



## Änderung des Datenschutzgesetzes

Bericht und Antrag der vorberatenden Kommission  
vom 21. Oktober 2019

Sehr geehrte Frau Präsidentin  
Sehr geehrte Damen und Herren

Die vorberatende Kommission des Kantonsrats betreffend Änderung des Datenschutzgesetzes hat die Vorlage des Regierungsrates vom 18. Juni 2019 (Vorlagen Nr. 2985.1 – 16094 und 2985.2 – 16095) in zwei Sitzungen vom 12. August und 21. Oktober 2019 beraten und verabschiedet. Sicherheitsdirektor Beat Villiger vertrat das Geschäft aus Sicht der Regierung. Er wurde von Yvonne Jöhri, Datenschutzbeauftragte, Meret Baumann, Generalsekretärin der Sicherheitsdirektion, und Carmen Lingg, juristische Mitarbeiterin der Sicherheitsdirektion, unterstützt. An der zweiten Kommissionssitzung nahm zudem Christine Andres, stellvertretende Datenschutzbeauftragte, teil. Das Protokoll führte Fabienne Küttel, Sachbearbeiterin der Sicherheitsdirektion.

Der Bericht ist wie folgt gegliedert:

1. Ausgangslage
2. Ablauf der Kommissionsberatung
3. Fragerunde
4. Eintretensdebatte
5. Detailberatung Datenschutzgesetz
6. Detailberatung Fremdänderungen
7. Schlussabstimmung
8. Kommissionsantrag

### 1. Ausgangslage

Der Kanton Zug passt das kantonale Datenschutzgesetz (Datenschutzgesetz vom 28. September 2000, BGS 157.1; nachfolgend: DSG) an die heutigen technischen Gegebenheiten und die damit einhergehende Weiterentwicklung des Datenschutzes sowie an die europäischen Vorgaben an. Das Gesetz regelt die Rechte und Pflichten hinsichtlich des Datenschutzes von öffentlichen Organen des Kantons Zug (Kanton, Gemeinden, Private mit Leistungsvereinbarungen). Diese werden präzisiert und der Schutz der Daten der betroffenen Personen verstärkt. Im Übrigen sollen geringfügige terminologische und praktische Anpassungen vorgenommen werden.

### 2. Ablauf der Kommissionsberatung

Der Kommissionspräsident eröffnete die erste Kommissionssitzung vom 12. August 2019 mit einem kurzen Überblick über den Ablauf der ersten Sitzung. Anschliessend führte Sicherheitsdirektor Beat Villiger in die Vorlage ein und orientierte über die Ausgangslage und den Handlungsbedarf. Weiter erklärte er, die Sicherheitsdirektion sei für die Bearbeitung dieser direktionsübergreifenden Gesetzesvorlage in ihrer Funktion als Rechtsdienst des Regierungsrates zuständig. Daraufhin gab Yvonne Jöhri der Kommission einen kurzen Überblick über die (Rechts-)Grundlagen sowie die Entwicklungen im Datenschutz. Sodann stellte Carmen Lingg die Gesetzesvorlage summarisch vor und erläuterte die vorgesehenen Änderungen einzelner Bestimmungen.

Nach Abschluss der Fragerunde (vgl. nachfolgend Ziff. 3) und auf Basis dieser Diskussion folgte die Eintretensdebatte (vgl. nachfolgend Ziff. 4) und daraufhin die Detailberatung der Vorlage (vgl. nachfolgend Ziff. 5). Dabei wurde die Sicherheitsdirektion im Hinblick auf die zweite Kommissionssitzung bei verschiedenen Bestimmungen mit der Klärung von spezifischen Fragen beauftragt (vgl. Ergebnis dieser Abklärungsaufträge nachfolgend in Ziff. 5 in Kästen). Die Kommission setzte die Detailberatung an ihrer zweiten Kommissionssitzung vom 21. Oktober 2019 fort und schloss ihre Arbeiten mit der Schlussabstimmung ab.

An der ersten Kommissionssitzung vom 12. August 2019 waren alle 15 Kommissionsmitglieder anwesend; bei der zweiten Kommissionssitzung vom 21. Oktober 2019 waren 14 Kommissionsmitglieder zugegen.

### **3. Fragerunde**

An der ersten Kommissionssitzung vom 12. August 2019 gab es im Anschluss zur Vorstellung der Gesetzesvorlage sowie zum Antrag und zum Bericht und Antrag des Regierungsrates vom 18. Juni 2019 eine ausführliche Fragerunde. Dabei wurden folgende Themen bzw. Fragen intensiv diskutiert:

#### **→ Mehraufwand für die Datenschutzstelle und die Gemeinden aufgrund DSGVO-Revision**

Auf Nachfrage eines Kommissionsmitgliedes erklärte die Datenschutzbeauftragte, dass unabhängig von der vorliegenden Revision eine Personalerhöhung von 50%-Stellenprozent für die Datenschutzstelle beantragt worden sei, weil die Anfragen über Cloud-Lösungen und Möglichkeiten ihrer technischen Umsetzung stark angestiegen seien und entsprechende neue Kompetenzen im IT-Bereich benötigt werden. Aufgrund der DSGVO-Revision werde nicht mit einem erheblichen Mehraufwand gerechnet. Weiter wurde ausgeführt, dass auch bei den Gemeinden – entgegen deren Befürchtung – nicht von einem wesentlichen Mehraufwand ausgegangen werde. Verschiedene Rechte und Pflichten würden sich bereits aus dem geltenden Recht ergeben. Der im Gesetz über die Organisation und die Verwaltung der Gemeinden vom 4. September 1980 (Gemeindegesezt, GG; BGS 171.1) vorgesehenen erweiterten Auskunftspflicht sollte mit bestehenden bzw. allenfalls einfachen zusätzlichen Instrumenten nachgekommen werden können. Im Übrigen wurde darauf hingewiesen, dass jede betroffene Person ihre Rechte und Ansprüche nur wahrnehmen könne, wenn ihr die Datenbearbeitung bekannt sei (Sinn des Auskunftsrechts). In diesem Zusammenhang wurden auch eine allfällige Einschränkung der Auskunftspflicht der Gemeinden sowie der Zeitpunkt des Inkrafttretens des revidierten DSGVO angesprochen.

#### **→ Verfügungskompetenz der Datenschutzstelle**

Auf Nachfrage eines Kommissionsmitgliedes wurde erklärt, dass dem/der Datenschutzbeauftragten in der vorliegenden Vorlage des Regierungsrats keine weiteren Kompetenzen zum Erlass von verbindlichen Verfügungen und/oder Verwaltungssanktionen vorgesehen seien (obwohl im europäischen Recht so vorgesehen).

