Vernehmlassungsverfahren

2. Februar 2018

Aktualisierung des kantonalen Datenschutzrechtes

Erläuterungen zum Vernehmlassungsentwurf

Kanton Luzern | www.lu.ch

Zusammenfassung

Die gesetzgeberischen Tätigkeiten von Europarat und Europäischer Union im Bereich des Datenschutzes verlangen von Bund und Kantonen Anpassungen ihrer Datenschutzgesetze. Die Vorlage sieht Ergänzungen und Präzisierungen verschiedener Bestimmungen des geltenden Gesetzes vor, aber auch Vereinfachungen. Aktualisiert wird der Katalog der besonders schützenswerten Personendaten: Darin aufgenommen werden die genetischen und biometrischen Daten. Gemäss der Vorlage soll auf den Schutz der Daten von juristischen Personen verzichtet werden, wodurch die Einheitlichkeit mit der vorgesehenen bundesrechtlichen Regelung geschaffen wird. Die Daten juristischer Personen, das sind insbesondere die Gesellschaften des Handelsrechts wie die Aktiengesellschaften, sind durch andere Erlasse genügend geschützt. Die Informations- und Meldepflichten der öffentlichen Organe und die Rechte der betroffenen Personen auf Auskunft über die bearbeiteten Daten werden in den Gesetzesbestimmungen klarer definiert. Bei gewissen Datenbearbeitungen werden die dem Gesetz unterstellten öffentlichen Organe verpflichtet, Datenschutz-Folgeabschätzungen zu erstellen. Die Gerichts- und Strafverfolgungsbehörden haben innerhalb ihrer Organisationseinheiten einen Datenschutzberater oder eine Datenschutzberaterin zu ernennen. Verzichtet wird auf das Register der Datensammlungen. Für den Bereich der Strafverfolgung ist indes ein Register der Datenbearbeitungen weiterhin nötig. Ein wichtiger Punkt der Revision ist die Stellung und Unabhängigkeit der Aufsichtsstelle im Bereich des Datenschutzes. In Übereinstimmung mit dem erhöhten europäischen Standard werden Verfügungsbefugnisse des oder der Beauftragten für den Datenschutz festgelegt und sind Wählbarkeitsvoraussetzungen und eine Wahl auf Amtsdauer durch den Kantonsrat vorgesehen. Bisher hat der Kanton auch die Aufsicht über den Datenschutz der Gemeinden und der übrigen dem Gesetz unterstellten Gemeinwesen finanziert. Neu sollen Kanton und Gemeinden die Aufsichtsstelle gemeinsam finanzieren.

Inhaltsverzeichnis

1 Ausgangslage

Gemäss der Bundesverfassung vom 18. April 1999 (SR 101) hat jede Person Anspruch auf Schutz der Privatsphäre und insbesondere auf den Schutz vor Missbrauch ihrer persönlichen Daten (Art. 13 BV). Die Gesetzgebung im Datenschutz ist in der Schweiz zwischen Bund und Kantonen aufgeteilt. Das Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1) gilt für private Personen und die Bundesorgane. Die Bundeskompetenz stützt sich auf die Verfassungsbestimmungen über die Ausübung privatwirtschaftlicher Tätigkeiten und über die Gesetzgebungen zum Zivilrecht und zum Konsumentenschutz sowie auf die allgemeine Kompetenz zur Organisation der Bundesbehörden (vgl. Art. 95, 97, 122 und 173 BV). Für die Organe von Kanton und Gemeinden gelten die entsprechenden kantonalen Datenschutzgesetze. Neben die eidgenössischen und kantonalen Datenschutzerlasse treten bereichsspezifische Datenschutzvorschriften des eidgenössischen und kantonalen Rechts, beispielsweise über die Bekanntgabe und die Löschung von Personendaten.

Die Datenschutzgesetzgebung von Bund wie Kantonen muss der Rechtsentwicklung im Völkerrecht und der europarechtlichen Entwicklung Rechnung tragen. Zum einen ist die Schweiz Mitglied des Europarates. Am 2. Oktober 1997 hat sie das Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten ratifiziert (SR 0.235.1). Dieses Übereinkommen wurde durch das Zusatzprotokoll vom 8. November 2001 bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung ergänzt (SR 0.235.11), welches die Schweiz am 20. Dezember 2007 ratifiziert hat. Im Jahr 2011 leitete der Europarat ein Verfahren zur Revision des Übereinkommens und seines Zusatzprotokolls ein. Der Revisionsvorschlag liegt in einer bereinigten Version vor. Er bedarf indes noch der definitiven Beschlussfassung.

