusammenhang mit der Einführung von Park-Apps involviert worden, nicht aber bei der anschliessenden Umrüstung der Parkuhren, welche die Eingabe des Fahrzeugkennzeichens anstelle der Parkplatz-Nummer erfordern. Nachdem nach der Umrüstung regelmässig Beschwerden eingingen, sah sich die Datenschutzstelle veranlasst, tätig zu werden, und bat nachträglich um die erforderlichen Informationen für eine Beurteilung. Dabei ging es um Informationen zur Rechtsgrundlage und zu den konkreten Umsetzungsmassnahmen (welche Daten erhoben und wo und wie lange diese Daten gespeichert werden, wer welche Zugriffs- und Bearbeitungsrechte hat, ob Zugriffe protokolliert werden). Zudem wurde die Frage nach der Rechtslage gestellt für den Fall, dass sich ein/e Automobilist/in vertippt. Letzteres dürfte u.a. aufgrund der viel längeren Zahlenreihe nicht nur öfters (unbeabsichtigt) der Fall sein, sondern auch, weil sich der eine oder andere – bewusst – (geringfügig) vertippt, um gegen das zwingend erforderliche aktive Eintippen des Fahrzeugkennzeichens (und damit die Bekanntgabe von Personendaten) zu «demonstrieren».

Betreffend Rechtsgrundlage wurde allgemein auf die Strassenverkehrsgesetzgebung des Bundes verwiesen und der Datenschutzstelle mitgeteilt, dass auf den 1. Januar 2022 eine neue Verordnung für die Parkraumbewirtschaftung in der Stadt Zug in Kraft treten soll (was inzwischen erfolgt ist). Was die vorgängige Klärung der Rechtslage bei Vertippen betrifft, wurde orientiert, dass es im Ermessen der Polizei bzw. des Staatsanwalts liege, zu entscheiden, ob die Parkbusse zurückgenommen werde.

Die für die Klärung der Verhältnismässigkeit relevanten Informationen (erhobene Daten, u.a. Handy-Nr. für ein digitales Parkticket, falls gewünscht/erforderlich; Dauer der Speicherung bei der Auftragnehmerin bzw. des Zugriffs von Stadt Zug und Zuger Polizei) sowie die Einhaltung der Anforderungen an eine Auftragsdatenbearbeitung erforderten im Übrigen einen nicht sachgerechten Aufwand der Datenschutzstelle.

Festzuhalten ist: Da die Datenbearbeitung an einen privaten Dritten ausgelagert worden ist, wäre die Stadt Zug gesetzlich verpflichtet, sicherzustellen, dass die erhobenen und gespeicherten Daten durch den Auftragsdatenbearbeiter nicht auch zu eigenen Zwecken, sondern nur so, wie sie die Stadt selbst nutzen dürfte, genutzt werden und die erhobenen Daten bei rechtskonformem Verhalten (Bezahlen der Gebühren) unmittelbar nach Ablauf der Parkzeit gelöscht werden. Die Datenschutzstelle hat die Stadt Zug im Übrigen darauf hingewiesen, dass diese Einschätzung auch jener des Datenschutzbeauftragten des Kantons Graubünden entspricht (siehe [Tätigkeitsbericht 2020](#)).

Bei der von der Stadt Zug an einen privaten Dritten ausgelagerten Datenbearbeitung werden die an der Parkuhr eingegebenen Daten (Kontrollschild und evtl. Handy-Nr., zusammen mit Parkuhr-ID, Datum, Zeit, Betrag) zwei Jahre gespeichert und sind während dieser Zeit auch für die Stadt Zug abrufbar. Das Kontrollorgan hat bis 72 Std. nach Beendigung des Parkvorgangs Zugriff auf die Daten.

Für die Datenschutzstelle sind die zweijährige

Aufbewahrungsdauer von Kontrollschild und Handy-Nr. und eine 72-stündige Verfügbarkeit nach Beendigung des Parktickets auf den Kontrollinstrumenten weder nachvollziehbar noch verhältnismässig.

Die Stadt Zug sieht sich als verantwortliches Organ weder in der Pflicht, die Anforderungen einer Auftragsdatenbearbeitung umzusetzen noch eine verhältnismässige Datenbearbeitung durch den beigezogenen Dritten sicherzustellen.

Weitere Anfragen

Weitere Anfragen von Privatpersonen betrafen im Berichtsjahr u.a.:

- Datensperren und deren Durchbrechung
- Erhebung von nicht erforderlichen Personendaten durch eine Einwohnerkontrolle
- Löschung der im Rahmen einer Sammelauskunft erhaltenen Personendaten
- E-Mail-Versand von Impfnachweisen
- Umgang mit Datensammlungen in einem Konkursverfahren
- Bekanntgaben von Informationen aus dem Patientendossier einer Klinik an die Kindes- und Erwachsenenschutzbehörde (KESB)
- Datenbekanntgabe einer Schule über den Schulwechsel eines Kindes an alle Eltern
- Bekanntgabe einer bei der Einwohnerkontrolle gesperrten Adresse durch ein anderes Organ im Rahmen einer Korrespondenz
- Auskunftsgesuche aufgrund von Generalvollmachten
- Bekanntgabe der vorherigen Besitzer bei einem Fahrzeugverkauf

2. Gesetzgebung und Vernehmlassungen

Die Datenschutzstelle nimmt aufgrund ihres gesetzlichen Auftrags aus datenschutzrechtlicher Sicht Stellung zu rechtsetzenden Erlassen des Kantons, der Gemeinden und des Bundes.