#### **→ Anpassungsbedarf im kantonalen Recht bzw. Konsequenzen bei Nichtanpassung durch Kanton Zug**

Die Relevanz der verschiedenen (europäischen) Rechtsgrundlagen für die Schweiz wurde intensiv diskutiert. Dabei wurde seitens Regierungsrat und Datenschutzstelle der Anpassungsbedarf nochmals aufgezeigt: Es wurde darauf hingewiesen, dass die Anforderungen der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts (nachfolgend: Richtlinie (EU) 2016/680) als Teil des Schengen-Besitzstandes übernommen werden sollten bzw. müssten. Diese würden insbesondere gewährleisten, dass die Schweiz bzw. auch die Organe des Kantons Zug (Polizei, Migrationsbehörden etc.) Zugang zu den wesentlichen Informationssystemen hätten. Andernfalls könnte mit einem

Ausschluss (auch beschränkt auf den Kanton Zug) gedroht werden. Weiter solle die Vorlage (aufgrund deren bevorstehenden Ratifizierung) mit der Konvention SEV 108 (nachfolgend: SEV 108) vereinbar sein. Schliesslich solle sich die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutz-Grundverordnung [DSGVO]) annähern. Diese sei zentrale Voraussetzung dafür, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätige, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspreche. Ohne Angemessenheitsbeschluss müssten im Einzelfall Garantien vereinbart werden, damit ein Datenaustausch stattfinden könne (fehlende Flexibilität, mehr Aufwand).

→ *Regelung von Cloud- und Blockchain-Technologien im Datenschutzgesetz*

Es wurde erläutert, dass Datenschutzgesetze technologieneutral formuliert sein sollen, damit sie nicht bei jeder zukünftigen Entwicklung bzw. jeder neuen Technologie angepasst werden müssten. Infolgedessen sei keine spezielle Regelung für einzelne (gerade aktuelle) Technologie ins DSG aufgenommen worden.

#### 4. Eintretensdebatte

Aufgrund der Befürchtung eines grossen Mehraufwandes bzw. erheblicher Kosten für die Gemeinden, dem diesen gegenüberstehenden vermuteten geringen Nutzen der Gesetzesvorlage und der Erwartung, dass die Vorlage mehr Unsicherheit als Sicherheit bringe, wurde beantragt, auf die Vorlage nicht einzutreten. Gleichzeitig wurde von anderer Seite mit der Begründung des Anpassungsbedarfs an die heutigen Gegebenheiten, sowie des erwarteten nicht allzu grossen Aufwandes aufgrund neuer technischer Lösungen der Antrag gestellt, auf die Vorlage einzutreten.

In der Folge beschloss die Kommission mit 12:3 Stimmen, auf die Vorlage zur Änderung des Datenschutzgesetzes (Nr. 2985.1 – 16094 und 2985.2 – 16095) einzutreten.

#### 5. Detailberatung Datenschutzgesetz

In der Detailberatung ging die Kommission die einzelnen Bestimmungen der Vorlage durch. Nachfolgend wird in lediglich auf diejenigen Bestimmungen eingegangen, bei welchen ein Änderungsantrag gestellt oder über einzelne Punkte vertieft diskutiert wurde:

##### **§ 2 Abs. 1 Bst. a Begriff «Daten» (neu: «Personendaten»)**

Es wurde die Frage aufgeworfen, ob der Begriff «Daten» im Rahmen der Revision nicht generell durch den Begriff «Personendaten» ersetzt werden sollte. Verschiedene Bestimmungen (bspw. § 15 Abs. 4 DSG oder §§ 57<sup>f</sup><sup>bis</sup> Abs. 2 Bst. c GG) würden immer noch den Begriff «Daten» anstelle von «Personendaten» beinhalten. Es wurde erklärt, dass im DSG klar zwischen Personendaten und Daten unterschieden und grundsätzlich überall der Begriff Personendaten verwendet werde. Allerdings werde der Einfachheit und Verständlichkeit halber bei zusammengesetzten Wörtern sowie innerhalb desselben Absatzes im DSG weiterhin der Begriff Daten verwendet, wenn eindeutig sei, dass damit Personendaten gemeint seien (bspw. § 10a Abs. 2 Bst. a DSG). Ausserdem seien in diesem Zusammenhang nicht sämtliche Gesetze (ausserhalb des DSG) angepasst worden, da der Begriff Daten in sehr vielen Gesetzen verwendet werde und eine konsequente Anpassung zahlreiche (nicht zwingend notwendige) Fremdänderungen nach sich gezogen hätte.

##### **§ 2 Abs. 1 Bst. b Begriff «Besonders schützenswerte Personendaten»**

Ein Kommissionsmitglied stellte die Frage, ob bei biometrischen Daten der Zusatz «die mittels technischer Verfahren die eindeutige Identifizierung einer natürlichen Person erlauben»

notwendig sei. Es wurde erläutert, dass diese Ergänzung nötig sei, weil ansonsten auch etwa gewöhnliche Portraitfotografien, bei denen es sich eigentlich auch um biometrische Daten handelt, unter die besonders schützenswerten Personendaten fallen würden.

### **§ 2 Abs. 1 Bst. b Begriff «Besonders schützenswerte Personendaten» / § 2 Abs. 1 Bst. b1 «Profiling»**

Der Begriff «Persönlichkeitsprofil» wird in § 2 Abs. 1 Bst. b aufgehoben und in § 2 Abs. 1 Bst. b1 durch den neuen Begriff «Profiling» ersetzt. Die Kommission diskutierte über diese Begriffsdefinition. Es wurde erwogen, dass der neue Begriff «Profiling» den neuen Technologien Rechnung trägt. Damit werde nicht nur das Ergebnis eines Bearbeitungsprozesses, nämlich das Persönlichkeitsprofil an sich, sondern eine bestimmte Form der Datenbearbeitung und der gesamte Datenverarbeitungsprozess verstanden. Neben den EU Staaten hätten auch der Bund sowie Kantone für die neue Begriffsdefinition entschieden. Einige Kommissionsmitglieder erklärten hingegen, es mache keinen Sinn, Anglizismen zu übernehmen. In diesem Zusammenhang wurden zwei Anträge gestellt, über die nacheinander abgestimmt wurde:

1. Antrag in § 2 Abs. 1 b1 den Begriff «Persönlichkeitsprofil» statt «Profiling» zu verwenden (*«Persönlichkeitsprofilerstellung ist jede, insb. ...»*).

Die Kommission lehnte den Antrag mit 9:6 Stimmen ab.