Zum andern ist die Entwicklung in der Europäischen Union zu berücksichtigen. Am 27. April 2016 haben das Europäische Parlament und der Rat der Europäischen Union eine Reform der Datenschutzgesetzgebung verabschiedet. Die Reform umfasst zwei Rechtsakte: Die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr. Für Bund und Kantone von Bedeutung ist die EU-Richtlinie. Aufgrund des Schengen-Assoziierungsabkommens (d.h. dem Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, SR 0.362.31) muss die EU-Richtlinie umgesetzt werden. Die Beratungen der EU-Mitgliedstaaten mit den vier assoziierten Schengen-Mitgliedern (Norwegen, Island, Schweiz, Liechtenstein) fand in den Jahren 2012–2015 statt. Die EU-Kommission hat am 1. August 2016 die Richtlinie der Schweiz als schengenrelevant notifiziert. Zusätzlich hat die Europäische Union die Datenschutz-Grundverordnung 2016/679 erlassen, die ab dem 25. Mai 2018 gilt. Formell gilt dieser Erlass für die Eidgenossenschaft zwar nicht, jedoch entscheidet die Europäische Kommission gestützt darauf, ob Drittstaaten (wie die Schweiz) ein angemessenes Datenschutzniveau haben. Nur dann ist der Datentransfer aus der EU in die Schweiz ohne zusätzliche Massnahmen möglich. Auf diesen Angemessenheitsbeschluss ist vor allem die Wirtschaft angewiesen. Das angemessene Datenschutzniveau wird durch die Europäische Kommission periodisch überprüft. Auch hinsichtlich der Schengen-Verpflichtungen finden regelmässige Überprüfungen statt.

Ende 2016 hat der Bund den Vorentwurf zu einer Totalrevision des Bundesgesetzes über den Datenschutz in die Vernehmlassung gegeben. Der Bundesrat beabsichtigt, das eidgenössische Datenschutzgesetz anzupassen, weil er damit die europäischen Rechtsentwicklungen aufnehmen will, aber auch weil er aufgrund einer Gesetzesevaluation Anpassungsbedarf festgestellt hat. Am 15. September 2017 hat der Bundesrat die Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz samt dem Bundesbeschluss über die Genehmigung des Notenaustausches betreffend die Übernahme der Richtlinie verabschiedet (Bundesblatt 2017 S. 6941). Darin finden sich auch weitere

Ausführungen zur Ausgangslage auf der internationalen Ebene (Kap. 1.2 und 2 der Botschaft des Bundesrates).

Wie der Bund müssen auch die Kantone ihre Datenschutzerlasse mindestens im Hinblick auf die völker- und europarechtlichen Rechtsentwicklungen hin überprüfen. Entsprechend den Verpflichtungen im Rahmen des Schengen-Assoziierungsabkommens sollten die Anforderungen der erwähnten EU-Richtlinie erfüllt werden. Die neue Europaratskonvention wird für das kantonale Datenschutzrecht massgebend sein, wenn die Konvention von der Schweiz ratifiziert ist. Ausserdem sollten die Datenschutzgesetzgebungen von Bund und Kantonen zumindest in den Grundzügen weiterhin aufeinander abgestimmt sein. Zu diesem Zweck hat die Konferenz der Kantonsregierungen den Kantonen einen Leitfaden zukommen lassen. Das Justiz- und Sicherheitsdepartement hat aufgrund dieses Leitfadens und der kürzlich veröffentlichten Botschaft des Bundesrates zur Totalrevision des eidgenössischen Datenschutzgesetzes die Änderungen des kantonalen Datenschutzgesetzes erarbeitet und dabei den kantonalen Beauftragten für den Datenschutz einbezogen. Vorgesehen ist eine Teilrevision des geltenden Datenschutzgesetzes vom 2. Juli 1990 (SRL Nr. 38).

2 Grundzüge der Revision

2.1 Umfang des Datenschutzes

2.1.1 Geltung des Datenschutzgesetzes

Die eingangs erwähnten neuen völker- und europarechtlichen Rechtsgrundlagen verlangen, dass die Regelungen über den Datenschutz möglichst für jedes Bearbeiten von Personendaten durch kantonale oder kommunale Organe, unabhängig von den angewandten Mitteln und Verfahren, Anwendung finden. Die §§ 1–3 des geltenden Datenschutzgesetzes sind deshalb in dieser Hinsicht zu überprüfen und Ausnahmen nur unter engen Voraussetzungen vorzusehen. Damit soll der Erlass in den Gemeinwesen und ihrer Behörden und Verwaltungseinheiten allgemein anwendbar sein. Diese notwendigen formellen Anpassungen haben jedoch weniger Konsequenzen, als es zunächst scheint, regeln doch neben dem allgemeinen Datenschutzgesetz mittlerweile zahlreiche bereichsspezifische Normen den Umgang mit Daten und Informationen (z.B. sind in Verfahren der Einbürgerung die besonderen Bestimmungen der Bürgerrechtsgesetzgebung anwendbar bei Entscheiden von Gemeindeversammlungen oder -parlamenten wie von Verwaltungsbehörden, vgl. §§ 33 und 34 Kantonales Bürgerrechtsgesetz vom 15. Mai 2017, SRL Nr. 2).

