



Ergebnis der ersten Lesung vom 18. Dezember 2018

## **Änderung des Datenschutzgesetzes**

Bericht und Antrag des Regierungsrats  
vom

Sehr geehrter Herr Präsident  
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen die Vorlage zu einer Änderung des Datenschutzgesetzes und erstatten Ihnen dazu den Bericht, den wir wie folgt gliedern:

<b>1.</b>	<b>In Kürze</b>	<b>2</b>
<b>2.</b>	<b>Ausgangslage</b>	<b>2</b>
<b>3.</b>	<b>Handlungsbedarf</b>	<b>4</b>
3.1	Richtlinie (EU) 2016/680	4
3.2	Datenschutzkonvention SEV 108	6
3.3	Datenschutz-Grundverordnung	7
3.4	Praxisanpassungen	7
3.5	Fazit	8
<b>4.</b>	<b>Umsetzung</b>	<b>8</b>
4.1	Bund	8
4.2	Kanton Zug	8
<b>5.</b>	<b>Ergebnis der Vernehmlassung</b>	<b>9</b>
<b>6.</b>	<b>Erläuterungen zum Gesetzesentwurf</b>	<b>9</b>
6.1	Ziffer I: Erläuterungen zu den einzelnen Bestimmungen	9
6.2	Ziffer II: Fremdänderungen	26
6.3	Ziffer III: Fremdaufhebungen	32
6.4	Ziffer IV: Inkrafttreten	32
<b>7.</b>	<b>Finanzielle Auswirkungen und Anpassungen von Leistungsaufträgen</b>	<b>32</b>
7.1	Finanzielle Auswirkungen auf den Kanton	32
7.2	Finanzielle Auswirkungen auf die Gemeinden	33
7.3	Anpassungen von Leistungsaufträgen	33
<b>8.</b>	<b>Zeitplan</b>	<b>33</b>
<b>9.</b>	<b>Antrag</b>	<b>33</b>

## 1. In Kürze

### **Kanton Zug passt Datenschutzgesetz europäischen Vorgaben an**

**Der Kanton Zug ist verpflichtet, das kantonale Datenschutzgesetz den europäischen Vorgaben anzupassen. Zu den wichtigsten Neuerungen zählt, dass Pflichten der verantwortlichen Organe präzisiert und stärker auf den Schutz der betroffenen Personen ausgerichtet werden. Im Übrigen sollen geringfügige terminologische und praktische Anpassungen vorgenommen werden. Die Änderungen beschränken sich auf das Notwendigste.**

Die gesetzgeberischen Tätigkeiten auf europäischer Ebene verlangen sowohl eine Anpassung des Bundesrechts (für Datenbearbeitungen durch Bundesorgane und Private) als auch des kantonalen Rechts (für Datenbearbeitungen durch Organe des Kantons Zug). Der Bund hat beschlossen, die notwendigen Anpassungen in zwei Teilen vorzunehmen: Zuerst soll insbesondere mit dem Erlass des Bundesgesetzes über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (nachfolgend: SDSG) sichergestellt werden, dass die Schengen-Anforderungen schnellstmöglich eingehalten werden können. In einem zweiten Schritt wird das Bundesgesetz über den Datenschutz (nachstehend: DSG-Bund) totalrevidiert. Im Kanton Zug ist eine Teilrevision des Datenschutzgesetzes vom 28. September 2000 (BGS 157.1; nachfolgend: DSG) nötig.

### **Umsetzung der Vorgaben des europäischen Rechts**

Die Pflichten der verantwortlichen Organe werden präzisiert und stärker auf den Schutz der betroffenen Personen ausgerichtet. Die verpflichtenden Vorgaben des europäischen Rechts verlangen zudem eine effektivere Kontrolle durch die Datenschutzstelle. Die Befugnisse der Datenschutzstelle werden künftig mit den Befugnissen der entsprechenden ausländischen Kontrollbehörden vergleichbar sein. Neu wird der Datenschutzstelle – anders als bisher mit dem Mechanismus des Aussprechens von Empfehlungen – unter anderem die Kompetenz zum Erlass von verbindlichen Verfügungen zugestanden. Im Gegensatz zum europäischen Ausland soll sie jedoch keine Verwaltungssanktionen aussprechen können.

### **Terminologische Neuerungen**

Der Revisionsentwurf modernisiert die verwendete Terminologie, insbesondere, um die Vereinbarkeit mit dem europäischen Recht zu verbessern. So werden gewisse Begriffe aus dem europäischen Recht übernommen. Der Begriff «Persönlichkeitsprofil», der eine schweizerische Besonderheit darstellt, wird neu durch den Begriff des «Profiling» abgelöst.

### **Geringfügige Praxisanpassungen**

Anpassungsbedarf besteht ferner bei der Bearbeitung von Daten zu Forschungszwecken oder hinsichtlich der Verantwortung der Organe, welche Personendaten bearbeiten. Wo möglich, soll eine Einheitlichkeit mit den vorgesehenen bundesrechtlichen Regelungen geschaffen werden. So soll beispielsweise der Geltungsbereich des kantonalen Datenschutzgesetzes insofern angepasst werden, als dass die Daten juristischer Personen davon ausgenommen sind.

## 2. Ausgangslage

Auf internationaler Ebene wird dem Datenschutz immer grössere Beachtung geschenkt. So hat die Europäische Union am 27. April 2016 ihre Datenschutzgesetzgebung revidiert. Diese umfasst zwei Rechtsakte: Zum einen die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (nachfolgend: Datenschutz-

Grundverordnung [DSGVO])<sup>1</sup> und zum anderen die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts (nachfolgend: Richtlinie (EU) 2016/680)<sup>2</sup>. Die Datenschutz-Grundverordnung ist am 25. Mai 2016 und die Richtlinie (EU) 2016/680 am 5. Mai 2016 in Kraft getreten.

Die Schweiz ist gemäss Artikel 2 Absatz 3 des Schengen-Assoziierungsabkommens<sup>3</sup> grundsätzlich verpflichtet, jede Weiterentwicklung des Schengen-Besitzstands zu akzeptieren, umzusetzen und anzuwenden. Nur die Richtlinie (EU) 2016/680 ist Teil des Schengen-Besitzstands. Die Datenschutz-Grundverordnung ist in der Schweiz nicht direkt anwendbar, jedoch ist sie insofern von Bedeutung, als dass die Europäische Kommission gestützt darauf entscheidet, ob Drittstaaten – wie die Schweiz – ein angemessenes Datenschutzniveau vorweisen können.

Der Europarat wiederum hat einen Entwurf für eine Revision der Konvention SEV 108 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten ausgearbeitet. Die revidierte Konvention SEV 108 (nachfolgend: SEV 108)<sup>4</sup> wurde am 18. Mai 2018 vom Ministerkomitee des Europarats verabschiedet. Da die Schweiz bereits Vertragspartei der Vorgänger-Konvention von 1981<sup>5</sup> ist, beabsichtigt der Bundesrat, dem Parlament auch das Änderungsprotokoll der Konvention zur Genehmigung vorzulegen. Bevor die revidierte Konvention ratifiziert werden kann, muss das schweizerische Recht den neuen Bestimmungen entsprechend angepasst werden.

Auf Bundesebene war der Datenschutz in den vergangenen Jahren vermehrt Gegenstand zahlreicher parlamentarischer Interventionen. Da der deutliche politische Wille besteht, die Bundesgesetzgebung in diesem Bereich zu stärken, unterzieht der Bund derzeit das DSG-Bund einer Totalrevision<sup>6</sup>. Die bundesrechtlichen Gesetzgebungsarbeiten beruhen auf einem Bundesratsbeschluss, wonach eine Vorlage mit zwei Zielsetzungen ausgearbeitet werden soll: Einerseits sollen die Schwächen des Datenschutzgesetzes behoben werden, die aufgrund der rasanten technologischen Entwicklung entstanden sind. Andererseits soll den Entwicklungen auf der Ebene des Europarats und der EU Rechnung getragen werden. Die künftige Gesetzgebung soll die Anforderungen der Richtlinie (EU) 2016/680 übernehmen, damit die Schweiz auch in Zukunft ihren Schengen-Verpflichtungen nachkommen kann. Darüber hinaus soll die Vorlage mit der SEV 108 vereinbar sein, damit die Schweiz das revidierte Übereinkommen so rasch als möglich ratifizieren kann. Zudem werden die Empfehlungen umgesetzt, welche die EU der Schweiz im Jahr 2014 im Rahmen der Schengen-Evaluation zukommen liess. Dabei wurde insbesondere empfohlen, die Kompetenzen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten auszubauen. Schliesslich soll sich die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Datenschutz-Grundverordnung annähern. Diese Annäherung bildet – zusammen mit der Ratifizierung der revidierten Konvention SEV 108 – die zentrale Voraussetzung dafür, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht.

Im Sommer 2018 hat sich der Nationalrat für eine Etappierung der Revision des DSG-Bund ausgesprochen. Der Ständerat ist diesem Anliegen in der Herbstsession gefolgt. Bereits am 28. September 2018 hat der Bund ein Bundesgesetz über die Umsetzung der Richtlinie (EU)

---

<sup>1</sup> <[https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/05/CELEX\\_32016R0679\\_DE\\_TXT.pdf](https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/05/CELEX_32016R0679_DE_TXT.pdf)>.

<sup>2</sup> <<https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/eu-richtlinie-d.pdf>>.

<sup>3</sup> SR 0.362.31.

<sup>4</sup> <[https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016807c65bf](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf)>.

<sup>5</sup> <<https://rm.coe.int/1680078b38>>.

<sup>6</sup> Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 ff.

2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (Weiterentwicklung des Schengen-Besitzstands) sowie darin enthalten (Anhang Ziff. I<sup>bis</sup>) das umfassende Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz, SDSG)<sup>7</sup> verabschiedet. Mit diesem Vorgehen soll sichergestellt werden, dass die Schengen-Anforderungen (Richtlinie [EU] 2016/680) schnellstmöglich eingehalten werden können. Die Arbeiten an der Totalrevision des DSG-Bund sollen im Anschluss an diese «erste Etappe» zügig an die Hand genommen werden.

Die Übernahme der Richtlinie (EU) 2016/680 und die Annahme des Änderungsprotokolls zur Konvention SEV 108 durch die Schweiz sind auch für die Kantone bindend. Diese müssen ihre kantonalen Gesetzgebungen insoweit anpassen, als sie die Anforderungen dieser Instrumente nicht erfüllen. Die vorliegende Umsetzung orientiert sich inhaltlich an dem von der Konferenz der Kantonsregierungen erarbeiteten Leitfaden zur EU-Datenschutzreform/Modernisierung der Europaratskonvention 108, der den Anpassungsbedarf der kantonalen Datenschutzgesetze aufzeigt (nachfolgend: KdK-Leitfaden). Ergänzend wird auch auf Bestimmungen des Entwurfs für die Totalrevision des DSG-Bund (Stand 15. September 2017) abgestellt oder verwiesen. Dabei ist zu berücksichtigen, dass im Rahmen des vorliegenden Berichts und Antrags nicht tagessaktuell auf bundesrechtliche Anpassungen eingegangen werden kann, da es sich um laufende Gesetzgebungsprojekte handelt. Überdies wird mit dem SDSG (dessen Referendumsfrist am 17. Januar 2019 abläuft) erst die Richtlinie (EU) 2016/680, insbesondere ohne die SEV 108 umgesetzt, weshalb vorliegend auch nicht auf das SDSG abgestellt werden kann.

Betreffend die Übernahme der Richtlinie (EU) 2016/680 gilt für die Schweiz eine Umsetzungsfrist von zwei Jahren ab dem Zeitpunkt der Notifikation durch die Europäische Union. Da diese am 1. August 2016 erfolgte, hätte die Datenschutzreform sowohl vom Bund als auch von den Kantonen bis zum 1. August 2018 umgesetzt werden müssen. Eine fristgerechte Umsetzung war unter Einhaltung des ordentlichen Gesetzgebungsprozesses aber unrealistisch. Der Kanton Zug hat, wie fast alle Kantone, die Vernehmlassungsarbeiten des Bundes zur Totalrevision des DSG-Bund sowie die Erstellung des KdK-Leitfadens abgewartet, um unnötige und zeitintensive Rechercharbeiten zu vermeiden. Der Bericht und Antrag übernimmt deshalb nachfolgend wesentliche Ausführungen der obgenannten Botschaft des Bundes zum Handlungsbedarf aufgrund der internationalen Vorgaben. Eine Inkraftsetzung des revidierten Gesetzes im Jahr 2020 ist realistisch und anzustreben.

### **3. Handlungsbedarf**

#### **3.1 Richtlinie (EU) 2016/680**

Die Richtlinie (EU) 2016/680 ist darauf ausgerichtet, personenbezogene Daten zu schützen, die zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschliesslich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, bearbeitet werden. Sie soll ein hohes Schutzniveau für personenbezogene Daten gewährleisten und gleichzeitig aber den Austausch dieser Daten zwischen den zuständigen Behörden der verschiedenen Schengen-Staaten erleichtern. Sie gilt sowohl für grenzüberschreitende Datenbearbeitungen als auch für Datenbearbeitungen, die von den Polizei- und Justizbehörden ausschliesslich auf innerstaatlicher Ebene durchgeführt werden. Die Richtlinie (EU) 2016/680 nimmt Justizbehörden nicht generell vom Anwendungsbereich aus, sondern

---

<sup>7</sup> <<https://www.admin.ch/opc/de/federal-gazette/2018/6003.pdf>>; BBl 2018 6017 ff.

lässt den Mitgliedstaaten lediglich die Möglichkeit offen, Justizbehörden gemäss Art. 45 Abs. 2 nicht der Aufsicht des oder der Datenschutzverantwortlichen unterstellen zu müssen («Die Mitgliedstaaten können vorsehen, dass ihre Aufsichtsbehörde nicht für die Überwachung der von anderen unabhängigen Justizbehörden im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen zuständig ist»).

Die wichtigsten **Neuerungen** sind:

- Ausnahmen vom Anwendungsbereich sind in der Richtlinie (EU) 2016/680 nicht vorgesehen. Sie gilt für alle Datenbearbeitungen, die von den Polizei- und Justizbehörden durchgeführt werden.
- Die verschiedenen Kategorien betroffener Personen müssen unterschieden sowie Regeln zur Unterscheidung der Daten und zur Überprüfung der Qualität der Daten eingeführt werden.
- Die Rechtmässigkeit der Datenbearbeitung wird vorgeschrieben, indem Datenbearbeitungen im Wesentlichen auf einer gesetzlichen Grundlage beruhen müssen.
- Neue Rechte für die betroffene Person sind vorzusehen. So ist die bzw. der Verantwortliche verpflichtet, die Datenbearbeitung einzuschränken, wenn die betroffene Person die Richtigkeit der Daten bestreitet und die Richtigkeit nicht festgestellt werden kann.
- Im Sinne der Pflichten des für die Datenbearbeitung Verantwortlichen und des Auftragsbearbeitenden führt die Richtlinie (EU) 2016/680 in Kapitel IV die beiden Grundsätze Datenschutz durch Technikgestaltung («privacy by design») und Datenschutz durch datenschutzfreundliche Voreinstellungen («privacy by default») ein.
- Die für die Datenbearbeitung Verantwortlichen sind verpflichtet, vor bestimmten Bearbeitungen eine Datenschutz-Folgenabschätzung durchzuführen und gegebenenfalls die Aufsichtsbehörde zu konsultieren.
- Es besteht die Pflicht, in gewissen Fällen der Aufsichtsbehörde eine Verletzung des Datenschutzes zu melden und gegebenenfalls die betroffene Person zu benachrichtigen.
- Die Europäische Kommission prüft das Schutzniveau, das ein Drittland, ein Gebiet oder ein Verarbeitungssektor in einem Drittland bietet. Hat die Europäische Kommission die Angemessenheit des Schutzniveaus in einem Drittstaat nicht durch Beschluss festgestellt, darf die Datenübermittlung nur erfolgen, wenn geeignete Garantien bestehen oder wenn in bestimmten Fällen eine Ausnahme vorliegt.
- Die Schengen-Staaten müssen im Bereich des Datenschutzes unabhängige Aufsichtsbehörden einsetzen. Diese Behörde ist aber nicht für die Aufsicht über Datenbearbeitungen zuständig, die Gerichte im Rahmen ihrer justiziellen Tätigkeit vornehmen. Die Schengen-Staaten können auch eine Ausnahme der Aufsichtsbefugnis für jene Datenbearbeitungen vorsehen, die durch andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit erfolgen.
- Die unabhängige Aufsichtsbehörde muss über wirksame Untersuchungsbefugnisse verfügen, d.h. sie muss zumindest vom Verantwortlichen und vom Auftragsbearbeitenden Zugang zu den bearbeiteten Daten und allen Informationen erhalten, die zur Erfüllung ihrer Aufgaben notwendig sind.
- Die Aufsichtsbehörde soll auch über wirksame Befugnisse verfügen, um gegen rechtswidrige Datenbearbeitungen wirksam vorgehen zu können. Es sind dies beispielsweise die Befugnis zur Verwarnung eines Verantwortlichen oder eines Auftragsbearbeitenden, zur Anordnung von vorschriftsgemässen Bearbeitungen, gegebenenfalls durch Berichtigung oder Löschung der Daten, sowie zur Verhängung einer vorübergehenden oder endgültigen Beschränkung der Bearbeitung, einschliesslich eines Verbots.