2. Antrag, § 2 Abs. 1 Bst. b1 und damit die Begriffsdefinition «Profiling» ganz zu streichen.

Die Kommission lehnte den Antrag mit 12:3 Stimmen ab.

### **§ 2 Abs. 1 Bst. c Begriff «Bearbeiten»**

Es wurde darüber diskutiert, ob die Änderungen in § 2 Abs. 1 Bst. c notwendig sind. Vor diesem Hintergrund wurde folgender Antrag gestellt:

Antrag, die geltende Begriffsdefinition zu belassen und lediglich den Begriff «Daten» mit «Personendaten» zu ersetzen.

Die Kommission lehnte den Antrag mit 8:7 Stimmen ab.

### **§ 3 Abs. 4 Geltungsbereich**

Die Kommission diskutierte den Geltungsbereich des DSG und weshalb das «Verfahren der internationalen Rechtshilfe» in der Bestimmung als separates Verfahren aufgeführt ist bzw. ob dies notwendig sei. Es wurde ausgeführt, dass die Formulierung geltendem Recht (bisheriger § 3 Abs. 2 Bst. a) entspricht und eine Aufhebung der Klammerbemerkung zu (unnötigen) Fragen führen könnte. Es erfolgte der

Antrag, die Klammerbemerkung «(inklusive Verfahren der internationalen Rechtshilfe)» zu streichen.

Die Kommission lehnte den Antrag mit 10:3 Stimmen, bei 2 Enthaltungen ab.

Weiter wurde festgestellt, dass die «erstinstanzlichen nicht strittigen Verwaltungsverfahren» im vorgeschlagenen Abs. 4 – im Gegensatz zum bisherigen Abs. 2 Bst. a in § 3 – nicht mehr explizit genannt werden. In diesem Zusammenhang wurde diskutiert, was der konkrete Unterschied vom geltenden Recht zum Antrag des RR vom 18. Juni 2019 sei (auch kostenmässig). Dabei wurde die Sicherheitsdirektion im Hinblick auf die zweite Sitzung beauftragt, dies genauer abzuklären und auszuführen.

An der zweiten Kommissionssitzung wurde erklärt, dass mit der neuen Formulierung klargestellt wird, dass das DSG – wie bisher – nicht auf «strittige» Verwaltungsverfahren (nach Erlass einer Verfügung) anwendbar sei, sondern nur auf «nicht strittige» Verwaltungsverfahren (vor Erlass einer Verfügung). Dass diese eigentlich logische Schlussfolgerung bisher explizit im Gesetzestext erwähnt worden sei, habe zu Unklarheiten geführt. Folglich sei im vorgeschlagenen Abs. 4 auf diese Nennung verzichtet worden. Materiell (auch kostenmässig) erfolge mit der neuen Formulierung keine Änderung.

Die Kommission nahm von der Abklärung ohne weitere Fragen Kenntnis.

#### **§ 5c Abs. 1 Bst. a/b Voraussetzungen für das Bekanntgeben von Personendaten zu einem nicht personenbezogenen Zweck**

Es wurde besprochen, was genau unter den Begriffen «Statistik, Planung und Forschung» verstanden wird bzw. wie sich die Begriffe voneinander unterscheiden. Zudem wurde die Frage aufgeworfen, ob auf die Formulierung «namentlich für Statistik, Planung oder Forschung» in Bst. a verzichtet und/oder ob Bst. b in Bst. a integriert werde könne. Ferner wurde diskutiert, weshalb sich die Voraussetzungen für das Bekanntgeben von Personendaten zu einem nicht personenbezogenen Zweck an Private (Bst. b) von jenem an andere kantonale oder gemeindliche Organe (Bst. a) unterscheiden. Die Sicherheitsdirektion wurde damit beauftragt, diese Fragen auf die zweite Kommissionssitzung hin genauer abzuklären und auszuführen.

Die Abklärungen der Sicherheitsdirektion zeigten, dass die Datenbearbeitungen für nicht personenbezogene Zwecke aus unterschiedlichen Gründen erfolgen: Bei der «Statistik», um über den Einzelfall hinaus generelle Zusammenhänge zu gewinnen; bei der «Planung», um Kosten und Folgen im Hinblick auf ein bestimmtes Ziel abzuschätzen; bei der «Forschung», um in einem bestimmten Wissensgebiet systematisch, planmässig und zielgerichtet mit wissenschaftlichen Methoden nach neuen Erkenntnissen zu suchen. Dabei könnte auf die beispielhafte Aufzählung für nicht personenbezogene Zwecke in Bst. a zwar verzichtet werden, der Klarheit halber (für die Rechtsanwenderinnen und -anwender) und aus Transparenzgründen (für die betroffenen Personen) wurde seitens der Sicherheitsdirektion jedoch empfohlen, die wichtigsten Beispiele im Gesetz aufzuführen. Weiter wurde erläutert, dass für die Unterscheidung von Bst. a und Bst. b wesentliche Gründe bestünden: So unterstehen staatliche Organe insbesondere dem Amtsgeheimnis und den Datenschutzbestimmungen für öffentliche Organe, sodass betreffend Datenempfang das Geheimnis-/Datenschutzniveau gehalten werde. Ausserdem gebe es – im Gegensatz zur Forschungsfreiheit – keine verfassungsmässige «Statistik-» oder «Planungsfreiheit», weshalb Personendaten Privaten gegenüber nur für den Zweck der Forschung bekannt gegeben werden dürften. Ferner solle damit vermieden werden, dass Private (natürliche und juristische Personen) ihre kommerziellen Angebote mit Personendaten von staatlichen Organen «unterfüttern» würden. Aus diesen Gründen solle bzw. könne Bst. b nicht in Bst. a integriert werden.

Die Kommission nahm von den Abklärungen Kenntnis. Auf Nachfrage wurde erläutert, dass unter «Private» in § 5c Abs. 1 Bst. b im Sinne des DSG auch juristische Personen fallen können.

#### **§ 5d Abs. 3 Verantwortung des Organs**

Es wurde die Frage gestellt, wie (mit welchen Instrumenten) ein Organ den Nachweis erbringen können müsse, dass es die Datenschutzbestimmungen einhalte. Es wurde erläutert, dass zur Erbringung dieses Nachweises, der auch heute schon erbracht werden müsse, verschiedene Dokumentationspflichten zur Verfügung stünden: bspw. das Führen eines Verzeichnisses der Bearbeitungstätigkeiten bei den Justiz- und Strafverfolgungsbehörden (§ 12) sowie die Datenschutz-Folgenabschätzung gemäss § 7b. Hinsichtlich des Nachweises würden periodische Überprüfungen stattfinden.