2.1.2 Beschränkung auf natürliche Personen

Aus der Umschreibung des Begriffs der Personendaten in § 2 Absatz 1 des geltenden Datenschutzgesetzes ergibt sich, dass dieses Gesetz nicht nur dem Schutz von *natürlichen Personen* vor unbefugtem Bearbeiten ihrer Daten durch öffentliche Organe, sondern auch dem Schutz von *juristischen Personen* und *Personengesellschaften des Handelsrechts* dient. Das Europaratsübereinkommen, die EU-Richtlinie, die meisten europäischen Staaten und die Botschaft des Bundesrates zur Totalrevision des eidgenössischen Datenschutzgesetzes sehen den Schutz von juristischen Personen nicht oder nicht mehr vor. Die europäischen Erlasse und das neue Bundesgesetz sollen lediglich auf die Daten von natürlichen Personen anwendbar sein. Nach diesem Verständnis sind die im Datenschutzrecht verankerten Rechte höchstpersönliche Rechte des Menschen. Auch ergibt sich aus der Praxis kein Bedürfnis für ein spezifisches Datenschutzrecht für juristische Personen, sind diese doch durch andere, gesamtschweizerische Regelwerke umfassend geschützt: Bei Persönlichkeitsverletzungen, soweit sie keine physische Existenz voraussetzen, kommen die Bestimmungen des Schweizerische Zivilgesetzbuches (SR 210) zum Tragen, beispielsweise bei Rufschädigung eines Unternehmens. Bei Vertragsverletzungen (z.B. Vertraulichkeitsabreden) ist das Obligationenrecht (SR 220) massgebend. Vor Verletzungen von Berufs-, Geschäfts- und Fabrikationsgeheimnissen und bei zahlreichen weiteren Tatbeständen von Bedeutung für die Wirtschaftsunternehmen schützt das Schweizerische Strafgesetzbuch (SR 311) vor Datenmissbrauch und im Wirtschaftsverkehr gelten ausserdem die Bestimmungen des Urheber- und Wettbewerbsrechts. Es wird daher auch für das kantonale Datenschutzgesetz vorgeschlagen, auf den Schutz der Daten juristischer Personen zu verzichten und das Gesetz auf den Schutz der Da-

ten von natürlichen Personen zu beschränken. Dadurch soll eine Einheitlichkeit mit der bundesrechtlichen Regelung geschaffen werden. Weitere Ausführungen können den Erläuterungen zum DSG-Entwurf in der Botschaft des Bundesrates vom 15. September 2017 entnommen werden (dort in Kap. 9.1.2 zu Art. 2 Abs. 2; in rechtlicher Hinsicht vgl. Drechsler, Plädoyer für die Abschaffung des Datenschutzes für juristische Personen, AJP 2016 S. 80). Der Bund sieht überhaupt keine Anwendung des eidgenössischen Datenschutzgesetzes mehr für die Daten von juristischen Personen vor, beabsichtigt jedoch im Regierungs- und Verwaltungsorganisationsgesetz eine separate Grundlage zur Bearbeitung von Daten von juristischen Personen zu schaffen. Entsprechend sieht auch der vorliegende Entwurf eine Ergänzung des kantonalen Organisationsgesetzes vom 13. März 1995 (SRL Nr. 20) vor.

2.1.3 Aktualisierung des Katalogs der besonders schützenswerten Daten

In Übereinstimmung mit dem europäischen Recht und dem DSG-Entwurf des Bundes soll der Katalog der besonders schützenswerten Daten aktualisiert werden. Besonders schützenswerte Daten sind besonders persönlichkeitsnahe Daten, deren Verwendung insbesondere wegen ihrer Bedeutung oder der Art der Bearbeitung, insbesondere mit weiteren Personendaten, heikel ist. Neu werden genetische Daten und die sogenannten biometrischen Daten in die Kategorie der besonders schützenswerten Daten aufgenommen. Genetische Daten sind Informationen über das Erbgut. Im Entwurf vorgesehen ist neu eine nicht abschliessende Umschreibung der besonders schützenswerten Daten (vgl. die Erläuterungen zu § 2 Abs. 2, Kap. 3.1).

2.2 Informationspflichten und Auskunftsrechte

Überarbeitet werden die Bestimmungen über die Informationspflichten beim Erheben von Personendaten und über die Auskunftsrechte hauptsächlich in den §§ 8 und 15 des geltenden Datenschutzgesetzes. Dabei wird die Informationspflicht nicht grundlegend geändert, deren Anwendung jedoch verbessert, indem klarer wird, über was das erhebende Organ von sich aus die betroffenen Personen zu informieren hat. Entsprechend wird auch der Umfang des Auskunftsrechts präzisiert. Zusätzlich anzugeben ist die Aufbewahrungsdauer der Personendaten. Das Recht auf Auskunft und auf Einsicht in die eigenen Personendaten muss weiterhin kostenlos gewährt werden.