- Die betroffene Person hat das Recht auf Beschwerde bei der Aufsichtsbehörde. Die betroffene Person hat auch das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden Entscheid der Aufsichtsbehörde.

Da die Richtlinie (EU) 2016/680 sowohl für die Mitgliedstaaten der EU als auch für die Schweiz nicht direkt anwendbar ist, bedarf es einer **Umsetzung in das jeweilige nationale Recht**. In der Schweiz braucht es zur Umsetzung der Richtlinie (EU) 2016/680 nicht nur Anpassungen des DSG-Bund und verschiedener Bundesgesetze, sondern aufgrund der unterschiedlichen Zuständigkeiten im Bereich der Datenschutzgesetzgebung auch der kantonalen Datenschutzgesetze und verschiedener kantonalen Erlasse.

### 3.2 Datenschutzkonvention SEV 108

Mit der revidierten SEV 108 wird der Datenschutz auf internationaler Ebene vereinheitlicht und verbessert. Dies verstärkt auch den Schutz der Schweizer Bürgerinnen und Bürger, wenn ihre Personendaten im Ausland bearbeitet werden. Die Bekanntgabe von Daten zwischen den Vertragsparteien wird zudem vereinfacht, wodurch Schweizer Unternehmen einen besseren Zugang zu den Märkten dieser Länder erhalten. Die Unterzeichnung des Änderungsprotokolls zur SEV 108 dürfte zudem eine zentrale Voraussetzung sein, damit die Europäische Union der Schweiz erneut ein angemessenes Datenschutzniveau bestätigt. Nur dadurch bleibt der Zugang zum europäischen Markt weiterhin uneingeschränkt gewährleistet. Die Vertragsparteien müssen die SEV 108 auf alle Datenbearbeitungen in ihrer Rechtsordnung im öffentlichen und privaten Sektor anwenden. Nicht durch diesen Entwurf geregelt werden nur Datenbearbeitungen, die eine Person ausschliesslich im Rahmen von persönlichen oder familiären Tätigkeiten vornimmt.

Der Bundesrat hat in mehreren Antworten auf parlamentarische Vorstösse zum Ausdruck gebracht, dass er die Modernisierung der SEV 108 unterstützt. Die Ratifizierung steht noch aus, denn zusammen mit dieser müssen die erforderlichen Massnahmen zur Umsetzung der Bestimmungen gemäss SEV 108 in Kraft treten.

Die **wesentlichsten Punkte** in der SEV 108 sind:

- Die Vertragsparteien sind verpflichtet, die SEV 108 grundsätzlich auf alle Datenbearbeitungen anzuwenden.
- Die Pflichten des für die Datenbearbeitung Verantwortlichen werden ausgeweitet, indem der zuständigen Aufsichtsbehörde bestimmte Verstösse gegen den Datenschutz zu melden sind. Die Informationspflichten gegenüber der betroffenen Person werden ausgeweitet; so müssen die für die Datenbearbeitung Verantwortlichen zusätzliche Informationen zur Datenbearbeitung als auch zu automatisierten Einzelentscheidungen abgeben. Zudem sind im Vorfeld bestimmter Datenbearbeitungen eine Datenschutz-Folgenabschätzung vorzunehmen und die beiden Grundsätze Datenschutz durch datenschutzfreundliche Technikgestaltung («privacy by design») und Datenschutz durch datenschutzfreundliche Voreinstellungen («privacy by default») anzuwenden.
- Der von der Datenbearbeitung betroffenen Person ist das Recht einzuräumen, nicht einer Entscheidung unterworfen zu sein, die ausschliesslich auf der Grundlage einer automatisierten Bearbeitung ihrer Daten ergeht, ohne dass die betroffene Person ihren Standpunkt geltend machen kann. Das Auskunftsrecht der betroffenen Person wird erweitert und die Bedingungen für deren Einwilligung in die Datenbearbeitung werden klar definiert.
- Die Vertragsparteien sind verpflichtet, ein Sanktionen- und ein Rechtsmittelsystem festzulegen. Der Ausbau des Sanktionensystems ist im Entwurf DSG-Bund vorgesehen; für

das kantonale Recht wird auf die Einführung von Sanktionsmöglichkeiten gegenüber den kantonalen Organen verzichtet.

- Personendaten dürfen nur in einen Drittstaat übermittelt werden, wenn ein angemessener Schutz gewährleistet ist. Ein angemessenes Datenschutzniveau kann durch Rechtsvorschriften des betreffenden Staates oder der empfangenden internationalen Organisation oder durch bestimmte Sicherheiten gewährleistet werden. Wenn kein angemessenes Schutzniveau garantiert ist, dürfen Daten an einen Drittstaat nur weitergegeben werden, wenn der Betroffene gültig eingewilligt hat oder wenn ein bestimmter Ausnahmefall vorliegt. Schliesslich müssen die Vertragsparteien gemäss der SEV 108 vorsehen, dass die Aufsichtsbehörde vom Organ, welches die Daten weitergibt, den Nachweis über die Wirksamkeit der aufgestellten Sicherheiten verlangen und die Datenweitergabe gegebenenfalls verbieten oder aussetzen kann.
- Die Vertragsparteien sind verpflichtet, eine unabhängige Aufsichtsbehörde zu schaffen. Die Aufsichtsbehörden müssen ermächtigt werden, verbindliche, anfechtbare Entscheidungen zu fällen und verwaltungsrechtliche Sanktionen zu verhängen. Der Aufsichtsbehörde muss auch der Auftrag erteilt werden, die Öffentlichkeit und die für die Bearbeitung Verantwortlichen für den Datenschutz zu sensibilisieren.

### **3.3 Datenschutz-Grundverordnung**

Die Datenschutz-Grundverordnung ist der grundlegende Datenschutzerlass auf Ebene der EU. Sie gehört nicht zum Schengen-Besitzstand. Die Richtlinie (EU) 2016/680 und die Verordnung sehen weitgehend übereinstimmende Regelungen vor. Allerdings ist die Verordnung detaillierter, während die Bestimmungen der Richtlinie (EU) 2016/680 auf die Bedürfnisse der Strafbehörden ausgerichtet sind. Die Datenschutz-Grundverordnung regelt hauptsächlich den Schutz von Personen, deren Daten im Rahmen des Binnenmarkts bearbeitet werden, doch sie gilt auch für den öffentlichen Sektor. Sie enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

Für die Schweiz sind die Bestimmungen der Datenschutz-Grundverordnung mangels Schengenrelevanz nicht verbindlich. Der Geltungsbereich ist sehr weit gefasst, indem sich die Verordnung gleichermaßen an Unionsbehörden wie Private richtet. Damit setzt sie verbindliche Minimal-Standards, die bei der Anwendung der beiden anderen Rechtserlasse im öffentlich-rechtlichen wie auch privatrechtlichen (wirtschaftlichen) Bereich (Binnenmarkt) zu beachten sind. Demnach ist sie auch für die Schweiz von Bedeutung. Gemäss Beschluss der Europäischen Kommission vom 26. Juli 2000 besteht in der Schweiz ein angemessenes Datenschutzniveau. Dieser Beschluss kann jedoch jederzeit widerrufen werden. Wenn die Schweiz erneut einen Angemessenheitsbeschluss der Europäischen Union erlangen will, muss sie ihre Gesetzgebung an die europäischen Anforderungen anpassen. Die in der Datenschutz-Grundverordnung festgelegten Kriterien sind künftig massgebend für die Beurteilung, ob die schweizerische Gesetzgebung einen angemessenen Datenschutz gewährleistet. Das kantonale Datenschutzrecht soll daher auch ein angemessenes Schutzniveau im Sinn der Verordnung garantieren.

### **3.4 Praxisanpassungen**

Einzelne Bestimmungen des bestehenden kantonalen Datenschutzgesetzes haben sich in der Praxis nicht bewährt. Anpassungsbedarf besteht etwa bei der Bearbeitung von Daten zu Forschungszwecken. Wo möglich und sinnvoll, soll darüber hinaus eine Einheitlichkeit mit den vorgesehenen bundesrechtlichen Regelungen geschaffen werden. So soll beispielsweise der Geltungsbereich des kantonalen Datenschutzgesetzes angepasst und Daten juristischer Personen davon ausgenommen werden. Nicht zuletzt soll das Gesetz aktualisiert werden, um mit

den fortschreitenden technischen Entwicklungen (z.B. Profiling) Schritt zu halten. Diese Änderungen beschränken sich auf das Notwendigste.

### **3.5 Fazit**

Die gesetzgeberischen Tätigkeiten und die Rechtsprechung auf europäischer Ebene wirken sich sowohl auf das Bundesrecht als auch auf kantonales Recht aus. In verschiedenen Bereichen liegt dabei die Rechtsetzungszuständigkeit beim Bund. Er hat die notwendigen Änderungen des DSG-Bund, das die Datenbearbeitungen durch Private und öffentliche Organe des Bundes regelt, und der bundesrechtlichen Spezialgesetzgebung (z.B. Migrationsrecht, Zivilrecht etc.) vorzunehmen. Bei der Bearbeitung von Personendaten durch kantonale und kommunale öffentliche Organe gelten die kantonalen Datenschutzbestimmungen. Im Kanton Zug steht die Anpassung des DSG, das die Bearbeitung von Personendaten durch kantonale und kommunale Organe regelt, aus. Insbesondere durch die Erweiterung des Anwendungsbereichs, die Einführung von neuen Begrifflichkeiten und der Erhöhung des Detaillierungsgrads der Bestimmungen im Datenschutz-Reformpaket der EU und des Europarats müssen Ergänzungen und Präzisierungen vorgenommen werden. Zudem sollen geringfügige Praxisanpassungen vorgenommen werden.

## **4. Umsetzung**

### **4.1 Bund**

Auf Bundesebene ist, wie erwähnt, zur schnellstmöglichen Einhaltung der Schengen-Anforderungen bislang insbesondere das umfangreiche SDSG erlassen worden. Die Referendumsfrist für das SDSG läuft am 17. Januar 2019 ab. Im nächsten Schritt wird das DSG-Bund totalrevidiert. Gleichzeitig mit diesen Gesetzgebungsarbeiten wird auch die EU-Datenschutzreform sowie die Modernisierung der Konvention SEV 108 des Europarats umgesetzt. In Zusammenhang mit der DSG-Bund Revision nimmt der Bund zudem in weiteren Erlassen Anpassungen des materiellen Datenschutzrechts vor (bspw. Regelungen des Zivilprozessrechts, des Strafrechts, des Strafprozessrechts etc.).

### **4.2 Kanton Zug**

Der unmittelbare Handlungsbedarf wurde eruiert und gestützt darauf wurde die vorliegende Erlassrevision ausgearbeitet. Nachdem sich die vorgesehenen Änderungen auf das Notwendigste beschränken, wird – wie in den meisten anderen Kantonen – eine Teilrevision vorgenommen, um die Kontinuität der Rechtsordnung möglichst weitgehend zu wahren. Dabei orientiert sich die Vorlage vornehmlich am Anpassungsbedarf, der sich aufgrund der EU-Datenschutzreform und den Änderungen der Konvention SEV 108 des Europarates ergibt. Im Übrigen werden geringfügige Praxisanpassungen vorgenommen.

Der Revisionsentwurf modernisiert die verwendete Terminologie, insbesondere, um die Vereinbarkeit mit dem europäischen Recht zu verbessern. So werden gewisse Begriffe aus dem europäischen Recht übernommen und beispielsweise das Register der Datensammlungen ersetzt durch ein Verzeichnis der verantwortlichen Organe über ihre Bearbeitungstätigkeiten. Der Begriff «Persönlichkeitsprofil», der eine schweizerische Besonderheit darstellt, wird neu durch den Begriff des «Profiling» abgelöst. Der Begriff «besonders schützenswerte Personendaten» wird um «biometrische Daten, die mittels technischer Verfahren die eindeutige Identifizierung einer natürlichen Person erlauben, sowie genetische Daten» erweitert.

Die generelle Ausnahme vom Geltungsbereich von hängigen Verfahren der Zivil- und Strafrechtspflege (inklusive Verfahren der internationalen Rechtshilfe) sowie Verfahren der Verwal-



tungsrechtspflege wird aufgehoben. Um Kollisionen zwischen den verfahrensrechtlichen und den datenschutzrechtlichen Informationsansprüchen der Parteien bzw. der betroffenen Personen zu vermeiden, wird ausdrücklich festgehalten, dass sich die Rechte und Ansprüche der betroffenen Personen während hängigen Verfahren nach dem anwendbaren Verfahrensrecht richten. Um die richterliche Unabhängigkeit zu gewährleisten, sind Datenbearbeitungen durch Justizbehörden im Rahmen ihrer justiziellen Tätigkeit von der Aufsicht der oder des Datenschutzbeauftragten ausgenommen.

Die Pflichten der verantwortlichen Organe werden präzisiert und stärker auf den Schutz der betroffenen Person ausgerichtet. So wird die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung neu ausdrücklich im Gesetz festgehalten. Zudem sollen sie mit technischen Vorkehrungen («privacy by design») und Voreinstellungen («privacy by default») für eine datenschutzfreundliche Ausgestaltung der Systeme sorgen. Diese Anforderungen werden ebenfalls in das DSG aufgenommen.

Die zwingenden Vorgaben des EU-Rechts verlangen zudem eine Stärkung der Kontrolle durch die Datenschutzstelle. Die Befugnisse der oder des Datenschutzbeauftragten werden künftig mit den Befugnissen der entsprechenden ausländischen Kontrollbehörden vergleichbar sein. Neu wird ihr oder ihm – anders als bisher mit dem Mechanismus des Aussprechens von Empfehlungen – unter anderem die Kompetenz zum Erlass von verbindlichen Verfügungen zugestanden. Anders als ihre Kolleginnen und Kollegen im europäischen Ausland soll sie oder er jedoch keine Verwaltungssanktionen aussprechen können. Auf die Einführung von neuen Strafbestimmungen auf kantonaler Ebene wird bewusst verzichtet.

## **5. Ergebnis der Vernehmlassung**

[Folgt, sobald durchgeführt].