## § 6 Ausgelagertes Bearbeiten von Daten (neu: «Auftragsdatenbearbeitung»)

Die Kommission diskutierte die Möglichkeit, die Bearbeitung von Personendaten sowie die Auftragsdatenbearbeitung (Übertragung des Bearbeitens von Personendaten durch Dritte) neu auf das Hoheitsgebiet der Schweiz zu beschränken. Dabei wurde die Meinung vertreten, dass sich die Daten- bzw. Informationssicherheit nur mit einer entsprechenden Regelung erreichen lasse. Andererseits wurde bezweifelt, dass dies insbesondere mit Blick auf die technologische Entwicklung in Zukunft überhaupt praktikabel wäre bzw. allenfalls hohe Kosten nach sich ziehen würde. Bei dieser Diskussion wurde auch auf das Merkblatt «Cloud-spezifische Risiken und Massnahmen» von Privatim<sup>1</sup>, der Konferenz der schweizerischen Datenschutzbeauftragten, hingewiesen. Aufgrund der Diskussion wurde die Sicherheitsdirektion beauftragt, bei der Finanzdirektion (AIO) eine Stellungnahme zu einer möglichen Beschränkung der Bearbeitung/Auftragsdatenbearbeitung auf das Hoheitsgebiet der Schweiz einzuholen und verschiedene Praxisfragen zu klären. Zudem wurde der Auftrag erteilt, dazu auf die zweite Sitzung einen konkreten Textvorschlag auszuarbeiten.

Die Stellungnahme der Finanzdirektion (AIO) zeigte insbesondere, dass die Datenhaltung für den Kanton heute nur auf Schweizer Servern bzw. bei Schweizer Firmen erfolgt. Auch Auftragsdatenbearbeitungen seien bisher nur an Schweizer Firmen vergeben worden. Bei der Beschaffung von Cloud-Lösungen im offenen Verfahren (d.h. ab 250 000 Franken Auftragswert) sei es standardmässig nicht möglich, den Kreis der Anbietenden auf Schweizer Firmen zu beschränken. In Zukunft werde das Bedürfnis nach einer Auslagerung der Sicherheits-, Auslastungs-, Know-how- und Technologierisiken an dafür optimierte Unternehmen zunehmen. Nach Einschätzung der Finanzdirektion (AIO) bestünde bei einer wie in der Kommission besprochenen Beschränkung die Gefahr, dem Kanton die Möglichkeit zu nehmen, sinnvolle Angebote (Alternativen) in Anspruch zu nehmen, welche die bestehenden gesetzlichen und insbesondere IT-sicherheitstechnischen Anforderungen erfüllen. Auch die Interkantonale Zusammenarbeit und jene mit der EU könnten bei einer Beschränkung gefährdet sein. Im schlimmsten Fall wären teure, ineffiziente und sicherheitstechnisch unvorteilhaftere Umstellungen auf einheimische oder eigene Lösungen erforderlich, sofern solche (dann) überhaupt noch verfügbar seien. Dabei sei auch zu berücksichtigen, dass Schweizer Angebote nicht immer die bestmögliche Sicherheit gewähren würden. Ferner ergaben Abklärungen der Sicherheitsdirektion, dass Schulen (die Office 365 verwenden), Gemeinden (z.B. Stadt Zug) oder Dritte mit einer Leistungsvereinbarung bereits heute Datenbearbeitungen an Dritte (Cloud bei nicht Schweizer Firmen) auslagern, was bei einer entsprechenden Einschränkung nicht mehr möglich wäre. Folglich wurde seitens der Sicherheitsdirektion (in Übereinstimmung mit der Finanzdirektion [AIO]) empfohlen, von einer entsprechenden räumlichen Beschränkung (Textvorschlag gemäss Auftrag [§ 4 Abs. 1 f.]: «Personendaten dürfen einzig im Hoheitsgebiet der Schweiz bearbeitet werden») ganz abzusehen.

Als alternativer Textvorschlag wurde seitens der Sicherheitsdirektion folgende Ergänzung in § 4 Abs. 2 eingebracht: «Datenbearbeitungsstandorte in der Schweiz sind zu bevorzugen». Dies mit dem Hinweis, dass diese Bestimmung viel Interpretationsspielraum lasse und wenig verbindlich wäre.

Die Kommission nahm davon Kenntnis und diskutierte den im Abklärungsauftrag von der Sicherheitsdirektion auf Wunsch der Kommission vorgebrachten Gesetzestextvorschlag gemäss Auftrag. Dabei wurde seitens der Datenschutzstelle erklärt, dass diese Formulierung im Widerspruch zu Bundesgesetzen und § 10a (der die grenzüberschreitende Datenbekanntgabe regelt) stünde. Infolgedessen verzichtete die Kommission auf eine entsprechende Anpassung und

<sup>1</sup> [http://www.privatim.ch/wp-content/uploads/2019/02/privatim\\_Merkblatt\\_Cloud\\_v1.0\\_20190206.pdf](http://www.privatim.ch/wp-content/uploads/2019/02/privatim_Merkblatt_Cloud_v1.0_20190206.pdf).

einigte sich im Sinne des alternativen Textvorschlags darauf, ausdrücklich darauf hinzuweisen und festzuhalten, dass Datenbearbeitungsstandorte in der Schweiz auch in Zukunft analog der heutigen Praxis zu bevorzugen seien.

### § 7 Datensicherung (neu: «Informationssicherheit»)

Auf Nachfrage wurde erläutert, dass mit der vorgesehenen Löschung des Teilsatzes die Gesetzesgrundlage der Online-Verordnung aufgehoben werde. Für die Aufhebung der Online-Verordnung selber sei dann der Regierungsrat zuständig. Damit müssten Online-Zugriffe neu nicht mehr durch die Exekutive bewilligt werden, was für diese eine wesentliche Entlastung zur Folge habe. Datenbekanntgaben würden bereits heute regelmässig elektronisch erfolgen. Unterschiedliche Vorgaben gegenüber nicht elektronischen Datenbekanntgaben seien im digitalen Zeitalter überholt. Aus datenschutzrechtlicher Sicht sei die Aufhebung nicht von erheblicher Bedeutung, zumal die verantwortlichen Organe in entsprechenden Fällen ohnehin schon – und auch weiterhin – eine Datenschutz-Folgenabschätzung vornehmen müssten. Und auch die Datenschutzstelle bleibe involviert.