Den gesetzlichen Grundlagen kommt aus Sicht des Grundrechts- und Persönlichkeitsschutzes grosse Bedeutung zu. Dies einerseits aufgrund des Legalitäts-/Gesetzmassigkeitsprinzips, wonach sich staatliches Handeln auf eine normstufengerechte und hinreichend bestimmte gesetzliche Grundlage stützen können muss; andererseits aus Gründen der Rechtssicherheit sowie der Transparenz und Information gegenüber den von staatlichen Datenbearbeitungen betroffenen Personen. Betroffene Personen sind dabei nicht nur Bürgerinnen und Bürger, sondern auch die Mitarbeitenden der Verwaltung selbst. Für Letztere haben klare Rechtsgrundlagen gleichzeitig auch insofern Bedeutung, als sie ihr Handeln im Rahmen ihrer Tätigkeit legitimieren.

Offen und unklar gehaltene gesetzliche Grundlagen führen dazu, dass der klare Wille des Gesetzgebers nicht aus dem Gesetz hervorgeht, die gesetzlichen Grundlagen auslegungsbedürftig bleiben und sie deshalb verwaltungsintern immer wieder Anlass zu Diskussionen geben. Insbesondere im Umfeld der Digitalisierung sind gesetzliche Defizite – aufgrund des Legalitätsprinzips – ein Hindernis und führen zu Verzögerungen.

2.1 Kantonale Vorgaben

Die Datenschutzstelle wird oft frühzeitig über anstehende kantonale Gesetzgebungsarbeiten mit Datenschutzbezug informiert. So berät und unterstützt sie die entsprechenden Stellen bei Vorhaben mit hoher Datenschutzrelevanz häufig schon vor dem internen Mitberichtsverfahren. Im Berichtsjahr war dies bei den beiden folgenden Gesetzgebungsvorhaben der Fall:

- Totalrevision des Gesetzes über soziale Einrichtungen (SEG): Neues Gesetz über Leistungen für Menschen mit Behinderung und Betreuungsbedarf (LBBG)
- Sozialhilfegesetz

Weitere Vorlagen, zu denen sich die Datenschutzstelle im Berichtsjahr geäussert hat oder in die sie involviert war, sind etwa Änderungen bzw. Revisionen folgender Rechtsgrundlagen:

- Teilrevision des Gesetzes betreffend die Einführung des Schweizerischen Zivilgesetzbuches für den Kanton Zug vom 17. August 1911
- Projekt Anstellungsbedingungen; Änderungen auf Gesetzes- und Verordnungsstufen
- Verordnung zum Einführungsgesetz zum Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister
- Verordnung über das Amtsblatt des Kantons Zug
- Änderungen der Verordnung zum Schulgesetz vom 7. Juli 1992 (BGS 412.111) betreffend Schularzt und Schulzahnarzt-Dienst

2.2 Kantonsrätliche Vorstösse

Nachdem die Datenschutzstelle 2020 zu keinem und 2019 zu einem einzigen kantonsrätlichen Vorstoss um Stellungnahme gebeten wurde, gingen im Berichtsjahr drei Interpellationen ein, zu denen die Datenschutzstelle teilweise ausführlich Stellung genommen hat:

- Interpellation von Luzian Franzini, Tabea Zimmermann Gibson und Rita Hofer betreffend Datensicherheit und Datenschutz beim Zuger Impfzentrum und allgemein beim Kanton Zug (Vorlage Nr. 3221.1 – 16563): Mitbericht zuhanden der Gesundheitsdirektion.
- Interpellation von Daniel Stadlin betreffend Austausch personenbezogener Daten innerhalb der kantonalen Verwaltung und zwischen Kantons- und Gemeindebehörden (Vorlage Nr. 3293 – 16700): Mitbericht zuhanden der Finanzdirektion.
- Interpellation von Daniel Stadlin betreffend Cybersicherheit – ist die kantonale Verwaltung genügend geschützt? (Vorlage Nr. 3308 – 16735): Mitbericht zu Frage 8b zuhanden der Finanzdirektion, wobei sich die Datenschutzstelle auf einen Verweis auf die bereits zur Interpellation Vorlage Nr. 3221.1 – 16563 gemachten Ausführungen beschränken konnte.

2.3 Bundesvorlagen

Die Datenschutzstelle wurde zu zahlreichen Bundesvorlagen zum Mitbericht eingeladen. Sie äussert sich aus Ressourcengründen nur vereinzelt zu Vorlagen des Bundes, im Berichtsjahr etwa zu folgenden:

- Verordnung über Zertifikate zum Nachweis einer Covid-19-Impfung, einer Covid-19-Genesung oder eines Covid-19-Testergebnisses
- Revision der Krebsregistrierungsverordnung
- Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBaG)

Dort, wo eine datenschutzrechtliche Stellungnahme von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, oder einer anderen Datenschutzstelle erarbeitet und zur Verfügung gestellt wird, beschränkt sich die Datenschutzstelle i.d.R. darauf, diese der zuständigen Direktion weiterzuleiten.