## **6. Erläuterungen zum Gesetzesentwurf**

### **6.1 Ziffer I: Erläuterungen zu den einzelnen Bestimmungen**

#### **1. Titel: Allgemeine Bestimmungen**

##### **§ 1**

Die Zweckbestimmung entspricht dem geltenden Recht (§ 1 DSG). Die Bestimmung wird insoweit geändert, als dass der Geltungsbereich des Gesetzes nicht wie bislang Daten juristischer Personen miterfasst, sondern sich neu ausdrücklich auf den Schutz der Daten natürlicher Personen beschränkt (siehe nachfolgend § 2 Abs. 1 Bst. a).

##### **§ 2 Abs. 1 Bst. a**

Um Missverständnisse zu vermeiden, wird der Begriff «Personendaten» im Gesetz nicht mehr wie bislang generell durch den Begriff «Daten» ersetzt. Die bisherige Klammerbemerkung «(im Folgenden «Daten»）」 wird deshalb gestrichen. Wo nötig, soll vielmehr klar zwischen Personendaten und anderen Daten unterschieden werden (vgl. § 2 Abs. 1 Bst. b1). «Daten» sind dabei all diejenigen Informationen, die keinen Personenbezug aufweisen und nicht unter den Begriff der «Personendaten» fallen (Umkehrschluss). Unter «Daten» fallen bspw. reine Sachdaten (die Höchstgeschwindigkeit auf der Baarerstrasse beträgt 50 km/h, 1 kg Gold kostet 39 400 USD), Statistikdaten, anonymisierte Personendaten etc. Bei zusammengesetzten Wörtern sowie innerhalb desselben Absatzes wird im Gesetz der Begriff «Daten» verwendet, wenn eindeutig ist, dass damit Personendaten gemeint sind (bspw. § 10a Abs. 2 Bst. a DSG).

Die schweizerischen Datenschutzgesetze schützen bisher nicht nur natürliche, sondern auch juristische Personen, das Datenschutzgesetz des Kantons Zug zusätzlich die Personengesellschaften des Handelsrechts. Dies im Gegensatz zu den internationalen Vorgaben und zu den meisten europäischen Staaten. Der Entwurf zum DSG-Bund will die juristischen Personen neu ebenfalls vom Schutzbereich ausnehmen. Es erscheint nicht sinnvoll, eine vom Bund unterschiedliche kantonale Regelung beizubehalten. Für die juristischen Personen bzw. die Personengesellschaften nach dem Handelsrecht entsteht dadurch kein Nachteil; sind sie doch nach wie vor umfassend geschützt durch die Art. 28 ff. des Schweizerischen Zivilgesetzbuches vom 10. Dezember 1907 (ZGB; SR 210), das Bundesgesetz vom 9. Oktober 1922 über das Urheberrecht und verwandte Schutzrechte (URG; SR 231.1), das Bundesgesetz vom 19. Dezember 1986 gegen den unlauteren Wettbewerb (UWG; SR 241) oder durch die Bestimmungen zum Schutz von Berufs-, Geschäfts- und Fabrikationsgeheimnissen sowie Art. 13 der schweizerischen Bundesverfassung (BV; SR 101).

#### *§ 2 Abs. 1 Bst. b*

Der Begriff «besonders schützenswerte Personendaten» wird ausgeweitet auf biometrische Daten, die mittels technischer Verfahren die eindeutige Identifizierung einer natürlichen Person erlauben, sowie auf genetische Daten. Mit dieser Änderung werden die Anforderungen der SEV 108 (Art. 6 Abs. 1) sowie der Richtlinie (EU) 2016/680 (Art. 10) umgesetzt. Für die biometrischen Daten ist die Ergänzung «zur eindeutigen Identifizierung von natürlichen Personen mittels technischer Verfahren» notwendig, weil ansonsten auch etwa gewöhnliche Porträtfotografien, bei denen es sich eigentlich auch um «biometrische Daten» handelt, unter die besonders schützenswerten Personendaten fallen würden.

Der Begriff «Persönlichkeitsprofil» wird aufgehoben. Weder das europäische Recht noch andere ausländische Gesetzgebungen kennen diesen Begriff. Seit dem Inkrafttreten des DSG kam ihm keine grosse Bedeutung bei, und heute scheint er durch die Entwicklung neuer Technologien überholt. Er wird deshalb durch den als neue Begriffsdefinition aufzunehmenden Begriff «Profiling» abgelöst (siehe nachfolgend die Erläuterungen zu § 2 Abs. 1 Bst. b1).

#### *§ 2 Abs. 1 Bst. b1*

Die Richtlinie (EU) 2016/680 regelt neu das Profiling als besondere, persönlichkeitsgefährdende Art des Bearbeitens von Personendaten, das denselben Anforderungen genügen muss wie das Bearbeiten besonders schützenswerter Personendaten. Dies muss zwingend auch in die kantonalen Datenschutzgesetze übernommen werden. Zur einfacheren Verständlichkeit wird «Profiling» in die Begriffsdefinitionen aufgenommen. Bei den Voraussetzungen des Bearbeitens bzw. Bekanntgebens von Personendaten sind die entsprechenden Anpassungen vorzunehmen (vgl. dazu § 5 ff.).

Die Begriffsdefinition erfasst die, insbesondere automatisierte, Auswertung von Personendaten und anderen Daten und trägt damit der Tatsache Rechnung, dass es durch die technische Entwicklung (Big Data) vermehrt möglich wird, Daten ohne persönlichen Bezug so auszuwerten, dass schliesslich doch Personendaten vorliegen.

In den bereichsspezifischen Fachgesetzen sind diese Änderungen (Streichung des Begriffs Persönlichkeitsprofil und Einführung des Profilings) ebenfalls nachzuvollziehen (siehe dazu Fremdänderungen, Ziff. 6.2). Auf formell-gesetzlicher Stufe ist zudem zu umschreiben, zu welchem Zweck ein Profiling vorgenommen werden darf (§ 5 Abs. 2 i.V.m. § 4 Abs. 1 Bst. c).

### § 2 Abs. 1 Bst. c

Der Begriff «Bearbeiten» bleibt inhaltlich unverändert. Neu wird indes ausdrücklich erwähnt, dass es nicht darauf ankommt, welche Mittel und Verfahren beim Bearbeiten angewendet werden. Die Liste der beispielhaft erwähnten Bearbeitungsvorgänge wird einerseits mit dem Löschen von Personendaten und andererseits mit dem Durchführen logischer und / oder rechnerischer Operationen mit Personendaten ergänzt (vgl. Art. 2 Bst. b SEV 108).

Eine klarstellende Erläuterung gilt es zudem hinsichtlich des Vernichtens respektive des Löschens von Personendaten festzuhalten: Das Löschen von Personendaten geht weniger weit als das Vernichten. «Vernichten» impliziert, dass die Personendaten unwiederbringlich zerstört werden. Wenn die Daten auf Papier vorhanden sind, ist dieses zu verbrennen oder zu schreddern. Bei Papierdossiers kommt mit anderen Worten nur die Vernichtung in Frage. Schwieriger gestaltet sich die Datenvernichtung bei elektronischen Daten. Wurden die Daten mittels CD oder USB-Stick übermittelt, muss einerseits der Datenträger selber unbrauchbar gemacht (physisch vernichtet) werden und andererseits sind alle Kopien so zu behandeln, dass die Daten auch nicht mehr lesbar gemacht werden können. Bei Personendaten, die im Anhang einer E-Mail übermittelt wurden, müssen allfällige Zwischenspeicherungen dieser E-Mail vernichtet werden. Übliche Löschbefehle oder eine reine Umformatierung stellen keine Vernichtung, sondern lediglich eine Löschung dar. Eine Löschung kann unter Umständen ebenfalls ausreichen (bspw. mehrfaches Überschreiben einer Harddisk). In diesen Fällen ist keine zusätzliche physische Vernichtung notwendig. Zusammenfassend ist es im Zuge der Digitalisierung folgerichtig, neben dem bereits verwendeten Begriff der «Vernichtung» neu die «Löschung» gesetzlich zu nennen.

### § 2 Abs. 1 Bst. d

Die Begriffsdefinition «Bekanntgabe» wird vereinfacht und auf das Wesentliche reduziert. Darunter fallen sämtliche Vorgänge, bei denen Daten aktiv übermittelt oder passiv zugänglich gemacht werden, die es einem anderen Organ oder Privaten ermöglichen, vom Inhalt personenbezogener Informationen Kenntnis zu nehmen.

### § 2 Abs. 1 Bst. e

Die Begriffsdefinition «Datensammlung» wird aufgehoben. Der Begriff hat zunehmend an Schärfe verloren, da aufgrund der Suchfunktionen in elektronischen Dokumenten immer nach Daten einer bestimmten Person gesucht werden kann. Anstelle des Registers der Datensammlungen soll neu ein praxisbezogenes Verzeichnis der Bearbeitungstätigkeiten geführt werden (siehe hierzu die Erläuterungen zu § 12).

### § 2 Abs. 1 Bst. f

Da das Gesetz nur noch auf das Bearbeiten von Personendaten von natürlichen Personen anwendbar ist, sind die juristischen Personen und die Personengesellschaften des Handelsrechts hier ebenfalls zu streichen (siehe die Erläuterungen zu § 2 Abs. 1 Bst. a).

### § 2 Abs. 1 Bst. k

Die Definition «Dritte» wird aufgehoben. Die bisherige Begriffsdefinition gibt den effektiven Sinn und Zweck der Bestimmung nur ungenügend wieder. So gelten bei der bisherigen Formulierung auch andere Kantone und der Bund als «Dritte», was nicht in allen Fällen korrekt ist. Die Schwierigkeit einer Definition liegt darin, dass der Begriff «Dritte» verschieden verwendet wird und sich seine Bedeutung aus dem jeweiligen Kontext ergibt. Eine einheitliche Definition des Begriffs «Dritte» erscheint unter diesem Aspekt nicht möglich. Auch der Bund sowie weitere Kantone (LU, BS, BL, ZH) verwenden den Begriff «Dritte» in den jeweiligen Datenschutzgesetzen unterschiedlich, ohne ihn zu definieren.

Infolgedessen wird auch der Verweis in § 2 Abs. 5 Archivgesetz auf diese Definition im DSG aufgehoben (siehe Fremdänderungen, Ziff. 6.2).

#### § 3 Abs. 1

Der Begriff «Daten» wird durch «Personendaten» ersetzt (siehe Näheres hierzu in den Erläuterungen zu § 2 Abs. 1 Bst. a).

#### § 3 Abs. 2 Bst. a und Abs. 4

Gestützt auf Art. 2 Richtlinie (EU) 2016/680 sowie Art. 3 SEV 108 dürfen im innerstaatlichen Recht keine generellen Ausnahmen vom Geltungsbereich des DSG mehr vorgesehen werden, somit auch nicht für hängige Verfahren der Zivil- und Strafrechtspflege (inklusive Verfahren der internationalen Rechtshilfe) sowie Verfahren der Verwaltungsrechtspflege. § 3 Abs. 2 Bst. a DSG ist mit den internationalen Anforderungen nicht mehr vereinbar und wird deshalb aufgehoben. Um Kollisionen zwischen den verfahrensrechtlichen und datenschutzrechtlichen Informationsansprüchen der Parteien bzw. der betroffenen Personen zu vermeiden, wird neu ausdrücklich festgehalten, dass sich die Rechte und Ansprüche der betroffenen Personen während hängigen Verfahren nach dem anwendbaren Verfahrensrecht richten (Abs. 4). An der richterlichen Unabhängigkeit soll sich selbstverständlich nichts ändern. Aus diesem Grund werden Datenbearbeitungen durch Justizbehörden im Rahmen ihrer justiziellen Tätigkeit von der Aufsicht der oder des Datenschutzbeauftragten ausgenommen (siehe § 19 Abs. 1 Bst. a).

#### § 3 Abs. 2 Bst. c

Die Ausnahme der öffentlichen Register des Privatrechtsverkehrs vom Geltungsbereich der Datenschutzgesetzgebung ist mit den Anforderungen von Art. 3 SEV 108 nicht mehr vereinbar. Von der Aufhebung betroffen sind nur die öffentlichen Register des Privatrechtsverkehrs, die von kantonalen Behörden geführt werden (z.B. Grundbuch, Schiffsregister, Handelsregister, Betreibungs- und Konkursregister, öffentliches Register über die Eigentumsvorbehalte). Soweit die Erlasse, welche diese Register regeln, Bestimmungen bspw. zum Bearbeiten oder Bekanntgeben von Personendaten oder zu Einsichts- und Auskunftsrechten enthalten, gehen diese dem DSG als *lex specialis* vor. Dies wird – bereits heute – explizit in § 3 Abs. 3 DSG festgehalten. Art. 2 Abs. 4 des Entwurfs zum DSG-Bund sieht eine entsprechende Regelung für die öffentlichen Register des Privatrechtsverkehrs der Bundesbehörden vor.

## 2. Titel: Grundsätze beim Bearbeiten von Personendaten

#### § 4 (Titel)

Im Titel wird der Begriff «Anonymisierung» gestrichen, da Abs. 1 Bst. e aufgehoben bzw. durch die Paragraphen 5a und 5c ersetzt wird (vgl. die Erläuterungen zu § 4 Abs. 1 Bst. e).

#### § 4 Abs. 1

Der Begriff «Daten» wird durch «Personendaten» ersetzt (siehe Näheres hierzu in den Erläuterungen zu § 2 Abs. 1 Bst. a).

#### § 4 Abs. 1 Bst. e

Die Bestimmung über das Bearbeiten und Bekanntgeben von Personendaten zu nichtpersonenbezogenen Zwecken, wie Forschung, Planung und Statistik, wird aufgehoben. Sie wird neu ausführlicher in den Paragraphen 5a und 5c geregelt.

### § 5 (Titel)

Der Begriff «Daten» wird durch «Personendaten» ersetzt (siehe Näheres hierzu in den Erläuterungen zu § 2 Abs. 1 Bst. a).

### § 5

Die Voraussetzungen für das Bearbeiten von Personendaten in § 5 Abs. 1 Bst. a und b sowie von besonders schützenswerten Personendaten in Abs. 2 Bst. a und b gelten weiterhin unverändert. Die Formulierungen in den Buchstaben c der beiden Absätze werden einander angeglichen.

Es sei darauf hingewiesen, dass die in Abs. 1 Bst. c und Abs. 2 Bst. c erwähnten Voraussetzungen nur ausnahmsweise als Rechtfertigungsgründe für Datenbearbeitungen herangezogen werden können, da sie grundsätzlich zum Legalitätsprinzip in Widerspruch stehen. Müssen Organe Personendaten regelmässig oder dauerhaft erheben bzw. bearbeiten, ist dafür die notwendige – unmittelbare oder mittelbare – gesetzliche Grundlage zu schaffen und nicht etwa der Umweg über Einwilligungen oder allgemein zugänglich gemachte Daten zu wählen. Zudem gilt grundsätzlich: Soweit das Bearbeiten von Personendaten zur Erfüllung der öffentlichen Aufgabe eines Organs unentbehrlich ist (bzw. bei besonders schützenswerten Personendaten offensichtlich unentbehrlich), braucht ein Organ keine Einwilligung. Jedoch dürfen nach dem Verhältnismässigkeitsprinzip nur diejenigen Personendaten erhoben bzw. bearbeitet werden, die ein Organ zur Aufgabenerfüllung benötigt. Der Anwendungsbereich von § 5 Abs. 1 Bst. c und Abs. 2 Bst. c ist somit eingeschränkt und die Berufung darauf nur im Einzelfall möglich.

Der Einleitungssatz von § 5 Abs. 2 wird aufgrund der Einführung des Begriffs «Profiling» angepasst (siehe Näheres hierzu in den Erläuterungen zu § 2 Abs. 1 Bst. b1).