### § 7b Datenschutz-Folgenabschätzung

Es wurde die Frage gestellt, was eine Datenschutz-Folgenabschätzung bedeute. Darauf wurde erklärt, dass es darum gehe, mögliche Folgen einer geplanten Datenbearbeitung für die betroffenen Personen abzuschätzen und allenfalls geeignete flankierende Massnahmen vorzusehen. Es gehe um die Beurteilung, wie sich die Bearbeitung auf die betroffenen Personen konkret auswirke. Eine solche Abschätzung sei nicht bei jeder Personendatenbearbeitung erforderlich. Sie betreffe Datenbearbeitungen von einer grösseren Anzahl betroffener Personen und v.a. IT- und Digitalisierungsprojekte. So seien bspw. beim Gewaltschutz unter anderem Überlegungen bei der Einschränkung der Zugriffsrechte in eine neue Datenbank gemacht worden, um die Risiken zu minimieren. Diese Pflicht ergebe sich bereits aus dem geltenden DSG (vgl. § 19a). Bisher war es aber als Aufgabe der Datenschutzstelle aufgeführt, was jedoch nicht richtig ist, weil es sich um eine Pflicht der Organe handelt.

Ein Kommissionsmitglied erkundigte sich danach, was passiere, wenn eine Datenbearbeitung ohne vorgängige Datenschutz-Folgenabschätzung durchgeführt werde (eine solche aber hätte vorgenommen werden müssen). Es wurde erläutert, dass dies ein Verstoß gegen diese bzw. eine Datenschutzbestimmung darstellen würde. Wenn *vorsätzlich* Datenschutzbestimmungen verletzt würden, könnte dies gemäss § 24 Abs. 1 mit Busse bestraft werden. Davon zu unterscheiden ist eine Datenschutzverletzung gemäss § 7c, wenn Daten bspw. vernichtet oder bei einem Hackerangriff Unberechtigten zugänglich gemacht würden.

Weiter wurde diskutiert, ob § 7b zwingend wie vorgeschlagen ins DSG aufgenommen werden müsse oder ob die Bestimmung bzw. allenfalls Abs. 2 f. gestrichen werden könnte. In diesem Zusammenhang wurde auf Art. 27 Richtlinie (EU) 2016/680 sowie die SEV 108 verwiesen. Bei den Aufzählungen in § 7b handle es sich um Mindestanforderungen gemäss der Richtlinie (EU) 2016/680, wovon nicht abgewichen werden sollte. Es wurde vereinbart, den Kommissionsmitgliedern die Richtlinie (EU) 2016/680 sowie die SEV 108 elektronisch zuzustellen und auf die Bestimmung anlässlich der nächsten Sitzung nochmals zu sprechen zu kommen.

An der zweiten Kommissionssitzung wurde nochmals darauf hingewiesen, dass sich die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung bereits heute aus § 19a ergebe und den europäischen Vorgaben von Art. 27 Richtlinie (EU) 2016/680 und Art. 10 Abs. 2 SEV 108 entspreche. Zudem diene die Angabe der Mindestanforderungen letztlich auch den Organen, welche sich an diesen orientieren könnten. So hätten die meisten Gemeinden in der externen Vernehmlassung gar explizit weitere Inhaltsumschreibungen und Konkretisierungen gewünscht. Diesem Anliegen solle im Rahmen der Revision der Datenschutzverordnung Rechnung getragen werden.

Hinsichtlich der diesbezüglichen Befürchtungen der gemeindlichen Einwohnerkontrollen informierte der Kommissionspräsident darüber, dass auf Initiative der Sicherheitsdirektion zwischen der ersten und der zweiten Kommissionssitzung ein Austausch zwischen Mitgliedern der Sicherheitsdirektion, der Datenschutzstelle und dem Kommissionspräsidenten mit Mitgliedern der Einwohnerkontrollen der Stadt Zug und Cham stattfand. Dabei konnten Fragen zur Gemeindepraxis geklärt und Auswirkungen der Änderungen des Datenschutzgesetzes auf die Einwohnerkontrollen konkretisiert werden. Hinsichtlich § 7b befürchteten die Einwohnerkontrollen konkret einen Mehraufwand durch die Datenschutz-Folgeabschätzung.

### **§ 7b Abs. 3 Datenschutz-Folgenabschätzung / § 7c Abs. 1 Meldung von Datenschutzverletzungen**

Die Kommission diskutierte, ob in den genannten Bestimmungen wie vom Regierungsrat beantragt von einem «Risiko für die Grundrechte» oder von einem «Risiko einer Verletzung der Grundrechte» gesprochen werden soll. Es wurde ausgeführt, dass richtigerweise von einem Risiko für die Grundrechte und nicht von einem Risiko einer Verletzung der Grundrechte gesprochen werden sollte. Es gehe um eine vertiefte Risikoanalyse. Falls eine Verletzung der Grundrechte im Raum stünde, wäre es schon zu spät. In der Folge erfolgte der:

Antrag. «Risiko für die Grundrechte» in § 7b Abs. 3 und § 7c Abs. 1 mit «Risiko einer Verletzung der Grundrechte» zu ersetzen.

Die Kommission stimmte dem Antrag mit 11:4 Stimmen zu und beschloss folgende Änderungen:

#### **§ 7b Abs. 3**

Das Organ legt der Datenschutzstelle Vorhaben zur Bearbeitung von Personendaten, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Personendaten zu einem hohen Risiko ~~für die~~ **einer Verletzung der** Grundrechte der betroffenen Personen führen, zur Stellungnahme vor.

#### **§ 7c Abs. 1**

Das Organ meldet der Datenschutzstelle unverzüglich eine Datenschutzverletzung, es sei denn, diese führt voraussichtlich nicht zu einem Risiko ~~für die~~ **einer Verletzung der** Grundrechte der betroffenen Personen.

### **§ 7c Meldung von Datenschutzverletzungen**

Es wurde die Frage gestellt, ob die «Verletzung» von § 7b (Datenschutz-Folgenabschätzung) als gemäss § 7c zu meldende Datenschutzverletzung ins Gesetz aufgenommen werden müsste. Es wurde erörtert, dass zwischen der Datenschutzverletzung gemäss § 7c und einer Verletzung einer bzw. dem Verstoss gegen eine Datenschutzbestimmung (geregelt in § 24) zu unterscheiden sei. § 7c erfasse Datenschutzverletzungen, nicht aber Verstösse gegen Datenschutzbestimmungen. Ein Verstoss gegen § 7b stelle mithin keine zu meldende Datenschutzverletzung im Sinne von § 7c dar.