3. Spezialgesetzliche Aufgaben

Die Aufgaben und Kompetenzen der Datenschutzstelle ergeben sich grundsätzlich aus dem Datenschutzgesetz. Darüber hinaus kommen der Datenschutzstelle aufgrund der beiden folgenden kantonalen Erlasse weitere Aufgaben im Rahmen der Bewilligungsverfahren für den elektronischen Datenaustausch und für Videoüberwachungen im öffentlichen und im öffentlich zugänglichen Raum zu.

3.1 Verordnung über das Bewilligungsverfahren für den elektronischen Datenaustausch (Online-Verordnung)

Die Verordnung über das Bewilligungsverfahren für den elektronischen Datenaustausch (Online-Verordnung; BGS 157.22) regelt «den elektronischen Zugriff auf Personendaten im Abrufverfahren (Online-Zugriff)». Sie wurde gestützt auf § 7 Abs. 2 DSG erlassen und ist am 28. Juni 2008 in Kraft getreten.

Übergangslösung

Die mit dem Bewilligungsverfahren einhergehenden Einzelfallbeurteilungen im Rahmen von Online-Zugriffen sind im Zeitalter der Digitalisierung überholt. Die im Rahmen der DSG-Revision diskutierte Aufhebung der Online-Verordnung wurde letztlich als Übergangslösung – bis zur Schaffung gesetzlicher Grundlagen für Online-Zugriffe – beibehalten (siehe Protokoll des Kantonsrats vom 30. April 2020, Ziff. 394). Die Datenschutzstelle hatte im letztjährigen Tätigkeitsbericht über ihre Bemühungen – und die Hintergründe –, entsprechende Gesetzgebungsprozesse in Gang zu setzen, berichtet. Dazu hatte sie u.a. eine Bedarfsanalyse bei den kantonalen und gemeindlichen Organen angeregt, die die Direktion des Innern bei den Gemeinden mit Blick auf das Gemeindegesetz durchgeführt hat (siehe Tätigkeitsbericht 2020, S. 11).

Mit Blick auf die angestrebte Ablösung der Online-Verordnung bedarf es allerdings primär Bestimmungen in den entsprechenden Fach-/

Sach-/Spezialgesetzen. Aus dem Berichtsjahr gibt es Beispiele solcher spezialgesetzlichen Bestimmungen, die elektronische Zugriffe regeln, und zwar die im Rahmen der laufenden Revisionen vorgesehenen entsprechenden Bestimmungen im Gesetz über Leistungen für Menschen mit Behinderung und Betreuungsbedarf (LBBG) und im Sozialhilfegesetz.

Es entbehrt allerdings nicht einer gewissen Ironie, dass die Datenschutzstelle im Berichtsjahr gleichzeitig um Stellungnahme zu einem Entwurf eines Regierungsratsbeschlusses zur «Anpassung Gesuchformular für den elektronischen Zugriff auf Daten im Abrufverfahren» eingeladen wurde. Auch die – abzulösende – Online-Verordnung wird weiter gepflegt und das überholte Bewilligungsverfahren «digitalisiert», indem es in einen elektronischen Workflow überführt werden soll.

Ein neu als elektronischer Workflow daherkommendes Bewilligungsverfahren ändert am verursachten Verwaltungsaufwand ebenso wenig wie an den bekannten gesetzgeberischen Defiziten (Digitalisierung auf dem Weg der Einzelfallbeurteilung/-bewilligung, fehlende Rechtssicherheit und Transparenz für Bürgerinnen und Bürgern sowie Mitarbeitende).

Die geplante Publikation der auf das kantonale Personenregister erteilten Zugriffsberechtigungen auf der Website des Kantons vermag allenfalls Transparenz betreffend die mittels Online-Bewilligungen erteilten Online-Zugriffe auf dieses eine kantonale Register zu schaffen. Die Frage, ob, wie und wo über all die anderen bewilligten (und künftig bewilligten) Online-Zugriffe Transparenz geschaffen werden soll, bleibt offen.

Es ist zu befürchten, dass der neue elektronische Workflow zusammen mit den wachsenden Begehrlichkeiten aufgrund der technologischen Möglichkeiten zu einer Vielzahl neuer Gesuche bei der Datenschutzstelle führt, obwohl sich die Einzelfallbeurteilungen durch die Datenschutzstelle schon längst nicht mehr zeitnah bewältigen lassen.

Online-Bewilligungen für identische Aufgaben

Die Datenschutzstelle hat bereits darauf hingewiesen, dass eine Ablösung des Bewilligungsverfahrens für Online-Zugriffe vor allem auch dort angezeigt ist, wo gemeindliche Verwaltungsstellen (wie bspw. Notariate, Betreibungsämter, Sozialdienste) oder Kirch- und Bürgergemeinden identische oder gleich gelagerte Aufgaben wahrnehmen (siehe Tätigkeitsbericht 2020, S. 11). Spätestens im Zeitalter der Digitalisierung macht hier nur eine standardisierte, einheitliche und transparente, gesetzlich geregelte Umsetzung Sinn. Im vergangenen Jahr sind bei der Datenschutzstelle wiederum solche Anfragen zu Online-Zugriffen eingegangen.