### § 5a

§ 4 Abs. 1 Bst. e DSGVO enthält in seiner geltenden Fassung eine kurze und knappe Regelung für das Bearbeiten von Personendaten zu einem nicht personenbezogenen Zweck. In der Praxis hat sich gezeigt, dass diese Bestimmung den Fragestellungen und Bedürfnissen rund um die Bearbeitung von Personendaten und insbesondere die Bekanntgabe von Personendaten an Dritte (bspw. zu Forschungszwecken), nicht zu genügen vermag. Zur besseren Strukturierung werden die Voraussetzungen für das Bearbeiten (§ 5a) und das Bekanntgeben (§ 5c) von Personendaten zu nicht personenbezogenen Zwecken im Erlassentext in zwei separate Paragraphen aufgeteilt.

§ 5a regelt das Bearbeiten von Personendaten zu einem nicht personenbezogenen Zweck durch dasjenige Organ, das die Daten bereits selbst – gestützt auf eine der Voraussetzungen in § 5 – für personenbezogene Zwecke bearbeiten darf. Erlaubt wird eine Zweckänderung, damit Erkenntnisse nicht mit Bezug auf die einzelne Person, sondern auf eine grössere Gesamtheit von Personen gewonnen werden können, etwa für Zwecke der Statistik, Forschung oder Planung. Auswertungen von Personendaten können zu statistischen oder planerischen Zwecken relevant sein (bspw. für die Information über die Behördentätigkeit oder für die Steuerung von finanziellen oder personellen Ressourcen eines Organs).

Die Zweckänderung wird zwar erleichtert, ist dafür aber an Auflagen bzw. Bedingungen geknüpft:

- Anonymisierung oder Pseudonymisierung, sobald es der Bearbeitungszweck zulässt (Bst. a): Anonymisierung bedeutet, dass der Personenbezug irreversibel so aufgehoben wird, dass ohne unverhältnismässigen Aufwand keine Rückschlüsse auf Personen mehr

möglich sind. Bei der Pseudonymisierung wird der Personenbezug ebenfalls aufgehoben, nur bleibt ein Schlüssel zur Re-Personifizierung erhalten.

- Keine Weitergabe (Bst. b): Organe dürfen «ihre» Personendaten, die sie selbst zu Statistik-, Planungs- oder Forschungszwecken zusammenstellen und auswerten, nicht an andere Organe oder Private weitergeben. Bei der Weitergabe handelt es sich mithin um eine spezifische Unterform der Bekanntgabe (gemäss § 2 Abs. 1 Bst. d).
- Bekanntgabe von Auswertungen nur anonymisiert (Bst. c): Spätestens bei der Bekanntgabe, insbesondere bei der Veröffentlichung, ist jeglicher Personenbezug zu entfernen. Im Zeitalter von Big Data ist hier besondere Vorsicht geboten. Wenn mit einer Re-Identifizierung / -Personifizierung gerechnet werden muss, ist auf eine Publikation zu verzichten.

### § 5b

Das Bekanntgeben von Personendaten bzw. von besonders schützenswerten Personendaten ist eine spezielle Form der Datenbearbeitung (siehe § 2 Bst. c und d). Dabei verlassen die Personendaten den Bereich eines Organs, und allenfalls findet auch eine Zweckänderung statt. Entsprechend rechtfertigt sich eine Regelung in einem separaten Paragraphen. Gemäss Bst. a gelten dabei die gleichen Voraussetzungen wie für das Bearbeiten von Personendaten (§ 5 Abs. 1) bzw. von besonders schützenswerten Personendaten und Profilings (§ 5 Abs. 2).

Die gesetzlichen Grundlagen können eine Datenbekanntgabe auf der Seite des datenbesitzenden Organs in Form einer Verpflichtung oder Ermächtigung vorsehen. Eine Datenbekanntgabe kann aber auch als Anspruch eines Organs, Daten zu erhalten, formuliert sein. Beispiele für gesetzliche Bestimmungen zur Datenbekanntgabe sind etwa Amtshilfebestimmungen, die sich in zahlreichen Fachgesetzen finden. Sie beschränken sich in aller Regel auf eine Datenbekanntgabe im Einzelfall auf begründete Anfrage hin. Auch eine Datenbekanntgabe kann ausnahmsweise – d.h. ohne das Vorliegen einer gesetzlichen Grundlage – im Einzelfall zulässig sein, wenn die betroffene Person ausdrücklich mit der Bekanntgabe ihrer Daten einverstanden ist oder ihre Personendaten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt hat.

Bst. b nennt die Voraussetzungen, unter denen Personendaten gestützt auf eine mutmassliche Einwilligung bekannt gegeben werden dürfen. Von der Konstellation her kann auch hier davon ausgegangen werden, dass es sich immer um Einzelfälle in Ausnahmesituationen handelt (z.B. Bekanntgabe von Medikamentenunverträglichkeiten bei notfallmässigen Einlieferungen in ein auswärtiges Spital).

### § 5c

§ 5c regelt neu die Voraussetzungen und Bedingungen für die Bekanntgabe von Personendaten zu nicht personenbezogenen Zwecken. Die Bestimmung kommt grundsätzlich nur dann zur Anwendung, wenn eine Empfängerin oder ein Empfänger tatsächlich Personendaten benötigt. Ist ein Projekt bereits mit anonymisierten Daten realisierbar, dürfen keine Personendaten bekanntgegeben werden, da die Datenbekanntgabe nicht nötig und somit nicht verhältnismässig wäre (vgl. § 4 Abs. 1 Bst. d DSG).

Auch die Datenbekanntgabe zu nicht personenbezogenen Zwecken ist an Voraussetzungen und Bedingungen geknüpft. Das angefragte Organ muss vorab bei jeder Anfrage zwingend prüfen, ob gesetzliche Bestimmungen bestehen, die eine besondere Geheimhaltungspflicht statuieren, und inwieweit damit auch eine Bekanntgabe der Personendaten zum Bearbeiten für einen nicht personenbezogenen Zweck verboten ist (Abs. 1). Die Datenbekanntgabe an andere kantonale oder gemeindliche Organe (zum Organbegriff siehe § 2 Abs. 1 Bst. i DSG) und an

Organe anderer Kantone oder an Bundesorgane (Abs. 1 Bst. a) ist zu denselben nicht personenbezogenen Zwecken zulässig wie die Bearbeitung nach § 5a Abs. 1. An Privatpersonen (natürliche oder juristische Personen) dürfen Personendaten ausschliesslich für die Bearbeitung zu Forschungszwecken bekanntgegeben werden (Abs. 1 Bst. b). Mit der Aufnahme dieser Bestimmung berücksichtigt das DSG den verfassungsrechtlichen Anspruch auf Wissenschaftsfreiheit (Art. 20 BV).

Damit ein Organ beurteilen kann, ob eine Bekanntgabe von Personendaten nach § 5c möglich ist, muss die Anfrage mindestens Informationen zu den verlangten Daten, zum geplanten (nicht personenbezogenen) Bearbeitungszweck und zum Ablauf der Datenbearbeitung enthalten. Die Empfängerin oder der Empfänger hat sich bei Bewilligung der Datenbekanntgabe schriftlich dazu zu verpflichten, die Personendaten zu anonymisieren oder zu pseudonymisieren, sobald es der Bearbeitungszweck zulässt, und die Auswertungen nur so bekannt zu geben, dass keine Rückschlüsse auf betroffene Personen möglich sind (Abs. 2). Privatpersonen haben sich zusätzlich ausdrücklich dazu zu verpflichten, die Personendaten nicht zu anderen Zwecken zu bearbeiten, die Personendaten nicht weiterzugeben und mit organisatorischen und technischen Massnahmen für die Informationssicherheit zu sorgen (Abs. 3). Welche Massnahmen dies sind, hat die Empfängerin oder der Empfänger darzulegen. Für die in Abs. 1 Bst. a erwähnten öffentlichen Organe ergeben sich diese Zusatzverpflichtungen bereits aus den für sie geltenden Datenschutzgesetzen: Die Zweckbindung ist für Organe der Zuger Verwaltung oder der Zuger Gemeinden in § 4 Abs. 1 Bst. c DSG niedergelegt, das Verbot der Weitergabe bzw. der Bekanntgabe (ohne gesetzliche Grundlage) findet sich in § 5b und die Pflicht, für die Informationssicherheit zu sorgen, folgt aus § 7 DSG. Bei Verletzung der Verpflichtungen gemäss Abs. 2 und Abs. 3 stehen der betroffenen Person gegenüber Organen Ansprüche aus widerrechtlicher Bearbeitung gemäss § 15 f. DSG sowie gegenüber privaten Empfängerinnen und Empfängern zivilrechtliche Ansprüche zu. Neu kann die vorsätzliche Verletzung der (in den Vereinbarungen enthaltenen) Verpflichtungen gestützt auf § 24 DSG auch mit Busse geahndet werden (vgl. hierzu § 24 Abs. 2).

Abweichende Bestimmungen in Spezialgesetzen gehen § 5c DSG vor (z.B. Bundesgesetz vom 30. September 2011 über die Forschung am Menschen [Humanforschungsgesetz, HFG; SR 810.30] oder Bundesstatistikgesetz vom 9. Oktober 1992 [BStatG; SR 431.01]).

#### § 5d

Die geltende Fassung des DSG enthält lediglich in § 25, der das Verfahren bei Haftungsansprüchen regelt, Hinweise zur Verantwortung der Organe. Die Praxis hat in der Vergangenheit gezeigt, dass das Bewusstsein um die Verantwortung für das Bearbeiten von Personendaten bei den Organen oft ungenügend ausgeprägt ist.

Sowohl die SEV 108 als auch die Richtlinie (EU) 2016/680 betonen die Wichtigkeit einer klaren Zuordnung der Verantwortung für das Bearbeiten von Personendaten. Das gilt insbesondere bei gemeinsamen Datenbearbeitungen, wo die Verantwortlichkeiten transparent zu regeln sind (§ 5d Abs. 2). Gemäss § 5d Abs. 1 trägt das Organ, das über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet, die Verantwortung für den Umgang mit den Personendaten. Dabei ist zu berücksichtigen, dass es sich bei «Privaten» ebenfalls um «Organe» handeln kann, soweit ihnen öffentliche Aufgaben übertragen werden (siehe Organbegriff in § 2 Abs. 1 Bst. i DSG). In dem Fall haben sie die Verantwortung selbst zu tragen. Handeln Private lediglich im Auftrag eines Organs im Sinne einer Auftragsdatenbearbeitung gemäss § 6, dann bleibt das auftraggebende Organ für die Einhaltung des Datenschutzes selbst verantwortlich – auch für die Einhaltung des Datenschutzes durch den beauftragten Privaten. Das auftraggebende Organ kann seine datenschutzrechtliche Verantwortung nicht an den Auftragnehmer delegieren

(siehe § 25 DSG). Die Frage eines allfälligen Rückgriffs auf einen beauftragten Privaten ist aufgrund des Verhältnisses zwischen dem Organ und dem beauftragten Privaten zu prüfen. Aus der Verantwortung entspringen primär Handlungspflichten und sekundär – im Verletzungsfall – Haftungsansprüche.

Art. 4 Abs. 4 der Richtlinie (EU) 2016/680 und Art. 10 Abs. 1 der SEV 108 verlangen, dass die Organe die Einhaltung der Datenschutzbestimmungen nachweisen können müssen. Eine entsprechende Bestimmung ist deshalb auch ins DSG aufzunehmen (§ 5d Abs. 3). Es ergeben sich daraus keine neuen Pflichten für die verantwortlichen Organe. Sie mussten schon bisher die Einhaltung der Datenschutzbestimmungen belegen können. Gemeint sind damit nicht etwa nur der Nachweis der Informationssicherheit, sondern auch der Rechtmässigkeit, der Verhältnismässigkeit oder der Zweckbindung. Zur Erbringung dieses Nachweises stehen verschiedene Hilfsmittel zur Verfügung wie etwa der Eintrag im Verzeichnis der Bearbeitungstätigkeiten (§ 12 DSG), der Massnahmenkatalog nach § 4 Abs. 3 der Datensicherheitsverordnung vom 16. Januar 2007 (DSV; BGS 157.12) inkl. Informationssicherheits- und Zugriffskonzepte, die Bewilligungen gemäss der Verordnung über das Bewilligungsverfahren für den elektronischen Datenaustausch vom 24. Juni 2008 (Online-Verordnung; BGS 157.22) sowie die Datenschutz-Folgenabschätzung gemäss § 7b.

#### § 6 (Titel)

Der Titel ist veraltet und wird deshalb neu in «Auftragsdatenbearbeitung» geändert.

#### § 6 Abs. 1

Der Text wird entsprechend der Titeländerung angepasst. Inhaltlich ergeben sich dadurch keine Änderungen. Weiterhin kann das Bearbeiten von Personendaten Dritten übertragen werden. Sofern die Auftragsdatenbearbeitung im Ausland erfolgt, stellt sich die Frage des anwendbaren Rechts. Dabei gilt grundsätzlich das Territorialitätsprinzip, wonach das Recht desjenigen Ortes zur Anwendung gelangt, an dem die Personendaten bearbeitet werden. Somit kommt in diesen Fällen für den/die Auftragsdatenbearbeiter/in das ausländische Recht (vor Ort) zur Anwendung. Das Organ bleibt seinerseits für die Einhaltung der Informationssicherheit nach DSG (durch den/die Auftragsdatenbearbeiter/in) verantwortlich, was es mittels Auflagen, Vereinbarungen oder auf andere Weise sicherstellen muss (vgl. § 6 Abs. 2).

#### § 6 Abs. 1 Bst. a und Abs. 2

Zum besseren Verständnis wird die Bestimmung adressatengerechter formuliert. Das Gewicht soll zudem klarer auf die Funktion und die Verantwortung des Organs gelegt werden, welches sich für eine Auftragsdatenbearbeitung entscheidet.

In Abs. 2 wird zudem ausdrücklich festgehalten, dass das Organ sicherstellen muss, dass der Auftragsdatenbearbeitende die Informationssicherheit gewährleistet und die Rechte der betroffenen Person wahrt. Diese Anpassung erfolgt in Umsetzung von Art. 22 Abs. 1 Richtlinie (EU) 2016/680. Der Begriff «Informationssicherheit» wird neu auch in § 7 verwendet und präzisiert.

#### § 6 Abs. 3

Es wird nun klar festgehalten, dass die Verantwortung das Organ nicht nur trifft, wenn es Personendaten selbst bearbeitet, sondern auch, wenn es durch einen Dritten Personendaten bearbeiten lässt. Diese Verantwortung kann nicht delegiert werden. Auch hier zeigte die Erfahrung in der Vergangenheit, dass sich die Organe dieser Verantwortung zu wenig bewusst sind (vgl. Erläuterungen zu § 5d).



#### § 6 Abs. 4

Mit der Aufnahme der Pflicht zur vorgängigen Einholung der Zustimmung werden die Vorgaben von Art. 22 Abs. 2 Richtlinie (EU) 2016/680 umgesetzt.

#### § 6a

In Art. 6a Abs. 1 wird neu der Grundsatz der Informationspflicht bei der Beschaffung von Personendaten festgehalten. Die Informationspflicht soll die Transparenz bei der Datenbearbeitung – eines der Kernanliegen des Datenschutzrechts – verbessern, indem das Organ die betroffene Person über die Beschaffung von Personendaten zu informieren hat. § 4 Abs. 1 Bst. b verlangt zwar, dass Personendaten grundsätzlich bei der betroffenen Person zu erheben sind, womit die Datenbearbeitung für diese auch erkennbar wird. Werden Personendaten indessen bei Dritten erhoben, kann die betroffene Person ohne Information regelmässig gar nicht erkennen, dass Personendaten über sie bearbeitet werden. Eine betroffene Person kann ihre Rechte ausserdem nur wahrnehmen, wenn ihr die Datenbearbeitung und deren Umstände bekannt sind.