### **§ 9 Abs. 3 Bst. b Sperrung der Bekanntgabe**

Die Kommission diskutierte die Praxis bzw. Pflicht eines Organs, der betroffenen Person bei Verweigerung oder Aufhebung einer Sperrung der Bekanntgabe im Sinne von § 9 Abs. 3 Bst. b vorab Gelegenheit zur Stellungnahme zu geben. Gemäss dem Antrag des Regierungsrates soll den betroffenen Personen in diesen Fällen künftig «immer» Gelegenheit zur Stellungnahme gegeben werden (Streichung von «wenn möglich»). Einzelne Kommissionsmitglieder befürchteten, dass eine solche Einholung einer Stellungnahme einen Mehraufwand für die betroffenen



Organe bedeuten würde. Als Beispiel wurde eine entsprechende Auskunftserteilung beim Strassenverkehrsamt (STVA) diskutiert. In diesem Zusammenhang wurde die Sicherheitsdirektion beauftragt, beim Strassenverkehrsamt abzuklären, wie die dortige diesbezügliche Praxis aussieht und wie häufig Sperrungen nach § 9 Abs. 3 Bst. b verweigert/aufgehoben werden.

Die Abklärungen der Sicherheitsdirektion zeigten, dass sich die Bekanntgaben von Führer- und Fahrzeugdaten aus den Registern bzw. dem Informationssystem Verkehrszulassung (IVZ) spezialrechtlich, nämlich nach dem Strassenverkehrsgesetz vom 19. Dezember 1958 (SVG, SR 741.01) sowie der Verordnung über das IVZ vom 30. November 2018 (IVZV, SR 741.58) richten. Bei Eingang eines entsprechenden Gesuchs prüfe das STVA nach sorgfältiger Abwägung aufgrund der eingereichten Beweismittel jeweils, ob die Auskunft erteilt werden könne. Dabei sehe das Spezialrecht beim STVA keine Pflicht zur Einholung einer Vorab-Stellungnahme (analog § 9 Abs. 3 Bst. b) vor. Praxisgemäss verzichte das STVA denn auch auf eine solche. Dabei gelte es zu berücksichtigen, dass sich eine Sperrung gemäss SVG lediglich auf die öffentliche Bekanntgabe im Internet beziehe. Im Gegensatz dazu beziehe sich § 9 auf jede Form der Bekanntgabe von Personendaten an Private.

Es wurde in diesem Zusammenhang auch nochmals auf den Austausch mit den Einwohnerkontrollen der Stadt Zug und Cham hingewiesen. Gemäss Auskunft beider Einwohnerkontrollen würden lediglich wenige Anfragen gesperrte Daten betreffen. Es werde aber aufgrund der neu vorgesehenen Informationspflicht (§ 9 Abs. 1a) in Zukunft mit mehr Anfragen zu gesperrten Daten gerechnet. In welchen Fällen Gelegenheit zur Stellungnahme gegeben worden sei (Umsetzung «wenn möglich»), sei eine Auslegungsfrage, wobei die Einwohnerkontrollen die Beibehaltung von «wenn möglich» bevorzugen würden, da in der Praxis nicht immer eine Stellungnahme eingeholt werden könne (z. Bsp., wenn Personen nicht auffindbar sind). In der folgenden Kommissionsdiskussion wurde darauf hingewiesen, dass eine Stellungnahme nur eingeholt werden kann, wenn eine Person auch erreicht werden könne (dies gelte heute und sei auch in Zukunft vorgesehen). Falls jemand nicht erreicht werden könne, müsse die zuständige Behörde eine Interessensabwägung machen und entsprechend entscheiden. Insofern führe die Streichung von «wenn möglich» nicht zu einer Änderung der heutigen Praxis. Auf Nachfrage hinsichtlich des konkreten Vorgehens und allfälliger Fristen für die Einholung der Stellungnahmen und die nötigen Entscheide wurde erläutert, dass im DSG keine Frist vorgesehen sei. Diesbezüglich wie auch im Allgemeinen könne aber an das Gesetz über den Rechtsschutz in Verwaltungssachen vom 1. April 1976 (Verwaltungsrechtspflegegesetz, VRG; BGS 162.1) angelehnt werden.

Im Zusammenhang mit der Informationspflicht der Organe (§ 9 Abs. 1a) wurde auf einen allfälligen Absprachebedarf zwischen dem Amt für Migration (AFM) und den Einwohnerkontrollen bei ausländischen Staatsangehörigen hingewiesen und die Frage aufgeworfen, ob dies in der Datensicherheitsverordnung vom 16. Januar 2007 (DSV; BGS 157.12) thematisiert werde. Es wurde erklärt, dass die DSV lediglich Bestimmungen im Zusammenhang mit der Gewährleistung der Sicherheit von Personendaten beinhalte. Es handle sich bei der DSV mithin nicht um eine eigentliche Ausführungsgesetzgebung zum DSG, weshalb auch ein allfälliger Absprachebedarf zwischen dem AFM und der Einwohnerkontrollen in der DSV nicht thematisiert werde. Der diesbezügliche Absprachebedarf sei des Weiteren eine operative Frage und gehöre daher nicht ins Gesetz.

### **§ 12 Anmeldung und Register (neu: «Verzeichnis der Bearbeitungstätigkeiten»)**

Es wurde die Frage gestellt, weshalb neu ein «Verzeichnis der Bearbeitungstätigkeiten» anstelle des «Registers der Datensammlungen» geführt und veröffentlicht werden soll. Es wurde erklärt, dass der Begriff «Datensammlung» veraltet sei (weshalb diese Begriffsdefinition in § 2 Abs. 1 Bst. e auch aufgehoben werden soll). Inhaltlich handle es sich um dasselbe Instrument,

jedoch sei der Inhalt der Verzeichnisse der Bearbeitungstätigkeiten wesentlich reduziert worden (vgl. § 12 Abs. 3).

Weiter wurde diskutiert, ob es notwendig sei, die Bearbeitungstätigkeiten bzw. Datensammlungen zu veröffentlichen oder ob diese auch lediglich «auf Anfrage» hin bekannt gegeben werden könnten. Mit Verweis auf die europäischen Vorgaben wurde erklärt, dass eine Bekanntgabe auf Anfrage hin zwar rechtlich zulässig, aber schon angesichts des Transparenzverlusts wenig sinnvoll wäre. Ausserdem verursache die Veröffentlichung für die Organe vermutlich keinen allzu grossen Aufwand. Ein Kommissionsmitglied hielt fest, dass die dauernde Veröffentlichung dennoch unnötig sei.

Ferner wurde der Antrag des Regierungsrates besprochen, dass die Pflicht zum Führen eines solchen Verzeichnisses neu nur noch die Justiz- und Strafverfolgungsbehörden (statt wie bisher alle Organe) treffen soll (Einschränkung). Es wurde erwogen, dass aufgrund der neuen Formulierung weniger Aufwand für die Gemeinden anfallen würde. Dem wurde entgegengehalten, dass die Organe trotzdem jederzeit innert nützlicher Frist Auskunft über ihre Datenbearbeitungstätigkeiten geben können müssten. Lediglich die Art und Weise, wie sie dies tun, sei ihnen freigestellt. Ausserdem gehe es auch um Transparenz; die beantragte Variante des Regierungsrates bedeute im Vergleich zu heute einen Transparenzverlust.