Wie langwierig und mühevoll der Weg über das Bewilligungsverfahren bei identischen oder gleich gelagerten Aufgaben ist, zeigt beispielsweise das von der Datenschutzstelle initiierte koordinierte Vorgehen betreffend die Online-Zugriffe der Kirchgemeinden auf die Einwohnerregister (siehe Tätigkeitsbericht 2019, S. 11). Ein Teil der Gesuche der (katholischen) Kirchgemeinden konnte abgeschlossen werden, ein Teil ist noch pendent, und ein Teil der Kirchgemeinden hat trotz Aufforderung noch (immer) kein Gesuch gestellt.

3.2 Gesetz über die Videoüberwachung im öffentlichen und im öffentlich zugänglichen Raum

Im Kanton Zug ist die Fachstelle Videoüberwachung der Zuger Polizei (FaVü) primäre Anlaufstelle im Bereich Videoüberwachung. Sie stellt ein Musterformular für Gesuche betreffend Videoüberwachung und weitere Informationen zur Verfügung. Der Datenschutzstelle kommen aufgrund der Video- und Datenschutzgesetzgebung die folgenden beiden Aufgaben zu:

- Stellungnahme bei Gesuchen um Bewilligungen
- Veröffentlichung von Entscheiden (siehe dazu Tätigkeitsbericht 2019, S. 12 f.)

In der Praxis führt die vorgängige, vor allem auf video- und kriminaltechnische Aspekte fokussierte Beratung des gesuchstellenden Organs durch die FaVü und die anschliessende datenschutzrechtliche Beurteilung durch die Datenschutzstelle teilweise zu Unverständnis bei den Gesuchstellern. Der unterschiedliche Fokus der FaVü und der Datenschutzstelle kann zu einer unterschiedlichen Beurteilung der eingereichten Gesuchunterlagen führen: Diese könnten für die Beurteilung von video- und kriminaltechnischen Aspekte durch die FaVü genügen, für die Beurteilung von Datenschutz und Informationssicherheit genügen sie aber in aller Regel nicht.

Videoüberwachung Schulareal

Die Datenschutzstelle hatte im Berichtsjahr zu einem Gesuch um Bewilligung der Videoüberwachungsanlage eines Schulareals Stellung zu nehmen. Die Videoüberwachung betraf u.a. Pausenplätze, Innenhof, gedeckte Eingangsbereiche, Aussensportanlagen, Spielplätze, Sitzgelegenheiten und Fahrradständer. Eine Begehung des Areals hatte zuvor (ohne Einladung bzw. Teilnahme der Datenschutzstelle) mit der Fachstelle Videoüberwachung der Zuger Polizei stattgefunden, welche das Gesuch positiv beurteilte.

Die Datenschutzstelle hatte nicht nur aufgrund der unklaren und missverständlichen Zweckumschreibung der Videoüberwachung, sondern auch aufgrund deren räumlichen und zeitlichen Ausdehnung und der ungenügenden Dokumentation betreffend Informationssicherheit verschiedene Empfehlungen abgegeben.

Das verantwortliche Organ hat lediglich (teilweise) eine der Empfehlungen (zur zeitlichen Einschränkung) berücksichtigt: Die ursprünglich vorgesehene Rund-um-die-Uhr-Überwachung an Samstagen und Sonntagen wurde auf die Zeitdauer von 20 bis 6 Uhr begrenzt, die auch an Wochentagen vorgesehen war.

Aufgrund der unbeantwortet gebliebenen Fragen und/oder fehlenden Informationen lassen sich die wesentlichsten offenen Punkte – aus Sicht Datenschutzstelle – wie folgt zusammenfassen:

- Keine Klärung der Verhältnismässigkeit möglich (u.a. keinerlei Angaben zu Ausmass/Schwere der Beschädigungen sowie zu Ausmass in örtlicher/räumlicher und zeitlicher Hinsicht; Fokus der Überwachung nicht objektbezogen; keine Offenlegung der protokollierten «sich wiederholenden» Sachbeschädigungen; Unklarheiten betreffend Überwachungszweck/Schutzobjekte).
- Keine von der Datenschutzstelle verlangten zusätzlichen Informationen, welche die Beurteilung der Informationssicherheit der (räumlich und zeitlich) sehr umfassenden Videoüberwachungsanlage erlauben (z.B. Schnittstelle zu Drittsystemen/Internet, Art der Zugriffe, Berechtigungskonzept).
- Unklarheit betreffend die «den Strafverfolgungsbehörden überlassenen» Möglichkeit der Echtzeitüberwachung.
- Keine Prüfung der vorgeschlagenen, andernorts erfolgreich praktizierten Umsetzung von Videoüberwachungen bei Schularealen und -anlagen insbesondere auch betreffend eine datenschutzkonforme und zweckdienliche Überwachung von Eingangsbereichen.

Schwerer als der Umstand, dass Bewilligungen erteilt werden, ohne dass die verantwortlichen Organe Fragen zu einer von ihnen in Auftrag gegebenen und betriebenen Videoüberwachung beantworten können, wiegt, dass diese Überwachung fortan auf Kosten der betroffenen Bürgerinnen und Bürger bzw. Einwohnerinnen und Einwohner einer Gemeinde erfolgt. Bspw. führt die bei (gedeckten) Eingangsbereichen bewegungsgesteuerte Videoüberwachung zu einer permanenten Videoüberwachung/-aufzeichnung der sich im Aufnahmebereich aufhaltenden Personen (während der Aufnahmezeiten). Dabei liesse sich der – berechnete und verhältnismässige – Zweck einer Videoüberwachung in Eingangsbereichen technisch ohne weiteres durch eine vorfallauslösende Videoüberwachung bei unberechtigtem Zutritts-/Einbruchversuch umsetzen (mit Frontal-Aufzeichnung der Täterschaft von innen).