In Ergänzung zu diesen grundsätzlich schon bestehenden Rechten und Pflichten ist eine Informationspflicht bei unbefugten Datenbearbeitungen im Grundsatz festzulegen. Werden Datenbestände verändert oder sind Personendaten ungesichert verloren gegangen und kann aus den Umständen dieses Vorgangs eine erhebliche Gefährdung der Persönlichkeitsrechte eintreten, sind die betroffenen Personen zu informieren. Solche Verletzungen der Datensicherheit können fahrlässig oder missbräuchlich durch Mitarbeiterinnen oder Mitarbeiter einer Behörde, aber auch durch Dritte, erfolgen. Die Informationspflicht ist dabei nicht um ihrer selbst willen zu erfüllen. Im Sinn einer Risikoorientierung werden in der Praxis Kriterien aufzustellen sein, welche eine Information nahelegen. Eine Informationspflicht ist insbesondere anzunehmen, wenn die betroffenen Personen zur Abwehr des Schadens selber Massnahmen ergreifen könnten (z.B. Zugangsdaten ändern).

2.3 Datenschutz-Folgeabschätzung

Die eingangs erwähnten neuen europäischen Rechtsgrundlagen verlangen eine Datenschutz-Folgenabschätzung durch das verantwortliche Organ. Dieses Instrument ist auch im DSG-Entwurf des Bundes vorgesehen. Künftig sollen bei heikleren Vorhaben eine etwas formalere Beurteilung des Datenschutzes als bisher durchgeführt und dokumentiert werden. Dabei soll ein risikobasierter Ansatz gelten: Eine Datenschutzfolgeabschätzung ist nötig, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt. In der Sache geht es um nichts Neues. Bei Informatikprojekten wurden solche Folgeabschätzungen schon vorgenommen. Mit der Abschätzung wird eine Prognose darüber gemacht, welche Folgen eine geplante Datenbearbeitung für die betroffenen Personen oder Personengruppen aufweist. Die Abschätzung enthält zumindest eine allgemeine Beschreibung der geplanten Datenbearbeitung (z.B. Zweck, Bearbeitungsvorgänge und verwendete Technologie, Aufbewahrungsdauer der Daten), eine Bewertung der genannten Risiken sowie eine Darstellung und Bewertung der geplanten Abhilfemassnahmen und anderen Vorkehren und Verfahren, durch die der Schutz der Grundrechte sichergestellt werden soll. Bei der Ausarbeitung von gesetzlichen Regelungen der Datenbearbeitung wird die Abschätzung in diesem Rahmen zu leisten sein.

2.4 Verzicht auf Register der Datensammlungen

In der Praxis hat sich das vom geltenden Recht verlangte Register der Datensammlungen[1] nicht bewährt. Da das Register auf Stufe der Gemeinwesen nachzuführen ist, wurde es rudimentär bewirtschaftet. Zudem ist der Informationsgehalt für die Bevölkerung beschränkt. Aus diesen Gründen soll das Register aufgegeben werden.

Die EU-Richtlinie 2016/680 verlangt hingegen für den Justiz- und Polizeibereich, dass ein Register der Datenbearbeitungen geführt wird und knüpft damit praxisbezogener an die Tätigkeit an. Es ist vorgesehen, diese Anforderung an die kantonale Datenschutzgesetzgebung mit einer Grundsatznorm aufzunehmen. Den Inhalt dieses spezifischen Registers soll der Regierungsrat durch Verordnung regeln.

2.5 Stellung und Unabhängigkeit des Datenschutzbeauftragen

Eine wesentliche Anforderung der eingangs erwähnten Übereinkommen und Erlassen ist, dass die Aufsichtsstellen des Bundes und der Kantone im Bereich des Datenschutzes über die erforderliche Unabhängigkeit verfügen müssen. In Übereinstimmung mit dem erhöhten europäischen Standard sollen insbesondere Verfügungs- und Finanzbefugnisse des oder der Beauftragten für den Datenschutz definiert werden.

2.5.1 Befugnisse

Nach geltendem Recht fordert der Beauftragte das öffentliche Organ auf, hinsichtlich einer strittigen datenschutzrechtlichen Frage einen Entscheid zu erlassen und konnte diesen Entscheid nach den Bestimmungen des Verwaltungsrechtspflegegesetzes anfechten. Neu erhält der Beauftragte wie beim Bund und in den anderen europäischen Ländern die Verfügungskompetenz. Entscheide des Beauftragten können vor Kantonsgericht angefochten werden (vgl. § 24 Abs. 4 in Verbindung mit § 21 Abs. 3 des Entwurfes).

Ebenfalls in Übereinstimmung mit den übergeordneten Anforderungen soll der oder die Beauftragte für den Datenschutz über die vom Parlament bewilligten Kredite in eigener Kompetenz verfügen dürfen (§ 22c Abs. 1 des Entwurfes). Damit wird die entsprechende Regelung für die Finanzkontrolle übernommen (vgl. § 6 Abs. 2 Finanzkontrollgesetz vom 8. März 2004, SRL Nr. 615). In Übereinstimmung mit der Botschaft B 171 vom 16. Januar 2007 betreffend die Teilrevision des Datenschutzgesetzes wird auf ein direktes Budgetantragsrecht für den Beauftragten oder die Beauftragte hingegen verzichtet (vgl. die Ausführungen in GR 2007 S. 834). Auch im Bundesrecht ist ein direktes Budgetantragsrecht des oder der eidgenössischen Datenschutzbeauftragten nicht vorgesehen.