Abs. 2 enthält den Katalog derjenigen Informationen, die mindestens anzugeben sind (Identität und Kontaktdaten des Organs, bearbeitete Personendaten und Zweck der Bearbeitung). Bei Datenbekanntgaben an andere Organe oder an Privatpersonen müssen auch die Empfängerinnen oder Empfänger angegeben werden (Abs. 3).

Abs. 4 bestimmt den Zeitpunkt, in welchem die betroffene Person informiert werden muss, wenn die Personendaten bei Dritten beschafft werden, nämlich spätestens bei der Speicherung der Personendaten.

#### § 6b

§ 6b regelt Ausnahmen von der Informationspflicht (Abs. 1) und Einschränkungen bei der Übermittlung von Informationen (Abs. 2).

Die Informationspflicht entfällt, wenn die betroffene Person bereits über die Informationen nach § 6a Abs. 2 bis 4 verfügt, etwa wenn sie bereits zu einem früheren Zeitpunkt informiert wurde und sich die Informationen in der Zwischenzeit nicht geändert haben (Abs. 1 Bst. a). Sie entfällt auch, wenn die Bearbeitung der Personendaten in einer gesetzlichen Grundlage ausdrücklich vorgesehen ist, d.h. wenn aus den gesetzlichen Grundlagen hinreichend klar hervorgeht, welche Daten über die betroffene Person zu welchem Zweck durch wen bearbeitet werden (Abs. 1 Bst. b). Die Information entfällt schliesslich auch, wenn sie nicht oder nur mit unverhältnismässigem Aufwand möglich ist (Abs. 1 Bst. c). Nicht möglich ist eine Information bspw. dann, wenn eine betroffene Person gar nicht identifiziert werden kann (Foto eines Unbekannten). Unverhältnismässig ist der Aufwand, wenn er im Verhältnis zum Informationszugewinn der betroffenen Personen sachlich nicht gerechtfertigt erscheint (z.B. weil eine sehr grosse Anzahl Personen betroffen ist). Letzteres könnte insbesondere bei Verarbeitungen für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken der Fall sein. Als Anhaltspunkte sollten dabei die Zahl der betroffenen Personen, das Alter der Daten oder etwaige geeignete Garantien in Betracht gezogen werden (vgl. Erwägungsgrund 62 der Datenschutz-Grundverordnung). Ein Organ darf sich nicht mit der Vermutung begnügen, dass die Information unmöglich oder nur mit unverhältnismässigem Aufwand zu bewerkstelligen ist. Das Organ muss grundsätzlich sämtliche Vorkehrungen treffen, die unter den konkreten Umständen von ihm erwartet werden können, um der Informationspflicht nachzukommen. Erst wenn diese erfolglos bleiben, darf es davon ausgehen, dass die Information unmöglich bzw. nur mit unverhältnismässigem Aufwand möglich ist.

Die Information kann ausserdem unter den gleichen Voraussetzungen und in gleichem Mass eingeschränkt werden wie die Auskunft über die eigenen Personendaten gemäss § 14 (ganz oder teilweise einschränken, mit Auflagen versehen oder aufschieben).

#### § 7 (Titel)

Im Titel wird der veraltete Begriff «Datensicherung» durch den geläufigen Begriff «Informationssicherheit» ersetzt. Die Informationssicherheit ist ein wesentliches Element, den Datenschutz zu gewährleisten. Die Begriffsanpassung führt dazu, dass auch die Terminologie in der DSV angepasst werden muss (siehe Inkrafttreten, Ziff 6.4).

#### § 7 Abs. 1

Der Begriff «Daten» wird durch «Personendaten» ersetzt (siehe Näheres hierzu in den Erläuterungen zu § 2 Abs. 1 Bst. a).

Zudem ist der Begriff «Sicherung» an den Titel anzupassen und durch «Sicherheit» zu ersetzen. Detailliertere Angaben dazu, wie die Informationssicherheit umzusetzen ist, finden sich in der DSV auf Verordnungsstufe (vgl. § 7 Abs. 2 DSG). Die Organe sind verpflichtet, die erforderlichen Sicherheitsmassnahmen zu ergreifen (§ 4 Abs. 1 DSV); siehe auch die Erläuterungen zur Datenschutz-Folgenabschätzung gemäss § 7b.

#### § 7a

Neu wird in § 7a die Pflicht zum Datenschutz durch Technik («privacy by design») sowie durch benutzerfreundliche Voreinstellungen («privacy by default») eingeführt, welche die SEV 108 (Art. 10 Abs. 3) sowie die Richtlinie (EU) 2016/680 (Art. 20 Abs. 1 und Abs. 2) vorsehen.

Abs. 1 verlangt vom Organ, ab dem Zeitpunkt der Planung eine Datenbearbeitung so auszugestalten, dass durch die getroffenen Vorkehren die Datenschutzvorschriften umgesetzt werden. Damit wird neu die Pflicht zum sogenannten «Datenschutz durch Technik» («privacy by Design») eingeführt. Die gesetzlichen Anforderungen für eine datenschutzkonforme Bearbeitung sollen bereits so im System verwirklicht werden, dass dieses die Gefahr von Verstössen gegen Datenschutzvorschriften reduziert oder ausschliesst. So kann bspw. dafür gesorgt werden, dass Daten in regelmässigen Abständen gelöscht oder standardmässig anonymisiert werden. Besonders bedeutsam ist dabei die sogenannte Datenminimierung, wonach eine Datenbearbeitung bereits von Beginn weg so angelegt ist, dass möglichst wenige Daten anfallen und bearbeitet werden oder dass Daten zumindest nur möglichst kurze Zeit aufbewahrt werden.

Abs. 2 präzisiert die Anforderungen an die Vorkehren nach Abs. 1. Die Norm bringt den risikobasierten Ansatz zum Ausdruck. Das Risiko, das mit einer Bearbeitung einhergeht, muss in Beziehung gesetzt werden zu den technischen Möglichkeiten, um dieses zu verringern. Je höher das Risiko, je grösser die Eintrittswahrscheinlichkeit und je umfangreicher die Datenbearbeitung ist, umso höher sind die Anforderungen an die technischen Vorkehren, damit sie im Sinne der vorliegenden Bestimmung als angemessen gelten können.

Abs. 3 führt neu die Pflicht zur Verwendung datenschutzfreundlicher Voreinstellungen («privacy by default») ein. Bei Voreinstellungen handelt es sich um jene Einstellungen, insbesondere von Software, die standardmässig zur Anwendung kommen, d.h. falls keine abweichende Eingabe durch den Nutzer erfolgt. Im Zusammenhang mit einer Datenbearbeitung bedeutet dies, dass der fragliche Bearbeitungsvorgang standardmässig möglichst datenschutzfreundlich eingerichtet ist, ausser die betroffene Person würde diese vorgegebenen Einstellungen verändern.

### § 7b

Neu wird in § 7b die Pflicht des verantwortlichen Organs zur Durchführung einer Datenschutz-Folgenabschätzung ausdrücklich im Gesetz festgehalten. Damit werden die europäischen Vorgaben von Art. 27 Richtlinie (EU) 2016/680 und Art. 10 Abs. 2 SEV 108 umgesetzt. Eine solche Abschätzung ist jedoch nicht bei jedem Verwaltungshandeln bzw. jeder Personendatenbearbeitung erforderlich. Vielmehr betrifft diese Pflicht Datenbearbeitungen von einer grösseren Anzahl von betroffenen Personen, wie sie primär in IT- und Digitalisierungsprojekten vorkommen. Dies ergibt sich bereits heute aus § 19a Abs. 1 DSG, weshalb der Wortlaut dieser Bestimmung zur Präzisierung in § 7b Abs. 1 übernommen wird. Für eine möglichst speditive Durchführung der Datenschutz-Folgenabschätzung wird die Datenschutzstelle eine Checkliste zur Verfügung stellen.

Die Datenschutz-Folgenabschätzung ist somit keine Neuheit: Schon heute sind die Organe verpflichtet, zum Schutz von Personendaten Sicherheitsmassnahmen festzulegen (§ 4 DSV) und Datenbearbeitungen, die mit besonderen Risiken für die Grundrechte der betroffenen Personen verbunden sind, der Datenschutzstelle vorgängig zur Stellungnahme vorzulegen (§ 19a DSG, sog. «Vorabkontrolle»). Die Datenschutz-Folgenabschätzung unterstützt die Organe dabei, die bestehenden Risiken vorgängig zu erkennen und zu bewerten. Auch hilft sie den Organen bei der Entscheidung, mit welchen technischen und organisatorischen Massnahmen sie die Risiken präventiv angehen können – was letztlich auch dazu beiträgt, Kosten zu sparen. Gleichzeitig dient das Ergebnis der Datenschutz-Folgenabschätzung dem verantwortlichen Organ auch dazu, den Nachweis über die Einhaltung der Datenschutzbestimmungen zu erbringen (siehe hierzu § 5d Abs. 3).

Abs. 2 umschreibt den Mindestinhalt, den eine Datenschutz-Folgenabschätzung zwingend enthalten muss. Der Gesetzestext folgt bei der Aufzählung des Mindestinhalts einem logischen Ablauf: Einer Vorbereitungsphase (Bst. a), einer Bewertungsphase (Bst. b) und einer Massnahmenphase (Bst. c). In der Vorbereitungsphase sind nicht nur die geplanten Bearbeitungsvorgänge (inkl. die verwendeten Technologien) zu umschreiben, sondern auch der Umfang und Zweck der Bearbeitung sowie die Aufbewahrungsdauer. In der Bewertungsphase müssen die verantwortlichen Organe eine Prognose darüber machen, welche Folgen eine geplante Datenbearbeitung für die betroffenen Personen hat. Massgebend ist dabei insbesondere, auf welche Weise und in welchem Umfang sich eine Bearbeitung auf die Grundrechte der Betroffenen auswirkt. Zu berücksichtigen sind etwa die Art der Personendaten (z.B. besonders schützenswerte Personendaten), die Datenbearbeitungsart (z.B. Profiling), der Zweck der Datenbearbeitung, die Menge der bearbeiteten Daten, eine Übermittlung in Drittstaaten oder der Kreis der Zugriffsberechtigten. In der Massnahmenphase ist darzulegen, mit welchen Massnahmen diese Risiken reduziert werden.

Abs. 3 verpflichtet die Organe, der Datenschutzstelle Vorhaben zur Bearbeitung von Personendaten, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Personendaten zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen, vorgängig zur Stellungnahme vorzulegen (siehe dazu auch § 19a «Vorabkonsultation»). Neue Pflichten werden den Organen damit nicht auferlegt, da sie bereits nach geltendem Recht bei bestimmten Vorhaben zur Vorabkonsultation der Datenschutzstelle verpflichtet sind (§ 19a DSG). Aus systematischen Gründen wird diese Pflicht neu in § 7b festgehalten. Damit kommt klar zum Ausdruck, dass Datenschutz-Folgenabschätzung und Vorabkonsultation thematisch zusammenhängen. Beide wirken präventiv und steigern die Effizienz bei der Umsetzung von Datenschutzvorhaben.

### § 7c

Verletzungen des Datenschutzes sind neu unverzüglich der Datenschutzstelle zu melden. Die Meldung kann ausbleiben, wenn die Verletzung voraussichtlich zu keinem Risiko für die Grundrechte der betroffenen Personen führt. Damit soll vermieden werden, dass Bagatellfälle gemeldet werden müssen oder Verletzungen, die ohne Risiken für die betroffenen Personen hinreichend eingedämmt oder beseitigt werden könnten (bspw. mit Backups bei Datenverlust). Mit der Meldepflicht werden die Anforderungen von Art. 30 Richtlinie (EU) 2016/680 und Art. 7 Abs. 2 SEV 108 umgesetzt.

Abs. 2 definiert, wann eine Datenschutzverletzung vorliegt. Wie aus der Aufzählung in Bst. a bis c hervorgeht, geht es nicht um eigentliche Rechtsverletzungen, sondern um unbefugte Zugriffe, Offenbarungen oder Datenverluste aufgrund von Brüchen der technischen und organisatorischen Massnahmen zur Wahrung der Informationssicherheit (z.B. Hackerangriffe; unzureichende oder fehlende Verschlüsselung). Dabei ist unerheblich, ob die Verletzung durch Dritte erfolgt oder intern durch eigene Mitarbeitende verursacht wird (z.B. durch unsachgemässe Entsorgung von Dokumenten). Ebenso unerheblich ist, ob die Beteiligten diese Folgen herbeiführen wollten oder nicht, oder ob sie rein zufällig eingetreten sind. Selbstverständlich muss dem verantwortlichen Organ die Datenschutzverletzung für die Meldepflicht aber bekannt sein. An den Inhalt der Meldung sind keine allzu hohen Forderungen zu stellen. Enthalten sein sollten mindestens:

- die Beschreibung der Art und des Umfangs der Verletzung und der wahrscheinlichsten Folgen daraus; sowie
- die Beschreibung der bereits ergriffenen und vorgesehenen Massnahmen zur Wiederherstellung des Schutzes bzw. zur Abmilderung der Folgen der Verletzung.

Bei Auftragsdatenbearbeitungen (§ 6) muss der Auftragnehmer das verantwortliche Organ unverzüglich über eine Datenschutzverletzung informieren (Abs. 3). Gegenüber der Datenschutzstelle hat er keine Meldepflicht. Es ist Aufgabe des Organs, darüber zu entscheiden, inwieweit eine Meldung auch an die Datenschutzstelle gemäss Abs. 1 zu erfolgen hat. Ebenso ist es Sache des Organs, die betroffenen Personen über eine Verletzung des Datenschutzes zu informieren, wenn die Umstände dies erfordern (Abs. 4).

### § 7d

Die weiteren Informationspflichten in § 7d ergänzen verschiedene Datenschutzregeln für den Fall, dass Personendaten an andere Behörden oder Private weitergegeben wurden. Sie setzen die Anforderungen von Art. 19 Richtlinie (EU) 2016/680 um. Personendaten sollen von den Empfängerinnen oder Empfängern nicht in Unkenntnis der entsprechenden Vorgänge weiterbearbeitet werden. Das Organ kann nur dann von der Informationspflicht absehen, wenn die Mitteilung nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

### § 8 (aufgehoben)

Die Regelung von Datenbekanntgaben aus den gemeindlichen Einwohnerregistern im DSG ist systemfremd, da es sich hier bereits um «materielles» Datenschutzrecht handelt. § 8 wird deshalb in das Gemeindegesetz verschoben (siehe Fremdänderungen, Ziff. 6.2).

### § 9 Abs. 1

Der Wortlaut der geltenden Fassung ist unklar und führt immer wieder zu Falschinterpretationen und folglich zu Beanstandungen bei der Datenschutzstelle. Die Neuformulierung trägt zum besseren Verständnis bzw. zur besseren Lesbarkeit bei. Sie stellt klar, dass eine Datensperre

ausschliesslich die Bekanntgabe von Personendaten an Private (und nicht an Organe) betrifft. Inhaltlich ändert sich indes nichts an dieser Bestimmung.

#### § 9 Abs. 1a

Um das Sperrecht geltend machen zu können, muss die betroffene Person erst einmal davon Kenntnis haben. In der Praxis ist dies heute nicht immer der Fall. Aus diesem Grund sollen die Organe neu verpflichtet werden, die Betroffenen in geeigneter Weise auf das Sperrecht aufmerksam zu machen. Dies kann etwa durch einen schriftlichen Hinweis auf Formularen geschehen, mit welchen das Organ Daten erhebt, durch einen Hinweis auf der Website des Organs bei Onlineerfassungen oder durch einen Hinweis in Publikationen, welche über die Datenerhebung informieren. Ebenso kann mündlich auf das Sperrecht aufmerksam gemacht werden, wenn Personen sich an einem Schalter zu melden haben, wie es bei gewissen Einwohnerkontrollen oder dem Strassenverkehrsamt bereits heute gelebte Praxis ist.