Eine Überwachung der (gedeckten) Eingangsbereiche, nur um Kinder und Jugendliche präventiv davon abzuhalten, sich dort aufzuhalten, lässt sich weder unter dem Aspekt des öffentlichen Interesses noch der Verhältnismässigkeit rechtfertigen und ist als unzulässiger Grundrechtseingriff zu qualifizieren.

Auf das Angebot, die Verantwortlichen bei einer datenschutzkonformen Ausgestaltung der geplanten Videoüberwachung zu unterstützen, ist die zuständige Gemeindeverwaltung nicht eingegangen. Die Datenschutzstelle hat Anfang 2022 aus dem Amtsblatt erfahren, dass die Videoüberwachung vom Gemeinderat bewilligt wurde.

4. Kontrollen

Es gehört zu den gesetzlichen Aufgaben der Datenschutzstelle, dass sie die Einhaltung der Datenschutzvorschriften in rechtlicher, technischer und organisatorischer Hinsicht überwacht und dazu auch Kontrollen bei den verantwortlichen Organen durchführt.

Die Datenschutzstelle verfügt seit März 2020 über einen Mitarbeiter mit IT-Know-how (50%-Pensum), zu dessen Aufgaben u.a. auch die Durchführung von Kontrollen und Audits zählt. Bisher konnte die Datenschutzstelle allerdings noch keine eigenen Kontrollen planen. Die zur Verfügung stehenden Ressourcen mussten für die Beratung in den zahlreichen – zunehmend auch grösseren – IT- und Digitalisierungsprojekten – und die erforderliche Erarbeitung von Informationen und Hilfsmitteln für die verantwortlichen Organe im Zusammenhang mit dem revidierten Datenschutzgesetz (Datenschutz-Folgenabschätzung) eingesetzt werden.

Nachaudit Printing-Lösung

Die Datenschutzstelle hatte 2019 ein Audit der kantonalen Printing-Lösung in Auftrag gegeben. Die Printing-Lösung war zuvor im Rahmen eines Outsourcings ausgeschrieben und einem privaten Dritten übertragen worden. Mittels Fragebogen und Interviews wurde u.a. die Umsetzung der Anforderungen aus dem Pflichtenheft der Ausschreibung überprüft. Die Feststellungen des Audit-Berichts wurden anschliessend vom AIO abgearbeitet, sodass im Berichtsjahr die Nachkontrolle durchgeführt und erfolgreich abgeschlossen werden konnte.

Follow-up-Prozess der Schengen-Evaluierung

Die Datenschutzstelle wurde auch im Berichtsjahr um eine Aktualisierung ihrer Stellungnahme betreffend die vom Rat der EU im Jahr 2019 veröffentlichten Empfehlungen aus der Schengen-Evaluierung gebeten (data.consilium.europa.eu/doc/document/ST-7281-2019-INIT/de/pdf; siehe dazu Tätigkeitsbericht 2019, S. 14).

Die Datenschutzstelle hatte bereits im Vorjahr darauf hingewiesen, dass der Empfehlung betreffend Verfügungskompetenz (Empfehlung 4) nicht gefolgt wurde und auch mit der (Teil-)Revision des Datenschutzgesetzes (am 1. September 2020 in Kraft getreten) keine Verfügungskompetenz der Datenschutzstelle eingeführt wurde. Im Vergleich zum Vorjahr verfügt die Datenschutzstelle neu über Unterstützung im administrativen Bereich (im Umfang eines 50%-Pensums).

5. Schulung und Öffentlichkeitsarbeit

Schulungen

Im Berichtsjahr hat die Fachstelle punkto Eltern, Kinder & Jugendliche, die über eine Leistungsvereinbarung mit dem Kanton in den Bereichen Mütter- und Väterberatung, Kinder- und Jugendhilfe, Kinder- und Jugendförderung sowie Gassenarbeit verfügt, eine Impulstagung über digitale Zusammenarbeit durchgeführt. Die Datenschutzstelle hat an der Tagung mit einem Referat zum Thema «Datenschutz und Datensicherheit in digitalisierten Arbeitsumgebungen» teilgenommen.

Im Übrigen fanden im Berichtsjahr keine Schulungen statt. Namentlich fielen auch die verwaltungsinternen Veranstaltungen für neue Mitarbeitende aus, an denen die Datenschutzbeauftragte üblicherweise mit einem Kurzreferat teilnimmt.

Website

Nachdem die (Teil-)Revision des Datenschutzgesetzes per 1. September 2020 in Kraft getreten war, ist die dazugehörige Revision der Verordnung über die Datensicherheit, die in «Verordnung über die Informationssicherheit von Personendaten» umbenannt wurde, erst Anfang Januar 2021 in Kraft getreten (VIP; BGS 157.12). Entsprechend hat die Datenschutzstelle ihre Website und die bereits zur Verfügung gestellten Informationen und Hilfsmittel im Berichtsjahr aktualisiert, weiterentwickelt und überarbeitet.