2.5.2 Wählbarkeitsvoraussetzungen und Wechsel auf Parlamentswahl mit Amtsdauersystem

Gemäss geltender Regelung wählt der Regierungsrat den Beauftragten oder die Beauftragte für den Datenschutz und unterbreitet dem Kantonsrat die Wahl zur Genehmigung. In Übereinstimmung mit der seit Mitte 2009 geltenden Zuständigkeitsordnung für die Wahl des Leiters der Finanzkontrolle wird vorgeschlagen, den Beauftragten oder die Beauftragte künftig durch den Kantonsrat wählen zu lassen; der Regierungsrat stellt dabei den Antrag (§ 22 Abs. 1 des Entwurfes; zur entsprechenden Regelung bei der Finanzkontrolle § 3 Abs. 2 Finanzkontrollgesetz und die Ausführungen in Botschaft B 81 vom 28. November 2008, in: GR 2009 S. 74).

Wie beim Bund und in den übrigen Schengen-Staaten ist die Wahl auf Amtsdauer zu regeln und zu bestimmen, ob und wenn ja wie oft eine Wiederwahl möglich ist. Aufgrund der Stellungnahme des Regierungsrates zum Postulat P 251 von Rosy Schmid-Ambauen über eine Überprüfung der Legislaturdauer[2] ist im Entwurf die übliche vierjährige Amtsdauer mit (zeitlich nicht weiter beschränkter) Wiederwahlmöglichkeit vorgesehen. Der Beauftragte für den Datenschutz hätte eine auf sechs

[1] Vgl. im Internet https://datenschutz.lu.ch/registerdatensammlung
[2] Vgl. im Internet http://www.lu.ch/kr/parlamentsgeschaefte

oder acht Jahre verlängerte Amtsdauer bevorzugt. Als Wählbarkeitsvoraussetzung wird ausdrücklich die Anforderung formuliert, dass die zu wählende Person eine in Datenschutzfragen ausgewiesene Fachperson sein muss. Diese darf kein anderes öffentliches Amt ausüben (vgl. § 22b des Entwurfes).

2.5.3 Finanzierung der Aufsicht

Bisher hat der Kanton auch die Aufsicht über den Datenschutz der Gemeinden und der übrigen dem Gesetz unterstellten Gemeinwesen finanziert. Neu sollen sich die Gemeinden an der Finanzierung beteiligen. Jedes Gemeinwesen, dessen Organe Daten bearbeiten, muss für den ordentlichen Vollzug der massgebenden Datenschutzerlasse sorgen. Die Einrichtung von Aufsichtsstellen des Datenschutzes gehört zu den internationalen Verpflichtungen, welche die Schweiz eingegangen ist. Hierfür können die Gemeinwesen mit anderen Gemeinwesen selbstverständlich zusammenarbeiten.

Wir schlagen deshalb vor, die Aufwendungen für den Beauftragten oder die Beauftragte für Datenschutz hälftig zwischen dem Kanton und den Gemeinden aufzuteilen, zumal der Aufwand von Vorgaben und Projekten des Bundes geschaffen werde. Der Anteil der Gemeinden könnte mit einem Grundbeitrag (Sockelbeitrag) und einem von den Einwohnerzahlen abhängigen Beitrag auf die einzelnen Gemeinden weiterverteilt werden. Dies entspricht den üblichen Aufgaben- und Finanzierungsgrundsätzen des Staatshaushalts. Eine Finanzierung nach Aufwand im Einzelfall im Sinn eines Gebührenmodells erachten wir als nicht praktikabel. Wir laden den Verband der Luzerner Gemeinden beziehungsweise die Gemeinden im Rahmen dieser Vernehmlassung ein, sich an der Entwicklung eines solchen Modells zu beteiligen.

Gemäss kantonalem Voranschlag betragen die Aufwendungen für die Aufsichtsstelle derzeit 190'000 Franken. Für die Zukunft ist unbestrittenermassen eine Erhöhung notwendig, wie dies auch der Beauftragte für den Datenschutz in seinen Tätigkeitsberichten begründet hat. Ursprünglich hatte der Regierungsrat das Budget des Beauftragten schon früher um 150'000 Franken beziehungsweise um das Äquivalent einer 100-Prozent-Stelle erhöhen wollen. Gemäss der kantonalen Finanzplanung ist diese Erhöhung auf 340'000 Franken nun per 2020 geplant. Mit der im vorliegenden Gesetzesentwurf vorgesehenen Finanzierung durch Kanton (1/2) und Gemeinden (1/2) stünde der Aufsichtsstelle künftig ein Betrag von 680'000 Franken zur Verfügung. Angesichts der anhaltend hohen Arbeitslast und im Hinblick auf die angestrebte Digitalisierung der Verwaltung auf Kantonsebene (und der Umsetzung auf Stufe Gemeinden) wäre nach Meinung des Beauftragten inzwischen eine Aufstockung von heute 90 Stellenprozenten auf insgesamt 400–600 Stellenprozente angezeigt (dies insbesondere auch im Quervergleich mit ähnlichen Kantonen). Der Beauftragte erachtet daher eine Aufstockung um 310 auf insgesamt 400 Stellenprozente als Mindestlösung.