#### § 9 Abs. 2

Der Wortlaut des 2. Satzes wird aufgrund des Wegfalls des Begriffs «Datensammlung» angepasst. Die meisten kantonalen Datenschutzgesetze verwenden ebenfalls diese Terminologie (neu: «Datenbestände eines Organs»).

#### § 9 Abs. 3 Bst. b

Inhaltlich ändert sich nichts an dieser Bestimmung. Der Begriff «Dritte» wird durch «Private» ersetzt, um zu verdeutlichen, dass die Datensperre eben nur gegenüber Privaten (und nicht gegenüber Organen) gilt (siehe hierzu auch die Erläuterungen zu § 9 Abs. 1). Zudem wird klar gestellt, dass zur Durchbrechung der Datensperre ein eigentlicher Rechtsanspruch vorliegen muss wie bspw. ein Nachweis über ausstehende Mietschulden, ausstehende Unterhaltszahlungen oder sonstige Geldforderungen. Die meisten kantonalen Datenschutzgesetze verwenden ebenfalls diese Terminologie.

#### § 10 Abs. 1

Der Begriff «Daten» wird durch «Personendaten» ersetzt (siehe Näheres hierzu in den Erläuterungen zu § 2 Abs. 1 Bst. a). Zudem wurde die doppelte Verneinung aufgehoben, da sie inhaltlich nicht korrekt war und nur für sprachliche Verwirrung sorgte.

#### § 10a Abs. 1 und 2

Der Begriff «Daten» wird durch «Personendaten» ersetzt (siehe Näheres hierzu in den Erläuterungen zu § 2 Abs. 1 Bst. a).

Hinsichtlich der Personendatenbekanntgabe ins Ausland ist zu berücksichtigen, dass die Veröffentlichung von Personendaten im Internet zwecks Information der Öffentlichkeit, wie bspw. im Falle der Medien, praxisgemäss keine Bekanntgabe von Personendaten ins Ausland darstellt, auch wenn die Daten vom Ausland aus zugänglich sind (vgl. auch Art. 15 Entwurf DSG-Bund).

#### § 11

Der Begriff «Daten» wird im Titel und in Abs. 1 durch «Personendaten» ersetzt (siehe Näheres hierzu in den Erläuterungen zu § 2 Abs. 1 Bst. a). Die in § 11 genannte Verpflichtung der Organe zur Anonymisierung oder Vernichtung von Personendaten, sobald sie diese nicht mehr benötigen, ergibt sich bereits aus dem allgemeinen Verhältnismässigkeitsgrundsatz. § 11 konkretisiert den Verhältnismässigkeitsgrundsatz in zeitlicher Hinsicht. Die Beachtung dieses Grundsatzes ist Voraussetzung für eine Personendatenbearbeitung (vgl. § 4 Abs. 1 Bst. d).

### 3. Titel: Kontrollrechte der betroffenen Personen

#### § 12 (Titel)

Der Titel wurde dem geänderten Inhalt dieser Bestimmung, analog zu Art. 11 Entwurf DSG–Bund angepasst.

#### § 12 Abs. 1

Auf eine Weiterführung des Begriffs «Datensammlung» wird künftig verzichtet (siehe dazu die Erläuterungen zu § 2 Abs. 1 Bst. e). Anstelle des Registers der Datensammlungen soll neu ein Verzeichnis der Bearbeitungstätigkeiten aller Organe geführt werden. Das Verzeichnis ist zu veröffentlichen. Damit wird der Grundsatz der Transparenz einer Datenbearbeitung für die betroffenen Personen aufrechterhalten. Für die Justiz- und Polizeibehörden ergibt sich die Pflicht zur Führung und Veröffentlichung eines solchen Verzeichnisses unmittelbar aus Art. 24 Richtlinie (EU) 2016/680. Der Kanton stellt den kantonalen und gemeindlichen Organen ein zentrales Erfassungs- und Publikationssystem zur Verfügung (siehe dazu finanzielle Auswirkungen auf den Kanton, Ziff. 7.1). Die Führung und Veröffentlichung des Verzeichnisses obliegt neu den kantonalen und gemeindlichen Organen und nicht mehr der Datenschutzstelle. Dabei dürfte sich der Initialaufwand in Grenzen halten, da die heutigen Registereinträge als Grundlage dienen können, der Inhalt des Verzeichnisses im Vergleich zum heutigen Register der Datensammlungen wesentlich beschränkt und der Kanton ein zentrales Erfassungs- und Publikationssystem zur Verfügung stellen wird. Im Verzeichnis sind nicht etwa die einzelnen Datenbearbeitungsschritte aufzuführen, sondern nur Datenbearbeitungs- bzw. Geschäftsprozesse (z.B. «Fallbearbeitung Prämienverbilligung»).

#### § 12 Abs. 2

In der Praxis hat dieser Absatz immer wieder zu Auslegungsfragen geführt. Da der Begriff «Datensammlungen» gestrichen wird (siehe Abs. 1), kann der ganze Absatz aufgehoben werden.

#### § 12 Abs. 3

Der Inhalt des Verzeichnisses wird wesentlich reduziert. Damit wird die Führung des Verzeichnisses stark vereinfacht.

#### § 12 Abs. 4 und Abs. 5

Abs. 4 und Abs. 5 werden aufgehoben. Die Datenschutzstelle wird von der Aufgabe der Registerführung für den Kanton entlastet (siehe Aufhebung von § 19 Abs. 1 Bst. i). Dies ist auch richtig, denn die Verantwortung für den Inhalt und die Vollständigkeit der Registereinträge liegt bei den Organen. Nur sie können die Richtigkeit und Vollständigkeit der Einträge gewährleisten, nicht die Datenschutzstelle. Die Meldepflicht an die Datenschutzstelle gemäss Abs. 4 wird damit hinfällig.

#### § 13 (Titel)

Der Titel wird aufgrund der Aufhebung von Abs. 2 (Wegfall des Begriffs «Einsicht») und der Anpassung an den neuen Inhalt der Bestimmung geändert.

#### § 13 Abs. 1

Das Auskunftsrecht jeder Person ist eines der Kernanliegen des Datenschutzrechts. Es ergänzt die Informationspflicht des Organs (siehe § 6a) und ist zentraler Ausgangspunkt dafür, dass eine Person ihre Rechte und Ansprüche nach diesem Gesetz überhaupt wahrnehmen kann. Die Änderungen in § 13 Abs. 1 drängen sich einerseits aufgrund der neuen Informationspflichten in

§ 6a auf, andererseits sind durch die Aufhebung bzw. Streichung einzelner Bestimmungen (wie § 8 oder § 12 Absätze 4 und 5) weitere Anpassungen notwendig geworden.

Die Regelung in § 13 Abs. 1 Bst. c, welche auf die Datenbekanntgaben aus den gemeindlichen Einwohnerregistern gemäss § 8 DSG Bezug nahm, ist systemfremd, da es sich hier bereits um «materielles» Datenschutzrecht handelt. § 13 Abs. 1 Bst. c wird deshalb in das Gemeindegesetz verschoben (siehe Fremdänderungen, Ziff. 6.2).

#### § 13 Abs. 2

Diese Bestimmung wird aufgehoben, da sie nicht mehr der gelebten Praxis entspricht. In der Regel verlangen die betroffenen Personen von den verantwortlichen Organen die Herausgabe von Kopien. Die Organe können aber selbstverständlich nach wie vor Einsicht vor Ort gewähren.

#### § 13 Abs. 3

Diese Anpassungen sind aufgrund der Änderungen in § 12 notwendig. Sie tragen auch zur besseren Verständlichkeit bzw. Lesbarkeit bei. Materiell ändert sich an der Bestimmung nichts.

#### § 14 Abs. 1

Der Begriff «Einsicht» wird gestrichen (siehe dazu die Erläuterungen zu § 13 Abs. 2). Zur Änderung des Begriffs «Daten» in «Personendaten» vgl. die Ausführungen zu § 2 Abs. 1 Bst. a.

#### § 14 Abs. 2

Abs. 2 wird begrifflich an § 6 angepasst.

#### § 15

Der Begriff «Daten» wird durch «Personendaten» ersetzt (siehe Näheres hierzu in den Erläuterungen zu § 2 Abs. 1 Bst. a).

#### § 16a

Mit § 16a erhält jede Person neu das Recht, bei der Datenschutzstelle vorstellig zu werden, wenn sie der Ansicht ist, dass die Bearbeitung der sie betreffenden Personendaten gegen datenschutzrechtliche Vorgaben verstösst. Dieses Recht steht ihr unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs zu. Es handelt sich dabei verwaltungsrechtlich um eine Art «Aufsichtsbeschwerde». Damit werden Art. 52 Richtlinie (EU) 2016/680 sowie Art. 15 Abs. 4 SEV 108 umgesetzt.

Die oder der Datenschutzbeauftragte muss sich mit der Eingabe der betroffenen Person befassen und ihr innert drei Monaten das Ergebnis oder den Stand der Abklärungen mitteilen. Bei offensichtlich unbegründeten Eingaben kann die oder der Datenschutzbeauftragte auch auf weitere Schritte verzichten. Dies muss der betroffenen Person jedoch unter Darlegung von Gründen mitgeteilt werden. Bei Unzuständigkeit ist die Eingabe unverzüglich an die zuständige Datenschutzstelle weiterzuleiten.

#### § 17 Abs. 3

Abs. 3 bezieht sich auf § 8 und wird zusammen mit dieser Bestimmung in das Gemeindegesetz verschoben (siehe dazu die Erläuterungen zu § 8 sowie die Fremdänderungen, Ziff. 6.2). An der Möglichkeit, für schriftlich erteilte Sammelauskünfte eine Gebühr zu erheben, ändert sich damit nichts.

#### **4. Titel: Wahl, Rechtsstellung, Aufgaben**

##### *§ 18 Abs. 2*

In Umsetzung von Art. 43 Abs. 2 Richtlinie (EU) 2016/680 legt das DSG neu ausdrücklich fest, dass nur eine qualifizierte Fachperson zur Datenschutzbeauftragten bzw. zum Datenschutzbeauftragten gewählt werden kann. Insbesondere muss die gewählte Person über ausreichende Erfahrung und fundierte Sachkunde im Bereich des Schutzes personenbezogener Daten verfügen. Die Fachkenntnisse können auf juristischen und/oder auf technischen Aspekten des Datenschutzes basieren.

##### *§ 19 Abs. 1 Bst. a*

Die generelle Ausnahme vom Geltungsbereich von hängigen Verfahren der Zivil- und Strafrechtspflege (inklusive Verfahren der internationalen Rechtshilfe) sowie der Verwaltungsrechtspflege ist mit den internationalen Vorgaben nicht vereinbar und wird aufgehoben (siehe dazu die Erläuterungen zu § 3 Abs. 2 Bst. a). An der richterlichen Unabhängigkeit soll sich selbstverständlich nichts ändern. Aus diesem Grund werden Datenbearbeitungen durch Justizbehörden im Rahmen ihrer justiziellen Tätigkeit von der Aufsicht der oder des Datenschutzbeauftragten ausgenommen. Diese Ausnahme von der Aufsicht ist auch in Art. 45 Abs. 2 Richtlinie (EU) 2016/680 sowie in Art. 11 Abs. 1 Bst. a SEV 108 vorgesehen.

##### *§ 19 Abs. 1 Bst. f*

Nach geltendem Recht hat die oder der Datenschutzbeauftragte Organe und die Öffentlichkeit über wesentliche Anliegen des Datenschutzes zu orientieren. In Umsetzung des Aufgabenkatalogs des Art. 46 Abs. 1 Bst. b und d Richtlinie (EU) 2016/680 wird diese Bestimmung angepasst. Zu den Aufgaben gehört demnach sowohl die Sensibilisierung der verantwortlichen Organe für ihre Pflichten als auch der Öffentlichkeit für die Anliegen des Datenschutzes (z.B. auch im Hinblick auf die Eigenverantwortung der betroffenen Personen).

##### *§ 19 Abs. 1 Bst. g*

Zum besseren Verständnis wird das Wort «diesen» eingefügt. Die Weisungsbefugnis der oder des Datenschutzbeauftragten in Bst. g bezieht sich auf die gemeindlichen Datenschutzstellen.

##### *§ 19 Abs. 1 Bst. i*

Die Registerführungspflicht der Datenschutzstelle für den Kanton wird aufgehoben. Die Führung des Verzeichnisses obliegt neu den kantonalen und gemeindlichen Organen. Der Kanton stellt dafür ein zentrales Erfassungs- und Publikationssystem zur Verfügung (siehe dazu die Erläuterungen zu § 12).



### § 19a (Titel)

In Anlehnung an die europäische Terminologie wird der Begriff «Vorabkontrolle» im Titel in «Vorabkonsultation» geändert. Dies entspricht dem Charakter der abzugebenden Stellungnahme der Datenschutzstelle. Denn es handelt sich dabei um eine beratende Tätigkeit im Zusammenhang mit der Datenschutz-Folgenabschätzung gemäss § 7b und nicht um eine eigentliche Kontrolle. Ziel der Vorabkonsultation ist es, den Datenschutz rechtzeitig sicher zu stellen, bevor Massnahmen ergriffen oder kostenintensive Investitionen getätigt werden. Der oder dem Datenschutzbeauftragten bleibt es indes unbenommen, zu einem späteren Zeitpunkt eine Kontrolle durchzuführen.

### § 19a Abs. 1

Abs. 1 wird aufgehoben. Die darin enthaltene Pflicht der Organe, entsprechende Vorhaben vorgängig der oder dem Datenschutzbeauftragten zur Stellungnahme vorzulegen, wird aus systematischen Gründen in § 7b Abs. 3 verschoben (siehe dazu die Erläuterungen zu § 7b Abs. 3).

### § 19a Abs. 2

Abs. 2 hält neu ausdrücklich die Pflicht der Datenschutzstelle fest, im Rahmen einer Vorabkonsultation gemäss § 7b Abs. 3 Stellung zu nehmen. Bisher ging diese Pflicht nur implizit aus § 19a Abs. 1 DSG hervor.

### § 19a Abs. 3

Um gegenüber den Organen Transparenz und Rechtssicherheit zu schaffen, soll die Datenschutzstelle eine Liste der Datenbearbeitungsvorgänge erstellen können, die vorab zur Konsultation vorzulegen sind. Kriterien dafür können etwa der Einsatz neuer Technologien und Verfahren, die Anzahl Betroffener oder die Sensitivität der Daten sein. Die Liste unterstützt auch die Datenschutzstelle darin, ihre Aufgaben effizient zu erfüllen. Die Datenschutzstelle entscheidet darüber, wo und in welcher Form sie diese Liste für die Organe zugänglich macht. Die Richtlinie (EU) 2016/680 verlangt, dass auch Rechtsvorhaben, welche das Bearbeiten von Personendaten betreffen, der Datenschutzstelle zur Vorabkonsultation vorzulegen sind. Diese Vorgabe ist gemäss geltendem Recht in § 19 Abs. 1 Bst. e DSG mitenthalten.

### § 20 Abs. 1

Zur Änderung des Begriffs «Daten» in «Personendaten» vgl. die Ausführungen zu § 2 Abs. 1 Bst. a. Aufgrund der Streichung des Begriffs «Datensammlung» (siehe § 2 Abs. 1 Bst. e) und der zunehmenden Komplexität von Bearbeitungsvorgängen (bspw. Profiling) werden die Befugnisse der oder des Datenschutzbeauftragten neu umschrieben. Die Einsicht in Unterlagen und die Vorführung von Datenbearbeitungsvorgängen entspricht der bisherigen Praxis, weshalb sich inhaltlich aus Abs. 1 keine Neuerungen ergeben.