6. Zusammenarbeit mit anderen Datenschutzstellen

privatim

Die Datenschutzstelle des Kantons Zug ist Mitglied von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten (privatim.ch). Privatim gehören die Datenschutzbehörden aller 26 Kantone und von acht Städten an sowie der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) und die Datenschutzbeauftragte des Fürstentums Liechtenstein.

Nach einer zweijährigen Pause wurde im Berichtsjahr die Herbst-Plenumsveranstaltung wieder durchgeführt. Ein Schwerpunkt der Veranstaltung war das Thema Cloud, namentlich die Überarbeitung des von privatim herausgegebenen «Merkblatt Cloud-spezifische Risiken und Massnahmen». Dazu wurde im Berichtsjahr vorgängig eine Konsultation bei den kantonalen Datenschutzstellen durchgeführt. Konzept und Hauptfragen aus der Konsultation zum Merkblatt wurden anlässlich der Plenumsveranstaltung diskutiert. Inzwischen hat privatim das überarbeitete «[Merkblatt Cloud-spezifische Risiken und Massnahmen](#)» publiziert.

Für die Datenschutzstelle ist der Austausch mit anderen Datenschutzbeauftragten über kantonsübergreifende Themen von grossem Nutzen und wird immer wichtiger. U.a. ermöglicht er, sich einen Überblick über Stand sowie Art und Weise der Umsetzung gleicher oder ähnlicher Vorhaben durch die Organe anderer Kantone zu verschaffen. Der Austausch erfolgt einerseits im Rahmen von Arbeitsgruppen, in denen sich die Datenschutzstelle engagiert (AG Digitale Verwaltung, AG ICT, AG Sicherheit), andererseits aber auch in Form des Ad-hoc-Austausches zu einzelnen Themen.

Themen der Zusammenarbeit im Berichtsjahr waren bspw. das Krebsregister (koordiniertes Vorgehen betreffend Vorabkonsultation zusammen mit Kantonen, welche dieselbe Krebsregistrierungssoftware einsetzen) und eUmzug (konsolidierte Rückmeldung an eOperations AG betreffend datenschutzrechtliche Anforderungen

an Auftragsdatenbearbeitung sowie technische und organisatorische Massnahmen [TOM]). Der ICT-Mitarbeiter der Datenschutzstelle des Kantons Zug leitete im vergangenen Jahr zudem eine Unterarbeitsgruppe der AG ICT, die sich mit dem Einsatz von Microsoft 365 beschäftigt.

Zusammenarbeit der Zentralschweizer Datenschutzbeauftragten

Die Datenschutzbeauftragten der Kantone Luzern, Schwyz, Obwalden, Nidwalden, Uri und Zug pflegen seit 2019 einen engeren Austausch untereinander. Zusammenarbeit und erforderliche Abstimmung ergeben sich einerseits aufgrund bestehender Konkordate (Polizei- und Psychiatrie-Konkordat) sowie weiterer gemeinsamer Themen.

Die Zentralschweizer Datenschutzbeauftragten wurden im Berichtsjahr zudem als Ansprechpartner im Zusammenhang mit einem interkantonalen Projekt der Zentralschweizer Polizeikommandantenkonferenz (ZPKK) konsultiert und von der Zentralschweizer Regierungskonferenz (ZRK) um Prüfung eines allfälligen Zusammenarbeitspotenzials gebeten.

Hintergrund der Anfrage betreffend Zusammenarbeitspotenzial waren die anlässlich der Schengen-Evaluation 2018 im Kanton Luzern festgestellten Mängel. Der im Evaluationsbericht ausgewiesene Handlungsbedarf betraf primär die Erhöhung der Ressourcen, um die Durchführung regelmässiger SIS-II- und VIS-Kontrollen sicherzustellen. Die Datenschutzbeauftragten von Luzern, Nidwalden, Obwalden, Schwyz, Uri und Zug haben im Berichtsjahr zur Anfrage der Zentralschweizer Regierungskonferenz im März 2021 Stellung genommen und dabei festgehalten, dass zwischen den Datenschutzbeauftragten der Zentralschweiz in den relevanten Bereich bereits eine gut funktionierende, in der Praxis ausreichende Zusammenarbeit besteht. Im Bereich der Informatik-, SIS-II- und VIS-Kontrollen erfolgt die Zusammenarbeit u.a. in der Koordinationsgruppe Schengen, der die kantonalen Datenschutzbeauftragten angehören und welche der EDÖB präsidiert.