2.6 Einheitlichkeit mit eidgenössischem Datenschutzgesetz und Modernisierung der Terminologie

Mit der vorliegenden Änderung des kantonalen Datenschutzgesetzes wird verschiedentlich die Einheitlichkeit mit dem eidgenössischen Datenschutzgesetz und damit die Annäherung an das europäische Datenschutzrecht angestrebt. Es kann auf die vorangehenden Ausführungen verwiesen werden. Darüberhinaus sind aus denselben Gründen auch terminologische Modernisierungen und Vereinheitlichungen nötig. Definitionen sind zu ergänzen (z.B. Umschreibung der Personendaten), auf gewisse Begriffe (z.B. Datensammlung) ist zu verzichten, um keine Abweichungen oder Unklarheiten zu schaffen und insgesamt eine Vereinfachung des Datenschutzrechtes zu erreichen. Zur Klarstellung gehört auch eine Änderung des Erlasstitels: In Abgrenzung zum Bundesgesetz über den Datenschutz beziehungsweise Datenschutzgesetz schlagen wir den Kurztitel kantonales Datenschutzgesetz vor. Im Folgenden wird für den kantonalen Erlass die Abkürzung KDSG verwendet.

Zu beachten ist, dass im heutigen Zeitpunkt lediglich die Botschaft des Bundesrates zur Totalrevision des eidgenössischen Datenschutzgesetzes und noch kein von den eidgenössischen Räten verabschiedetes Gesetz vorliegt.

3 Der Erlassentwurf im Einzelnen

3.1 Datenschutzgesetz

§ 2
Absätze 1 und 3: Aus der Umschreibung des Begriffs der Personendaten in § 2 Absatz 1 des geltenden kantonalen Datenschutzgesetzes vom 2. Juli 1990 (KDSG, SRL Nr. 38) ergibt sich, dass dieses Gesetz nicht nur dem Schutz von natürlichen Personen vor unbefugtem Bearbeiten ihrer Daten durch öffentliche Organe, sondern auch dem Schutz von juristischen Personen, dient. Aufgrund des internationalen Rechts kann auf Letzteres verzichtet werden, ausserdem wäre eine abweichende Regelung zum DSG-Entwurf des Bundes nicht sinnvoll (vgl. Kap. 2.1.2). In § 2 Absatz 1 sollen daher Personendaten nur noch als Angaben über bestimmte oder bestimmbare *natürliche* Personen definiert werden. Wie bisher sind Personendaten im Sinn des Datenschutzrechtes Angaben, mit der eine solche Person direkt oder indirekt identifiziert werden kann (bspw. durch die AHV-Nummer). Es kann auf den bundesrechtlichen Datenbegriff verwiesen werden. In den weiteren Bestimmungen des Erlasses werden die natürlichen Personen, über die Daten bearbeitet werden, wie bisher als *betroffene Personen* bezeichnet. Aufgrund der Änderungen der Absätze 1 und 2 ist die Umschreibung in Absatz 3 anzupassen. Insbesondere ist nur noch der Begriff "Person" zu verwenden; der Begriff der Personengesellschaft entfällt. Dagegen bleibt die Zweckbestimmung des § 1 unverändert.

Absatz 2: In diesem Absatz werden neu die genetischen Daten unter der Kategorie der besonders schützenswerten Personendaten aufgeführt, dies mit dem Begriff des Erbgutes. Genetische Daten können eindeutige Informationen über das Aussehen oder die Gesundheit einer Person liefern. Soweit sich solche Daten auf bestimmte oder bestimmbare Personen beziehen, sollen sie besonders schützenswerte Personendaten im Sinn des Gesetzes sein. Dabei sind Gensequenzen so lange als anonym zu betrachten und keine Personendaten, als es nicht möglich ist, sie – zum Beispiel mit einer Datenbank – tatsächlich mit einer einzelnen, vorbekannten Person zu verknüpfen (sog. relativer Charakter von Personendaten, vgl. Rosenthal, Personendaten ohne Identifizierbarkeit?, in: Digma, 2017, S. 198 ff.; BGE 136 II 508 E. 3). Im Sinn der Aktualisierung des Datenschutzrechtes ist vorgesehen, die mit dem Kurzbegriff "biometrische Daten" umschriebenen Personendaten ebenfalls in die Kategorie der besonders schützenswerten Personendaten aufzunehmen. Biometrische Daten sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer Person, welche die eindeutige Identifizierung ermöglichen oder bestätigen (wie durch Gesichtserkennungsprogramme gewonnene Daten zu einem Gesicht, daktyloskopische Daten der Polizei, Stimmmuster, Irismuster der Augen einer Person). Dabei gilt es festzuhalten, dass keineswegs jedes Photo unter die Definition im Sinn des Gesetzes fällt. Die genetischen wie die biometrischen Daten wurden auch in den DSG-Entwurf des Bundes aufgenommen. Die Begriffe sollen gleich ausgelegt werden wie im Bundesrecht. Im Unterschied zum geltenden Recht soll die Kategorie der Daten, die besonders schützenswerte Personendaten sind, im Gesetz nicht mehr in abschliessender Form enthalten sein. Damit werden die Konzepte neuerer kantonaler Datenschutzerlasse (wie BS und ZH) übernommen, womit die Anwendung des Gesetzes flexibler wird. Der Aufzählung vorangestellt wird eine kurze Umschreibung der besonders schützenswerten Personendaten. Aus redaktionellen Gründen wird ausserdem auf eine Aufzählungsform mittels Buchstaben gewechselt, was die Übersichtlichkeit erhöht und damit die Anwendung des Gesetzes erleichtert. Dem besseren Verständnis dient auch die Verwendung des Begriffs der verwaltungsrechtlichen Massnahmen (anstelle administrative Massnahmen), dies wiederum entsprechend dem Bundesentwurf.