### § 20 Abs. 2a

Neu muss ein Organ, an das eine Empfehlung gemäss Abs. 1 gerichtet ist, sich ausdrücklich zu dieser Empfehlung äussern. Es muss innerhalb der angesetzten Frist der Datenschutzstelle mitteilen, ob es der Empfehlung folgt oder nicht. Gestützt auf diese Mitteilung kann die oder der Datenschutzbeauftragte die weiteren Verfahrensschritte gemäss Abs. 3 einleiten.

### § 20 Abs. 3

Der oder dem Datenschutzbeauftragten muss neu die Befugnis zukommen, bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen in Form einer Verfügung treffen zu können (z.B. ein widerrechtliches Bearbeiten oder eine widerrechtliche Bekanntgabe von Personendaten einzustellen). Damit wird Art. 47 Abs. 2 Bst. b und c Richtlinie (EU) 2016/680 sowie Art. 15 Abs. 2 Bst. c SEV 108 umgesetzt. Eine verbindliche Anordnung kann nach Mitteilung

der Ablehnung einer Empfehlung (siehe Abs. 2a) erlassen werden. Diese verbindliche Anordnung in Form einer Verfügung ist beim Verwaltungsgericht anfechtbar (Abs. 4).

#### § 20 Abs. 3a

Falls schutzwürdige Interessen offensichtlich gefährdet oder verletzt werden, muss die oder der Datenschutzbeauftragte gemäss den europäischen Vorgaben die Befugnis haben, vorsorglich eine Datenbearbeitung zu untersagen.

#### § 20 Abs. 3b

Die Ausnahme ist selbstverständlich und ergibt sich aus dem Grundsatz der Gewaltentrennung.

#### § 20 Abs. 4

Die Verfügungen der oder des Datenschutzbeauftragten können vom betroffenen Organ an das Verwaltungsgericht weitergezogen werden. Das Verfahren richtet sich nach dem Gesetz über den Rechtsschutz in Verwaltungssachen vom 1. April 1976 (VRG; BGS 162.1). Ein allfälliger verwaltungsinterner Rechtsmittelweg würde zusätzliche Aufwände verursachen und die Unabhängigkeit der oder des Datenschutzbeauftragten in Frage stellen.

### 5. Titel: Rechtspflege und Strafbestimmung

#### § 24 Abs. 2

Neu kann mit Busse bestraft werden, wer vorsätzlich gegen Verpflichtungen in Vereinbarungen verstösst, die auf § 5c Abs. 2 oder 3, § 6 Abs. 2 DSG oder § 57<sup>bis</sup> Abs. 2 Bst. c Gesetz über die Organisation und die Verwaltung der Gemeinden vom 4. September 1980 (Gemeindegesezt [GG]; BGS 171.1) beruhen. Damit soll eine wirksame Durchsetzung der (in den Vereinbarungen enthaltenen) Verpflichtungen gewährleistet werden.

### 6. Titel: Übergangs- und Schlussbestimmungen

#### § 26 Abs. 1

Diese Anpassungen sind aufgrund der Änderungen in § 12 notwendig, wonach auf die Weiterführung des Begriffs «Datensammlung» künftig verzichtet wird.

Im Übrigen ist bei der Anpassung an das neue Recht unbestritten, dass die Umsetzung einige Zeit bedarf. Die Datenschutzstelle erwartet nicht, dass alle Arbeiten per Stichtag des Inkrafttretens umgesetzt sein werden. Sie wird den Organen einen angemessenen Zeitraum für die notwendigen Anpassungsarbeiten einräumen. Zudem wird die Datenschutzstelle den Organen bei der Implementierung behilflich sein. Abgesehen davon können sich die Organe bereits während des laufenden Gesetzgebungsprozesses auf die Neuerungen einstellen.

#### 6.2 Ziffer II: Fremdänderungen

##### Publikationsgesetz

###### Ausgangslage

Die Revision des Gesetzes über die Veröffentlichung der Gesetze und das Amtsblatt des Kantons Zug (Publikationsgesetz) vom 29. Januar 1981 (BGS 152.3) hat zum Ziel, das Amtsblatt in gedruckter Form durch das elektronische Amtsblatt als massgebliche Fassung abzulösen. Dieser Paradigmen- bzw. Primatwechsel bedarf einer gesetzlichen Grundlage.

Mit der raschen Entwicklung des Internets hat dieses Informationsmedium innert weniger Jahre eine zentrale Bedeutung erlangt. Gemäss jüngster Statistik benutzen über 80 % der Schweizer

Bevölkerung das Internet, Tendenz steigend. Sowohl in der Geschäftswelt als auch im privaten Bereich ist das Internet zu einem unverzichtbaren Instrument geworden.

Seit dem 1. Januar 2018 gibt die Staatskanzlei die «Amtliche Sammlung der Gesetze und der weiteren Erlasse des Kantons Zug» (GS) sowie die «Bereinigte Gesetzessammlung» (BGS) ausschliesslich in elektronischer Form heraus (§ 5 Abs. 1 Publikationsgesetz).

Bezüglich «Amtsblatt des Kantons Zug» (nachfolgend Amtsblatt) ist die Rechtslage so, dass dieses sowohl in gedruckter als auch in elektronischer Form erscheinen kann; hiervon ausgenommen sind aktuell einzig besonders schützenswerte Daten (§ 6 Abs. 3 Satz 2 Publikationsgesetz; Änderung vom 28. September 2000 anlässlich der Schaffung des Datenschutzgesetzes vom 28. September 2000 [GS 26, 867]). Gestützt auf § 10 Abs. 1 Publikationsgesetz ist die Herausgabe des Amtsblatts durch Vertrag vom 3. September 2002 einem privaten Herausgeber übertragen, nämlich der Speck Medien AG, Poststrasse 14, 6300 Zug. Das Amtsblatt der Speck Medien AG, Zug, erscheint in gedruckter Form.

Obwohl gestützt auf § 6 Abs. 3 Publikationsgesetz das Amtsblatt aus rechtlicher Sicht auch in elektronischer Form erscheinen kann und die Staatskanzlei aus technischer Sicht bereits über ein Amtsblatt-Tool verfügt (vgl. nachfolgend § 7a), so wurde bislang ein eigentlicher Paradigmen- bzw. Primatwechsel – weg vom Amtsblatt in gedruckter Form, hin zum elektronischen Amtsblatt – (noch) nicht vollzogen. Dieser soll jetzt – wie eingangs erwähnt – aufgrund eingangs genannter Überlegungen im Publikationsgesetz festgeschrieben werden. Die Revision des Publikationsgesetzes sieht im Unterschied zur gegenwärtigen Rechtslage vor, dass die Veröffentlichungen im elektronischen Amtsblatt auch Personendaten und besonders schützenswerte Personendaten gemäss § 2 Abs. 1 Bst. a und b des Datenschutzgesetzes enthalten dürfen, soweit dies für eine in einem Gesetz vorgeschriebene Veröffentlichung notwendig ist. Aus diesem Grund sind im Publikationsgesetz auch entsprechende datenschutzrechtliche Bestimmungen aufzunehmen. Es macht deshalb Sinn, die Revision des Publikationsgesetzes im Rahmen der aktuell laufenden Revision des Datenschutzgesetzes vorzunehmen (Fremdänderung). Die Revision des Publikationsgesetzes beschränkt sich im Wesentlichen darauf, die rechtlichen Grundlagen für das elektronische Amtsblatt als massgebliche Fassung zu schaffen; im Zuge dieser Revision werden weitere Normen, die das Amtsblatt betreffen, geändert bzw. aufgehoben, was nachfolgend erläutert wird. Zu erwähnen ist vorweg, dass die Staatskanzlei neu als Herausgeberin des elektronischen Amtsblatts bezeichnet wird (§ 7a). Zudem werden im elektronischen Amtsblatt nur noch amtliche Texte veröffentlicht; der nichtamtliche Anzeigenteil entfällt.

Insbesondere die neu eingefügten § 7a – 7c Publikationsgesetz sowie die dazugehörigen Erläuterungen orientieren sich stark an den einschlägigen Bestimmungen des Publikationsgesetzes des Kantons Zürich vom 30. November 2015 (LS 170.5).

#### Erläuterungen zu einzelnen Bestimmungen

##### *§ 6 (Zweck und Erscheinen)*

§ 6 enthält eine Zweckbestimmung (Abs. 1), eine Bestimmung bezüglich eines amtlichen Teils und eines nichtamtlichen Anzeigenteils (Abs. 2) sowie eine Bestimmung betreffend des Erscheinens sowie besonders schützenswerter Daten (Abs. 3).

§ 6 Abs. 1 (Publikation von Anzeigen natürlicher und juristischer Personen) und § 6 Abs. 2 (Bestimmung bezüglich eines nichtamtlichen Anzeigenteils) sind nach Sinn und Zweck in Verbindung mit § 10 Abs. 1 Publikationsgesetz so auszulegen, dass die Bewirtschaftung eines nichtamtlichen Anzeigenteils («Marktblatt») eine private Aufgabe darstellt, nicht eine staatliche.

Mit anderen Worten sind diese Bestimmungen für den Fall gedacht, dass der Regierungsrat die Herausgabe des Amtsblatts aufgrund einer öffentlichen Ausschreibung durch Vertrag einem privaten Herausgeber überträgt, wie dies aktuell der Fall ist. Eine gegenteilige Rechtslegung lässt sich auch aus den einschlägigen Materialien zum Publikationsgesetz nicht entnehmen.

Neu wird nun die Staatskanzlei ausdrücklich als Herausgeberin des elektronischen Amtsblatts bezeichnet (§ 7a Abs. 1). Als staatliches Organ hat sie einzig amtliche Texte zu veröffentlichen (vgl. nachfolgend § 7); die Bestimmungen betreffend Publikation von Anzeigen natürlicher und juristischer Personen (§ 6 Abs. 1) sowie eines nichtamtlichen Anzeigenteils (§ 6 Abs. 2) sind somit aufzuheben.

Weiter aufzuheben sind die in § 6 Abs. 3 enthaltenen die datenschutzrechtlichen Bestimmungen; der Datenschutz wird neu in § 7b geregelt.

Schliesslich wird die Überschrift zu § 6 den vorstehend genannten Änderungen angepasst (der Begriff «Gestaltung» entfällt dort infolge Bedeutungslosigkeit).

#### § 7 (Inhalt)

In § 7 Abs. 1 ist zu ergänzen, dass bei den zu publizierenden gesetzgeberischen Erlassen nebst denjenigen, die in die Amtliche Gesetzessammlung aufgenommen werden, auch diejenigen zu publizieren sind, die in die Bereinigte Gesetzessammlung aufgenommen werden. Dies ergibt sich aus § 5 Abs. 3, wonach die beiden Gesetzessammlungen gleichwertig sind. Der Zusatz hingegen, dass diese Gesetzessammlungen im Amtsblatt zu publizieren «oder bekannt zu geben» sind, kann infolge Bedeutungslosigkeit gestrichen werden. Die vorgenannten Publikationen werden nirgendwo anders als im Amtsblatt «bekannt gegeben».

In § 7 Abs. 3 – 5 werden die weiteren zu publizierenden Texte im Vergleich zur geltenden Fassung präziser umschrieben:

- Im Amtsblatt werden weitere amtliche Texte veröffentlicht, deren Veröffentlichung rechtlich vorgeschrieben ist (Abs. 3).
- Zudem können weitere amtliche Texte veröffentlicht werden, wenn ein hinreichendes öffentliches Interesse besteht (Abs. 4).
- Schliesslich können die Behörden in besonderen Fällen ein anderes Publikationsmittel benützen, sofern die Veröffentlichung im Amtsblatt nicht gesetzlich vorgeschrieben ist; diese heute schon geltende Bestimmung findet sich neu in Abs. 5 (aktuell Abs. 3).

#### § 7a (Herausgabe des Amtsblatts)

Wie schon mehrfach erwähnt, ist die Herausgabe des Amtsblatts aktuell gestützt auf § 10 Abs. 1 durch Vertrag vom 3. September 2002 einem privaten Herausgeber übertragen, nämlich der Speck Medien AG, Poststrasse 14, 6300 Zug. Das Amtsblatt der Speck Medien AG, Zug, erscheint in gedruckter Form. Die gedruckte Form somit aktuell die massgebende, rechtsverbindliche Fassung.

§ 7a Abs. 1 und Abs. 4 Satz 2 regeln neu, dass die Staatskanzlei das elektronische Amtsblatt als massgebliche Fassung herausgibt. Die Gründe für diesen Paradigmen- bzw. Primatwechsel wurden bereits eingangs genannt. In diesem Zusammenhang ist zu erwähnen, dass die Staatskanzlei bereits seit November 2017 über ein sogenanntes Amtsblatt-Tool verfügt. Das Amtsblatt-Tool erlaubt den Direktionen, Gerichten, Gemeinden und weiteren Stellen, die amtliche Publikationen vorzunehmen haben, ihre amtlichen Texte mittels Login selbstständig zu erfassen und an die Herausgeberin des gedruckten Amtsblatts, also der Speck Medien AG, zu übermitteln. Aufgrund dessen ist die Staatskanzlei in der Lage, sozusagen von heute auf mor-

gen das elektronische Amtsblatt herauszugeben. Dies setzt nebst der Schaffung der gesetzlichen Grundlagen selbstverständlich voraus, dass der Konzessionsvertrag mit der Speck Medien AG gekündigt wird. Gemäss Ziff. 5.02 des Konzessionsvertrags ist dieser unter Einhaltung einer zweijährigen Kündigungsfrist (erstmalig ab 31. Dezember 2010) kündbar. Diesen Umstand gilt es insbesondere auch bezüglich der Inkraftsetzung der fraglichen Bestimmungen des Publikationsgesetzes zu berücksichtigen.

Gemäss § 7a Abs. 2 wird das elektronische Amtsblatt auf einer Internetseite des Kantons veröffentlicht. Dabei stellt die Staatskanzlei die Authentizität und Integrität durch geeignete Massnahmen sicher (§ 7a Abs. 3). Dies bedingt insbesondere, dass deren Unveränderbarkeit durch geeignete Massnahmen sichergestellt werden muss. Dies soll in erster Linie auf technischem Weg erfolgen. Vorgesehen ist, die Inhalte mit einer digitalen Signatur zu versehen, die deren Authentizität und Integrität zweifelsfrei bestätigt. Diese Mittel werden bei den elektronischen Veröffentlichungen des Schweizerischen Handelsamtsblatt ([www.shab.ch](http://www.shab.ch)) seit 2003 erfolgreich angewendet.

Gleichwohl kann das Amtsblatt zusätzlich ganz oder teilweise in gedruckter Form veröffentlicht werden (§ 7a Abs. 4 Satz 1). Diese Regelung berücksichtigt den Umstand, dass Teile der Bevölkerung das Internet noch nicht nutzt. Für diesen Bevölkerungsteil, bei dem gegebenenfalls noch eine Nachfrage nach dem gedruckten Amtsblatt vorhanden ist, soll die Möglichkeit bestehen, dass das Amtsblatt ganz oder teilweise in gedruckter Form herausgegeben werden kann. Aufgrund des hohen Durchdringungsgrades des Internets ist davon auszugehen, dass die Nachfrage nach einem Amtsblatt in gedruckter Form zukünftig wohl stetig abnehmen wird.

Die elektronische Fassung ist jedoch neu von Gesetzes wegen die massgebende (§ 7a Abs. 4 Satz 2). Dies bedeutet einen Primatwechsel zum rechtsverbindlichen elektronischen Amtsblatt.