Zurzeit würden im ganzen Kanton gemäss aktuellem Datenregister (abrufbar unter <http://register.datenschutz-zug.ch/c050016/zg/datenregister.nsf/xSearch.xsp> [Stand 21. Oktober 2019]) 1451 verschiedene Datensammlungen und bei den Justiz- und Strafverfolgungsbehörden total 26 Datensammlungen bestehen: 8 bei der ZUPO, 1 bei der Staatsanwaltschaft, 6 beim Obergericht, 4 beim Kantonsgericht und 7 beim Strafgericht. Mit der vorgeschlagenen Variante würden im Internet neu nur noch diejenigen der Justiz- und Strafverfolgungsbehörden bekannt gemacht werden. Zudem wurde darauf hingewiesen, dass – sollten wie bisher – alle Organe Verzeichnisse führen, dafür ein neues Tool (zentrales Erfassungs- und Publikationssystem) zur Verfügung gestellt werden müsste. Dessen Kosten würden gemäss ersten Abklärungen einmalig ca. 75 000 Franken (Maximalbetrag) und danach jährlich ca. 20 000 Franken betragen.

In der Diskussion wurden folgende Anträge gestellt, über die nacheinander abgestimmt wurde:

1. Antrag, dass die Justiz- und Strafverfolgungsbehörden das Verzeichnis ihrer Bearbeitungstätigkeiten nur noch «auf Anfrage» hin bekannt geben (statt «dieses veröffentlichen»).

Die Kommission lehnte den Antrag mit 9:5 Stimmen ab.

2. Antrag, die Pflicht zur Führung eines Verzeichnisses über die Bearbeitungstätigkeiten für alle kantonalen und gemeindlichen Organe beizubehalten statt neu auf die Justiz- und Strafverfolgungsbehörden zu beschränken.

Die Kommission lehnte den Antrag mit 8:6 Stimmen ab.

## § 20 Befugnisse

Die Kommission diskutierte, ob der Datenschutzstelle die Kompetenz zukommen soll, Empfehlungen an Organe als Verfügungen zu erlassen. Dies würde eine Stärkung der Datenschutzstelle bedeuten. Ihr Entscheid wäre dann aber nach wie vor gerichtlich anfecht- bzw. überprüfbar. Die Verfügungskompetenz der Datenschutzstelle werde jeweils im Rahmen von Schengen Follow-up Prozessen thematisiert (analysiert), wobei die Wichtigkeit dieser Kompetenz betont worden sei. Auch der Kanton Zug könnte in diesem Rahmen «überprüft» und bei Nichtübernahme der im europäischen Recht vorgesehenen Verfügungskompetenz gerügt werden. Sollte der Datenschutzstelle keine Verfügungskompetenz eingeräumt werden, würde die Gefahr bestehen, dass der Schweiz bzw. dem Kanton Zug kein angemessenes Datenschutzniveau bescheinigt und der Zugriff auf Schengen-Datenbanken eingeschränkt werden würde. Damit

würde letztlich auch ein Nachteil für Unternehmen entstehen. Die Frage, ob die Datenschutzstelle gegen einen Entscheid der heute zuständigen Behörde auch schon Beschwerde ergriffen habe, verneinte die Datenschutzstelle mit dem Hinweis, dass ihre Empfehlungen bislang immer umgesetzt worden seien. Das fachliche Wissen fehle dem Regierungsrat und den Gemeinden regelmässig, weshalb es sinnvoll sei, dass die Datenschutzstelle Verfügungsmöglichkeit habe. Ansonsten müsse ein Umweg über den Regierungsrat oder die Gemeinden erfolgen, welcher für diese einen Mehraufwand bedeute. Dagegen wurde argumentiert, dass die Datenschutzstelle unabhängig und keine Verwaltungsstelle sei, weshalb eine solche Kompetenz auch im Rahmen der Gewaltenteilung und Rechtsweggarantie als nicht zulässig erachtet werde. Darauf wurde erwidert, dass die Verfügungskompetenz auch delegiert werden könne. Auf dieser Diskussionsgrundlage erfolgte der

Antrag, dass der Datenschutzstelle die Kompetenz zum Verfügungserlass (Erlass einer Empfehlung als Verfügung, Anordnung vorsorglicher Massnahmen) zugestanden werden soll.

Die Kommission lehnte den Antrag mit 9:5 Stimmen ab.

## **6. Detailberatung Fremdänderungen**

### **§ 57f<sup>bis</sup> Gemeindegesetz**

Bei den Fremdänderungen führte die Anpassung des Gemeindegesetzes zu eingehenden Diskussionen. Dabei wurde anhand einer Spezialsynopse zunächst darauf hingewiesen, dass §§ 8, 13 Abs. 1 Bst. c und 17 Abs. 3 DSG (bisher) neu in § 57f<sup>bis</sup> GG zusammengefasst werden. Die Regelung von Datenbekanntgaben aus den gemeindlichen Einwohnerregistern im DSG sei systemfremd, da es sich um «materielles» Datenschutzrecht handle. Neu sei die Pflicht, dass die Einwohnerkontrollen Auskunft über jede Auskunftserteilung (insbesondere zusätzlich auch über einfache Einzelauskünfte sowie Sammelauskünfte) erteilen müssten (§ 57f<sup>bis</sup> Abs. 3 GG; vorher § 13 Abs. 1 Bst. c DSG).