Absatz 4: Als Bearbeitungsform wird aufgrund der hohen Praxisrelevanz zusätzlich das Löschen aufgeführt (Satz 1). Zur besseren Verständlichkeit soll der Begriff des Bekanntgebens von Personendaten konkretisiert werden als Übermitteln (z.B. durch telephonische oder EDV-Mittel) und als Zugänglichmachen, wobei in Satz 2 das Einsichtgewähren, Weitergeben und Veröffentlichen als Arten des Zugänglichmachens genannt werden. Diese Konkretisierungen lehnen sich an den DSG-Entwurf des Bundes an und sollen zur besseren Verständlichkeit der Datenschutzgrundsätze beitragen.

Absatz 4*bis*: In diesem neuen Absatz wird der Begriff des Profiling (als besondere Art des Bearbeitens von Personendaten) definiert: Profiling ist jede Art der automatisierten Verarbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte einer Person zu bewerten. Insbesondere kann Profiling dazu dienen, die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, die persönlichen Vorlieben und Interessen, das Verhalten (z.B. das Bewegungsverhalten) oder der Aufenthaltsort einer bestimmten natürlichen Person zu analysieren oder vorherzusagen. Als automatisierte Auswertung gilt jede Auswertung mit Hilfe computergestützter Analysetechniken, mit oder ohne Algorithmen. Die Definition stützt sich auf den DSG-Entwurf des Bundes. Das Profiling stellt einen besonderen Datenbearbeitungsvorgang dar: Aus dem "Datenbild" einer Person wird eine Schlussfolgerung mit Bezug auf persönliche Aspekte einer Person gezogen. Der bisher benützte Begriff des Persönlichkeitsprofils knüpft dagegen an die Art der Daten an und ist auch im DSG-Entwurf des Bundes nicht mehr enthalten. Soweit die aufgrund eines Profiling entstandenen Daten Personendaten oder besonders schützenswerte Personendaten sind, gelangt das Datenschutzgesetz zur Anwendung; dient es zur Erzeugung von anonymen Daten, sind die Resultate des Profiling nicht datenschutzrelevant.

Absatz 6: Mit elektronischen Suchfunktionen, die Daten nach Personen durchsuchen können, hat der Begriff der Datensammlung, der im Gesetz dadurch definiert ist, dass Daten nach den betroffenen Personen erschliessbar sind, an Schärfe verloren. In der Praxis wurde zunehmend darauf abgestellt, ob Personendaten bearbeitet werden. Zudem kann bei der Methode des Profiling auf Quellen zurückgegriffen werden, die keine Datensammlungen darstellen. Wie im DSG-Entwurf des Bundes soll der veraltete Begriff daher gestrichen werden. Wir verweisen auch auf unsere Ausführungen zu den damit verbundenen Anpassungen weiterer Paragraphen, welche den Begriff der Datensammlung verwenden. Konsequenterweise ist auch vom Begriff des Inhabers einer Datensammlung abzusehen (vgl. Abs. 7), zumal bei zentralen Datenbanken im Sinn des § 5 des Informatikgesetzes vom 7. März 2005 (SRL Nr. 26), bei denen mehrere Organe Personendaten in eine einzige Datensammlung einbringen und gemeinsam bearbeiten, Schwierigkeiten bei der Definition der Inhaberfunktion bestehen.

Absätze 7 und 8: In ersterem Absatz wird der Begriff des für die Datenbearbeitung verantwortlichen öffentlichen Organs eingeführt. Damit kann die gleiche Terminologie wie im DSG-Entwurf des Bundes beziehungsweise in den internationalen Rechtsgrundlagen Verwendung finden. Verantwortlich ist das Organ, das allein oder zusammen mit anderen Organen über den Zweck oder die Mittel (z.B. verwendete Software) der Datenbearbeitung entscheidet. Demgegenüber gilt als Auftragsdatenbearbeiter die private Person oder das andere Organ, das im Auftrag des datenverantwortlichen Organs Personendaten bearbeitet (Abs. 8).