Die Zentralschweizer Datenschutzbeauftragten wiesen darauf hin, dass die Kontrollen zum einen Kenntnisse der kantonalen Gegebenheiten erfordern, zum anderen aber auch ausreichende personelle und finanzielle Ressourcen voraussetzen. Eine noch engere Zusammenarbeit, aber auch häufigere Kontrollen seien nur möglich, wenn ihnen in den jeweiligen Kantonen oder aus einem gemeinsamen Pool mehr Ressourcen zur Verfügung gestellt würden. Festgehalten wird zudem, dass u.a. der Föderalismus eine Hürde für den Ausbau der Zusammenarbeit darstellt, wenn Kontrollen kantonsübergreifend vorgenommen werden sollten. Der Ausbau der Zusammenarbeit bringt viele Umsetzungsfragen mit sich, die auf politischer Ebene zu beantworten sind und nicht durch die kantonalen Datenschutzbeauftragten beantwortet werden können.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

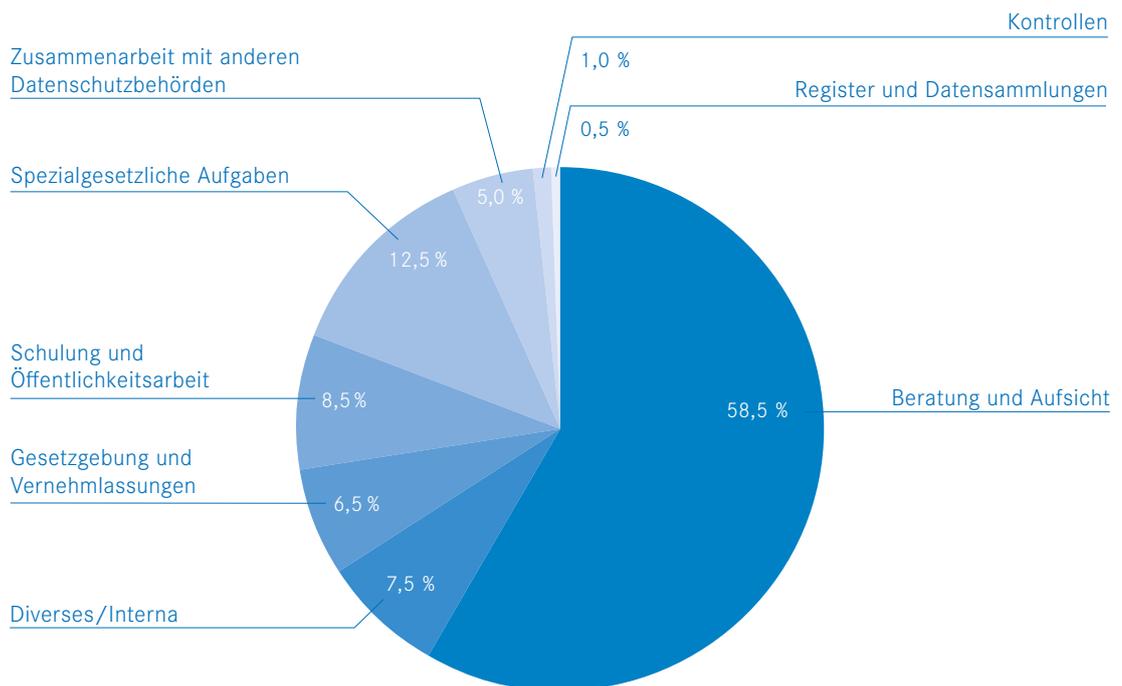
Im Rahmen des Schengen-Assoziierungsabkommens ist die Zusammenarbeit der kantonalen Datenschutzbeauftragten mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB (www.edoeb.admin.ch) gesetzlich vorgeschrieben. So sind die Aufsichtsstellen verpflichtet, bei der Beaufsichtigung der Datenbearbeitungen, die im Rahmen des Assoziierungsabkommens erfolgen, aktiv zusammenzuarbeiten. Die Zusammenarbeit erfolgt über die «Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Umsetzung des Schengen-Assoziierungsabkommens». Im Berichtsjahr fanden keine physischen Treffen statt, die kantonalen Datenschutzbeauftragten wurden via Onlinekonferenz und auf schriftlichem Weg informiert.

7. Personal und Statistik

Personal

Dank der bewilligten 50%-Stelle für einen/eine Mitarbeiter/in im Bereich Administration konnte die Datenschutzstelle ihre Stellenprocente im Berichtsjahr erhöhen. Die Datenschutzstelle verfügt seit 1. August 2021 über 260 Stellenprocente, verteilt auf die Datenschutzbeauftragte (80%), ihre Stellvertreterin (80%), den Mitarbeiter ICT (50%) und die neue Fachmitarbeiterin Administration (50%).

Statistik



Der Schwerpunkt der Tätigkeit der Datenschutzstelle liegt wie in den Vorjahren auf der Beratung und Aufsicht. Die Aufwendungen in diesem Bereich sind im Berichtsjahr weiter angestiegen (58,5%; 2020: 55,5%). Zurückzuführen ist dies auf die Beratung und Aufsicht der kantonalen Verwaltung, wo der Aufwand auf 49,7% (2020: 43%) gestiegen ist. Im Vergleich zum Vorjahr etwas weniger Ressourcen wurden für die Beratung und Aufsicht der Gemeinden (7,1%; 2020: 10,5%) sowie für die Beratung von Privaten (1,7%; 2019: 2%) eingesetzt.