Hinsichtlich der diesbezüglichen Praxis der Gemeinden wies der Kommissionspräsident auf den Austausch mit den Einwohnerkontrollen der Stadt Zug und Cham hin, bei welchem auch diese Bestimmung thematisiert worden war (vgl. vorstehend zu § 7b und zu § 9 Abs. 3 Bst. b). Ein Praxis-Vergleich mit anderen Kantonen habe zudem gezeigt, dass diese vielfach nur schriftlichen Anfragen bzw. Auskünfte zuließen, einen Interessennachweis verlangten und für die Auskunftserteilung Gebühren erheben würden. Hingegen seien im Kanton Zug aktuell sogenannte einfache Einzelauskünfte auch mündlich möglich. Zudem müsse lediglich bei erweiterten Auskünften ein schriftlicher Interessennachweis vorliegen und Gebühren könnten nur bei Sammelauskünften erhoben werden. Eigenen Angaben zufolge verzichte aber sowohl die Stadt Zug wie Cham darauf, in diesen Fällen Gebühren zu erheben. Dass um Auskunft über die Bekanntgabe von Daten ersucht werde, passiere höchst selten (in der Stadt Zug geschätzt alle drei in Cham alle zehn Jahre einmal). Mit den vom Regierungsrat vorgesehenen Änderungen müssten neu insbesondere auch mündliche Einzelauskünfte im System erfasst werden. Dies würde gemäss Auskunft der Einwohnerkontrollen einen geschätzten Mehraufwand von rund drei Minuten pro Telefon bedeuten, da die jeweiligen Informationen im System erfasst werden müssten. Bislang seien lediglich alle schriftlichen Anfragen im System gespeichert worden. Am Austausch mit den beiden Einwohnerkontrollen seien verschiedene Varianten diskutiert worden: (1) Der Antrag des Regierungsrates, wonach neu über jede Auskunftserteilung Auskunft gegeben werden sollte; (2) Die Beibehaltung der geltenden Fassung (Wunsch der Einwohnerkontrollen); Und (3), dass (analog der Praxis in anderen Kantonen) neu nur noch schriftliche Einzelauskünfte zugelassen würden. Gemäss den Einwohnerkontrollen sollten den Gemeinden, wenn diese nun alle Anfragen verzeichnen müssten, auch die Option für eine allfällige Gebührenerhebung im Gesetz eingeräumt werden.

In diesem Zusammenhang wurde in der Kommission darauf hingewiesen, dass die heutige Bestimmung zur Datenbekanntgabe den Materialien zufolge (erst) in den damaligen Kommissionsarbeiten aufgenommen und bewusst so «liberal» formuliert worden sei. Entscheidend seien die Gedanken gewesen, dass Basisinformationen einfach zugänglich sein sollten und die Daten einfach gesperrt werden könnten. Wenn bei einer Anfrage festgestellt werde, dass eine Datensperre bestehe, müsse nach § 9 DSG verfahren werden.

Weiter wurde diskutiert, was genau unter dem Begriff der «Sammelauskunft» gemäss § 57f<sup>bis</sup> Abs. 2 Bst. c GG zu verstehen ist und ob hierfür auch noch zukünftig Gebühren erhoben werden sollten. Dabei wurde zunächst erläutert, dass diesbezüglich das Stimmregister vom Einwohnerregister zu unterscheiden sei und Sammelauskünfte gemäss § 8 DSG bzw. neu § 57f<sup>bis</sup> GG sich nur auf das Einwohnerregister beziehen würden. Sodann wurde festgehalten, dass Sammelauskünfte meist durch Vereine oder politische Parteien angefragt würden. Dass diese dann Gebühren bezahlen müssten, sei nicht der richtige Ansatz. Zudem entstünden für die Gemeinden durch Sammelauskünfte im Gegensatz zu früher mit der heutigen IT-Infrastruktur keine grossen Mehrkosten.

Gestützt auf die vorangehende Diskussion folgte der

Antrag, Abs. 4, wonach für Sammelauskünfte Gebühren erhoben werden können, aufzuheben bzw. zu löschen.

Die Kommission stimmte dem Antrag mit 13:0 Stimmen bei einer Enthaltung zu. Dies hat gleichzeitig eine Anpassung im ehemaligen Abs. 5 (neu Abs. 4) zur Folge: dieser soll neu auf Abs. 1 bis 3 (statt wie bis anhin auf Abs. 1 bis 4) verweisen.

### **§ 6 Abs. 2 Bst. g Videoüberwachungsgesetz / § 69 Abs. 2 Gerichtsorganisationsgesetz**

Nach der Überweisung der Gesetzesvorlage vom Regierungsrat an den Kantonsrat wurde festgestellt, dass in § 6 Abs. 2 Bst. g Gesetz über die Videoüberwachung im öffentlichen und im öffentlich zugänglichen Raum (Videoüberwachungsgesetz, VideoG; BGS 159.1) und in § 69 Abs. 2 Gesetz über die Organisation der Zivil- und Strafrechtspflege (Gerichtsorganisationsgesetz, GOG; BGS 161.1) noch der Begriff «Datensicherheit» anstelle von «Informationssicherheit» verwendet wird. Es wurde darauf hingewiesen, dass der veraltete Begriff «Datensicherheit» im Titel von § 7 DSG durch den geläufigen Begriff «Informationssicherheit» ersetzt wird. Folglich sollten auch die zwei (nachträglich festgestellten) Begriffsanpassungen als weitere Fremdänderungen in die laufende Revision aufgenommen werden. Der Kommissionpräsident stellte in der Folge die entsprechenden Anträge auf Anpassung von § 6 Abs. 2 Bst. g VideoG und § 69 Abs. 2 GOG.

Die Kommission stimmte den Anträgen nacheinander stillschweigend zu und beschloss folgende Fremdänderungen:

#### **§ 6 Abs. 2 Bst. g VideoG**

mit welchen Massnahmen für die ~~Datensicherheit~~**Informationssicherheit** bei der Aufzeichnung, Bearbeitung, Auswertung sowie Vernichtung der Daten gesorgt wird;

#### **§ 69 Abs. 2 GOG**

Die Informatikausstattung trägt den besonderen betrieblichen Bedürfnissen Rechnung, insbesondere den erhöhten Anforderungen an die Übermittlungs- und ~~Datensicherheit~~**Informationssicherheit**.

## **7. Schlussabstimmung**

Die Kommission stimmte der Vorlage mit den Änderungen der vorberatenden Kommission in der Schlussabstimmung mit 10:3 Stimmen bei einer Enthaltung zu.

## **8. Kommissionsantrag**

Die vorberatende Kommission beantragt dem Kantonsrat

1. mit 12:3 Stimmen auf die Vorlage 2985.2 – 16095 einzutreten;
2. mit 10:3 Stimmen bei einer Enthaltung der Vorlage mit den Änderungen der vorberatenden Kommission zuzustimmen.

Steinhausen, 21. Oktober 2019

Mit vorzüglicher Hochachtung  
Im Namen der vorberatenden Kommission

Der Präsident: Anastas Odermatt

Beilage:

- Synopse

### **Kommissionsmitglieder:**

Odermatt Anastas, Steinhausen, Präsident  
Alaj Drin, Cham  
Andermatt Urs, Baar  
Balmer Kurt, Risch  
Brunner Philip C., Zug  
Dittli Laura, Oberägeri  
Hürlimann Andreas, Steinhausen  
Küng Hans, Baar  
Leemann Manuela, Zug  
Moos Adrian, Zug  
Muheim Quick Petra, Cham  
Rust Peter, Walchwil  
Schuler Hubert, Hünenberg  
Soltermann Claus, Cham  
Werner Thomas, Unterägeri