#### *§ 7b (Datenschutz und Einsichtnahme)*

Wie schon erwähnt, kann das Amtsblatt gestützt auf § 6 Abs. 3 bereits heute im Internet publiziert werden. Ausgenommen davon sind allerdings besonders schützenswerte Daten im amtlichen Teil.

Neu dürfen gemäss § 7b Abs. 1 im elektronischen Amtsblatt die Veröffentlichungen nach Publikationsgesetz auch Personendaten und besonders schützenswerte Personendaten gemäss § 2 Abs. 1 Bst. a und b des Datenschutzgesetzes enthalten, soweit dies für eine in einem Gesetz vorgeschriebene Veröffentlichung notwendig ist. Die Verordnung legt die Zeiträume fest, während derer die Veröffentlichungen über eine Suchfunktion erschlossen werden. Dabei sind insbesondere die Interessen an der Öffentlichkeit und privaten Interessen zu berücksichtigen (§ 7a Abs. 2).

Die besondere Bedeutung des Datenschutzes im Zusammenhang mit der Veröffentlichung von Personendaten und besonders schützenswerten Personendaten im Internet erfordert eine eigene Bestimmung über den Datenschutz. Die Veröffentlichung von Personendaten und besonders schützenswerten Personendaten darf regelmässig nur gestützt auf eine Ermächtigung in einem Spezialgesetz erfolgen. So sehen verschiedene Verfahrensgesetze (z. B. § 10 Abs. 4 VRG, Art. 141 ZPO, Art. 88 StPO) öffentliche Bekanntmachungen von Personendaten und besonders schützenswerten Personendaten im Amtsblatt vor.

Die häufig Einzelpersonen belastenden Meldungen im Amtsblatt bedingen eine Güterabwägung. Einerseits haben die amtlichen Publikationen gerade den Sinn und Zweck, Informationen allen Interessierten zugänglich zu machen. Andererseits sind aus Gründen des Persönlichkeits-

schutzes Personendaten und besonders schützenswerten Personendaten nicht länger als notwendig mit Suchfunktionen zu erschliessen. Der Grundsatz der Verhältnismässigkeit in Bezug auf die Dauer, während der Personendaten und besonders schützenswerten Personendaten mithilfe einer Suchfunktion ohne weiteres auffindbar sind, soll im Gesetz verankert werden. Eine zeitlich unbeschränkte Suchmöglichkeit über den gesamten Datenbestand wäre unverhältnismässig, weil der Zweck der meisten Meldungen durch Fristablauf bereits erfüllt ist.

Nach Ablauf des Suchzeitraums sollen die Amtsblatt-Ausgaben vom Netz genommen werden. Dies erfordern Verhältnismässigkeitsgründe, weil Internetpublikationen im Gegensatz zu Papierausgaben weitergehende Möglichkeiten bieten: Sie können weltweit rund um die Uhr leicht eingesehen, gespeichert, kopiert, weiterverwendet, weiterverbreitet und mit anderen Daten verknüpft werden. Internetpublikationen bringen insgesamt eine grössere Gefahr für Persönlichkeitsverletzungen mit sich. Die von Meldungen im Amtsblatt betroffenen Personen haben ein gewichtiges Interesse daran, dass ihre Personendaten und besonders schützenswerten Personendaten zeitlich nicht unbeschränkt über das Internet abrufbar bleiben. Um berechtigten Anliegen Dritter, auch nach Ablauf des Suchzeitraums bestimmte Meldungen auffinden zu können, Rechnung zu tragen, wird die Verwaltung sich so einzurichten haben, dass ältere Ausgaben des Amtsblattes offline zugänglich gemacht werden. Die Einzelheiten sind auf Verordnungsstufe zu regeln.

In die im Internet veröffentlichten amtlichen Publikationen kann bei der Staatskanzlei Einsicht genommen werden (§ 7a Abs. 3). Die Staatskanzlei soll damit verpflichtet werden, der Öffentlichkeit die Einsichtnahme in die elektronischen Fassungen zu gewähren. Dies kann mittels einer öffentlich zugänglichen Internetstation in der Staatskanzlei oder mittels Ausdruck der nachgefragten Informationen aus dem Publikationsorgan im Internet durch die Mitarbeitenden der Staatskanzlei erfolgen. Aufgrund des hohen Durchdringungsgrades des Internets ist davon auszugehen, dass diese Dienstleistung wenig nachgefragt und zukünftig wohl stetig abnehmen wird.

#### *§ 7c (Gebühren)*

Die Einsichtnahme in die im Internet veröffentlichten amtlichen Publikationen sowie deren Herunterladen für die individuelle Bearbeitung sind unentgeltlich (§ 7a Abs. 1). Zur Wahrung der Kenntnisnahme-Fiktion ist eine kostenlose Einsichtnahme in das elektronische Amtsblatt notwendig, was im Übrigen auch für die Gesetzessammlungen in elektronischer Form gilt. Auch hier muss sichergestellt sein, dass die Rechtsunterworfenen unentgeltlichen Zugang zum geltenden Recht haben (vgl. § 5 Abs. 1). Es wäre aus rechtsstaatlicher Sicht unhaltbar, wenn Rechtssuchende bzw. Adressatinnen und Adressaten von im Amtsblatt veröffentlichten amtlichen Texten erst nach Bezahlung einer Entschädigung die sie betreffenden Rechtserlasse bzw. amtlichen Texte einsehen könnten.

Allerdings ist die Erhebung von Gebühren für besondere Dienstleistungen vorgesehen (§ 7c Abs. 2). Analog zur bestehenden Lösung des Schweizerischen Handelsamtsblattes ist dies beispielsweise bei einem Abonnement für die elektronische Lieferung von neuen Mitteilungen im Amtsblatt gemäss einem hinterlegten Suchprofil denkbar.

Auf Verordnungsstufe sind sodann besondere Anforderungen an die Verwertung der amtlichen Publikationen durch Dritte festzulegen, namentlich bezüglich Personendaten und besonders schützenswerten Personendaten (§ 7c Abs. 3). Es soll sichergestellt werden, dass eine Drittperson, die Daten zu Verwertungszwecken bezogen hat, bei deren Behandlung den gleichen Bedingungen und Verpflichtungen unterstellt ist wie die herausgebende Verwaltungsstelle. Insbesondere ist der gleiche Umgang mit Personendaten und besonders schützenswerten Perso-

nendaten zu gewährleisten. Namentlich sind die zeitlichen Beschränkungen einer Online-Zugänglichkeit zu beachten. Die Erstellung oder Verbreitung von Persönlichkeitsprofilen, die durch systematische Bearbeitung der mit den amtlichen Publikationsorganen und dem Behördenverzeichnis zur Verfügung gestellten Daten erfolgt, soll unterbunden werden können.

Wie vorstehend unter § 7a erwähnt, kann (nebst dem elektronischen Amtsblatt) das Amtsblatt zusätzlich ganz oder teilweise in gedruckter Form veröffentlicht werden. Für diesen Fall regelt § 7c Abs. 4, dass der Bezug des Amtsblatts in gedruckter Form kostenpflichtig ist und die Erhebung der Gebühren in einer Verordnung zu regeln sind.

#### *§ 9 (Redaktion und formelle Berichtigung)*

Da durch die Herausgabe des elektronischen Amtsblatts durch die Staatskanzlei der nichtamtliche Anzeigenteil entfällt (vgl. vorstehend § 6), ist § 9 Abs. 1 entsprechend anzupassen, und zwar so, dass der Staatskanzlei generell die Redaktion des Amtsblatts obliegt. Mit anderen Worten trägt die Staatskanzlei für die Veröffentlichung der amtlichen Texte im Amtsblatt weiterhin auch dann die Verantwortung, wenn die Direktionen, Gerichte, Gemeinden und weiteren Stellen, die amtliche Publikationen vorzunehmen haben, diese mittels Login im Amtsblatt-Tool selbstständig erfassen.

Infolge des Verzichts auf einen nichtamtlichen Teil im Amtsblatt sind zudem in § 9 die Abs. 2 und 3 aufzuheben.

Gemäss § 5a berichtigt die Staatskanzlei in der GS und BGS sinnverändernde Fehler und Formulierungen, die nicht dem Beschluss des erlassenden Organs entsprechen. Sinnverändernde Fehler und Formulierungen sind Grammatik-, Rechtschreib- und Darstellungsfehler, falsche Zahlen und Nummerierungen, falsche Verweise, terminologische Unstimmigkeiten. Derartige Berichtigungen soll die Staatskanzlei als Redaktorin des Amtsblatts auch bei im Amtsblatt veröffentlichten Texten vornehmen dürfen (§ 9 Abs. 1 Satz 2). Die Überschrift zu § 9 ist entsprechend zu ergänzen.

#### *§ 10 (Private Herausgabe des Amtsblatts)*

Die Überschrift lautet neu «Private» Herausgabe des Amtsblatts. Diese Präzisierung ist notwendig, weil die Überschrift zu § 7a exakt so lautet, wie aktuell in § 10. Mit dem Zusatz «Private» wird auch verdeutlicht, dass die Herausgabe des Amtsblatts grundsätzlich durch die Staatskanzlei erfolgt (eine Regelung, die im bisherigen Recht im Übrigen gänzlich fehlt), und die Herausgabe durch Private eben nur dann erfolgt, wenn der Regierungsrat die Herausgabe des Amtsblatts durch Vertrag einem privaten Herausgeber überträgt, wie dies gegenwärtig mit der Medien Speck AG der Fall ist.

### **Archivgesetz**

#### *§ 2 Abs. 5*

Aufgrund der Streichung der Begriffsdefinition «Dritte» in § 2 Abs. 1 Bst. k DSG ist der Verweis auf diesen Begriff in § 2 Abs. 5 Archivgesetz vom 29. Januar 2004 (BGS 152.4) ebenfalls zu streichen.

#### *§ 2 Abs. 5 / § 12 Abs. 1*

Der Begriff «Persönlichkeitsprofil» wird in § 2 Abs. 1 Bst. b DSG aufgehoben und in § 2 Abs. 1 Bst. b1 DSG durch den Begriff «Profiling» ersetzt (vgl. die Erläuterungen zu § 2 Abs. 1 Bst. b und b1). Dementsprechend ist auch die Terminologie in § 2 Abs. 5 sowie § 12 Abs. 1 des Archivgesetzes anzupassen.

## Gemeindegesezt

### § 57f<sup>bis</sup>

Die Regelung von Datenbekanntgaben aus den gemeindlichen Einwohnerregistern im DSG ist systemfremd, da es sich hier bereits um «materielles» Datenschutzrecht handelt. Die bisherigen § 8, 13 Abs. 1 Bst. c und 17 Abs. 3 DSG sind inhaltlich eng miteinander verknüpft. Sie werden deshalb verschoben und neu in § 57f<sup>bis</sup> in einem einzigen Paragraphen des Gesetzes über die Organisation und die Verwaltung der Gemeinden 4. September 1980 (Gemeindegesezt; BGS 171.1) zusammengefasst.

## Polizeigesetz

### § 38a Abs. 3 Bst. a

Der Begriff der «Datensammlung» wird aufgehoben (vgl. die Erläuterungen zu § 2 Abs. 1 Bst. e), was eine entsprechende Umformulierung von § 38a Abs. 3 Bst. a des Polizeigesetzes vom 30. November 2006 (BGS 512.1) notwendig macht.

### § 40 Abs. 2

Der Begriff «Persönlichkeitsprofil» wird in § 2 Abs. 1 Bst. b DSG aufgehoben und in § 2 Abs. 1 Bst. b1 DSG durch den Begriff «Profiling» ersetzt (vgl. die Erläuterungen zu § 2 Abs. 1 Bst. b und b1). Dementsprechend ist auch die Terminologie in § 40 Abs. 2 des Polizeigesetzes anzupassen.

## 6.3 Ziffer III: Fremdaufhebungen

Es gibt keine Fremdaufhebungen.

## 6.4 Ziffer IV: Inkrafttreten

Die revidierte Fassung des Gesetzes wird nach Ablauf der Referendumsfrist durch den Regierungsrat in Kraft gesetzt. Für den Vollzug muss die Datensicherheitsverordnung vom 16. Januar 2007 (DSV; BGS 157.12) angepasst werden.

## 7. Finanzielle Auswirkungen und Anpassungen von Leistungsaufträgen

### 7.1 Finanzielle Auswirkungen auf den Kanton

Der Kanton stellt für die kantonalen und gemeindlichen Organe ein zentrales Erfassungs- und Publikationssystem zur Verfügung (§ 12 Abs. 1). Die heutige Anwendung «Register der Datensammlung» ist nicht geeignet, um dezentral das «Verzeichnis der Bearbeitungstätigkeiten» pflegen zu können. Die Initialkosten für das Erstellen einer IT-Lösung (bzw. Anpassen der bestehenden IT-Lösung) betragen je nach Funktionsumfang und Betriebsmodell schätzungsweise zwischen 30'000 und 55'000 Franken. Dazu kommen die entsprechenden jährlichen externen und/oder internen Betriebskosten. Bei Übernahme der Bundeslösung entstehen beispielsweise Investitionskosten von rund 55'000 Franken und jährliche Betriebskosten von rund 20'000 Franken. Wird die Anwendungsverantwortung sowie die technische Verantwortung hingegen kantonsintern (bspw. durch das AIO) wahrgenommen, würden entsprechende finanzielle und personelle Ressourcen intern benötigt.

A	Investitionsrechnung	2019	2020	2021	2022
1.	Gemäss Budget oder Finanzplan: bereits geplante Ausgaben				
	bereits geplante Einnahmen				
2.	Gemäss vorliegendem Antrag:				



	effektive Ausgaben				
	effektive Einnahmen				
<b>B</b>	<b>Erfolgsrechnung (nur Abschreibungen auf Investitionen)</b>				
3.	Gemäss Budget oder Finanzplan: bereits geplante Abschreibungen				
4.	Gemäss vorliegendem Antrag: effektive Abschreibungen				
<b>C</b>	<b>Erfolgsrechnung (ohne Abschreibungen auf Investitionen)</b>				
5.	Gemäss Budget oder Finanzplan: bereits geplanter Aufwand				
	bereits geplanter Ertrag				
6.	Gemäss vorliegendem Antrag: effektiver Aufwand		75'000	20'000	20'000
	effektiver Ertrag				

## 7.2 Finanzielle Auswirkungen auf die Gemeinden

Die gemeindlichen Organe sind ebenso verpflichtet, ein Verzeichnis ihrer Bearbeitungstätigkeiten zu führen und zu veröffentlichen (§ 12 Abs. 1). Der Kanton stellt das zentrale Erfassungs- und Publikationssystem (vgl. Erläuterungen zu Ziff. 7.1) den gemeindlichen Organen unentgeltlich zur Verfügung.

## 7.3 Anpassungen von Leistungsaufträgen

Diese Vorlage hat keine Anpassungen von Leistungsaufträgen zur Folge.

## 8. Zeitplan

Dezember 2018	1. Lesung im RR
Dez. 2018 bis April 2019	Verwaltungsexterne Vernehmlassung
Juni 2019	2. Lesung im RR
August 2019	Kantonsrat, Kommissionsbestellung
Sept. bis November 2019	Kommissionssitzung(en)
Dezember 2019	Kommissionsbericht
Februar 2020	Kantonsrat, 1. Lesung
Mai 2020	Kantonsrat, 2. Lesung
Juni 2020	Publikation Amtsblatt
August 2020	Ablauf Referendumsfrist
November 2020	Allfällige Volksabstimmung
2020	Inkrafttreten

## 9. Antrag

Gestützt auf die vorstehenden Ausführungen beantragen wir Ihnen auf die Vorlage Nr. - einzutreten und ihr zuzustimmen.

Zug,

Mit vorzüglicher Hochachtung  
Regierungsrat des Kantons Zug

Die Frau Landammann: Manuela Weichelt-Picard

Der Landschreiber: Tobias Moser

115/