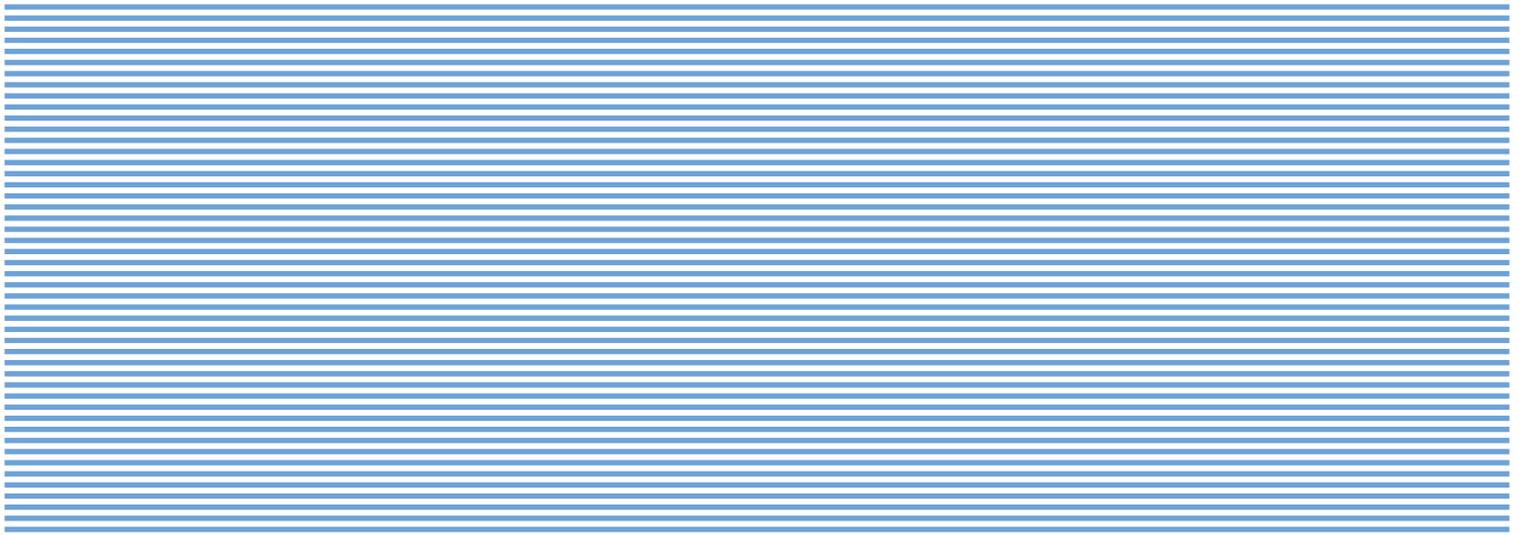
Weiter gesunken ist im Berichtsjahr der Aufwand in der Gesetzgebung (auf 6,5%; 2020: 12%). Nachdem der Gesetzgebungsprozess zur Revision des Datenschutzgesetzes (DSG; BGS 157.1) und der Verordnung über die Informationssicherheit von Personendaten (VIP; BGS 157.12) abgeschlossen werden konnte, standen keine kantonalen Gesetzgebungsprojekte an, in welche die Datenschutzstelle in vergleichbarer Weise involviert wäre. Dennoch hat sie sich mit einzelnen kantonalen Gesetzgebungsvorhaben intensiv auseinandergesetzt und sich dazu geäußert. Aus Ressourcengründen verzichtet sie allerdings zunehmend auf Stellungnahmen zu eidgenössischen Vorlagen.

Im Vergleich zum Vorjahr um 3,5% gestiegen sind dagegen die für die spezialgesetzlichen Aufgaben aufgewendeten Ressourcen (12,5%; 2020: 9%). Darunter fallen namentlich die Stellungnahmen und Empfehlungen, welche die Datenschutzstelle im Rahmen der Bewilligungsverfahren gemäss Online-Verordnung und Videoüberwachungsgesetz abzugeben hat (siehe Ziff. 3).

Für die Kontrolltätigkeit wird im Berichtsjahr ein Aufwand von 1% ausgewiesen (2020: unter 0,5%). Dieser ist auf den Abschluss der Nachkontrolle des Audits der kantonalen Printing-Lösung zurückzuführen.

Der Aufwand im Bereich Schulung und Öffentlichkeitsarbeit ist im Vergleich zum Vorjahr etwas gesunken (-3%) und betrug 8,5%. Darunter fallen Schulungen, die Erstellung des Tätigkeitsberichts, die Überarbeitung verschiedener Hilfsmittel, Aktualisierungen der Website sowie die Planung von Massnahmen im Bereich Information und Sensibilisierung für das kommende Jahr. Intensiviert hat sich im Berichtsjahr die Zusammenarbeit mit anderen Datenschutzbehörden (5%; 2020: 3,5%), was insbesondere auf die Zusammenarbeit im Rahmen von privatim und die Zusammenarbeit der Zentralschweizer Datenschutzbeauftragten in einzelnen Projekten zurückzuführen ist (siehe Ziff. 6, Zusammenarbeit mit anderen Datenschutzstellen).

Die unter Diverses/Interna verbuchten Aufwendungen sind leicht gesunken (7,5%, 2020: 8%), namentlich auch, weil im Berichtsjahr die unter Diverses/Interna verbuchten Weiterbildungsveranstaltungen der Mitarbeitenden der Datenschutzstelle grösstenteils wegfielen. Neben dem Aufwand für eigene Weiterbildungen fallen unter diesen Posten alle internen Arbeiten, die nicht den anderen Aufgaben zugeordnet werden können: Budget/Rechnungswesen, Personal, Aufwendungen für Administratives, Archivierung usw.



© 2022 Kanton Zug

Herausgeberin

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

Gestaltung

Christen Visuelle Kommunikation, Zug