§ 3

Aufgrund des internationalen Rechts problematisch sind die allgemeine Ausschlüsse von der Geltung des Datenschutzgesetzes. In § 3 werden daher bisherige Ausnahmen reduziert (Abs. 1c, 2a–d), um diesen Anforderungen besser zu genügen.

Absatz 3 tritt anstelle des Absatzes 2a. Geregelt wird das Verhältnis der Prozess- und Verfahrensordnungen in Gerichts- und Verwaltungsverfahren mit dem Datenschutzrecht. Die Umschreibung orientiert sich am DSG-Entwurf des Bundes, welche ihrerseits den Anforderungen des internationalen Rechts genügt. Das Datenschutzgesetz wird nicht angewendet auf sämtliche Verfahren vor kantonalen Gerichten, insbesondere die verwaltungsgerichtlichen Verfahren, und auf Verfahren an Schiedsgerichten. Weiter umfasst die Ausnahme die Verfahren nach den kantonalen Verfahrensordnungen, sowohl die allgemeine Verfahrensordnung gemäss Verwaltungsrechtspflegegesetz wie auch besondere Verfahrensordnungen oder -regelungen, insbesondere denjenigen im Justizgesetz oder im kantonalem Enteignungsgesetz. Angewendet wird das Datenschutzgesetz wie bisher im erstinstanzlichen Verwaltungsverfahren. In den Prozess- und Verfahrensordnungen gelten eigenständige Regelungen über den Umgang mit Personendaten und die Einsicht in Personendaten, wie sie in den amtlichen Akten erscheinen. Selbstverständlich können solche Erlasse auch die Regelungen im Datenschutzrecht verweisen. Aus Absatz 3 ergibt sich per Umkehrschluss, dass das Datenschutzgesetz auf Datenbearbeitungen angewendet wird, welche von den Gerichtsbehörden

in administrativer Hinsicht vorgenommen werden, beispielweise durch eine Gerichtskanzlei über Daten des eigenen Personals.

Absatz 4 regelt die Anwendung des Datenschutzrechtes, wenn öffentliche Organe am wirtschaftlichen Wettbewerb teilnehmen und dabei privatrechtlich handeln, zum Beispiel wenn eine Verwaltungseinheit ausnahmsweise in Einzelfällen gewerbliche Leistungen an Dritte erbringt. Im Sinn der Gleichbehandlung sollen die Bestimmungen des eidgenössischen Datenschutzrechtes zur Anwendung gelangen, welche für die Privaten gilt.

Das Datenschutzgesetz als Querschnittsgesetz regelt den Datenschutz im Allgemeinen. Im Anwendungsbereich kantonaler Spezialgesetze können diese besondere Normen über den Datenschutz aufweisen, die vorgehen. Absatz 5 stellt dies klar.

§ 5

Die Datenbearbeitung durch ein Organ bedarf einer Rechtsgrundlage oder muss zur Erfüllung einer gesetzlichen Aufgabe erforderlich sein. Somit genügt auch eine mittelbare gesetzliche Grundlage, wenn sich daraus der Bearbeitungszweck ergibt. Absatz 1 soll entsprechend ergänzt werden.

Für die Vornahme eines Profiling im Sinn des neuen § 2 Absatz 4bis gelten die gleichen Voraussetzungen wie bei der Bearbeitung besonders schützenswerter Personendaten. Der Einleitungssatz von Absatz 2 ist entsprechend zu ergänzen. In den Absätzen 2a und b wird der Begriff "formelles Gesetz" zu "Gesetz" verkürzt; eine inhaltliche Änderung ergibt sich dadurch nicht und die Abgrenzung zur Rechtsgrundlage im Sinn von Absatz 1 ist genügend klar, kann doch nur das Parlament Gesetze verabschieden (§ 45 Abs. 1 KV). Im Übrigen sei darauf hingewiesen, dass bereits nach dem Artikel 36 Absatz 1 der Bundesverfassung vom 18. April 1999 (SR 101) schwerwiegende Einschränkungen von Grundrechten einer (vom Parlament beschlossenen) gesetzlichen Grundlage bedürfen.

§ 5a

Absatz 2 ist sprachlich anzupassen, da aufgrund der Änderung von § 2 Absatz 7 der Begriff des Inhabers der Datensammlung nicht mehr verwendet werden kann.

§ 6

Die neuen internationalen Rechtsgrundlagen betonen die Wichtigkeit, die Verantwortung für Datenbearbeitungen klar zuzuordnen und verlangen insbesondere, dass das öffentliche Organ nachweisen muss, dass es die Datenschutzbestimmungen einhält. Der neue Absatz 1bis und die Änderungen des Absatzes 2 nehmen diese Anforderungen auf. Für Datenbearbeitungen mittels aus der Verwaltung ausgelagerter Informatikdienstleistungen sind die Bestimmungen des Informatikgesetzes massgebend (vgl. §§ 13 ff. Informatikgesetz vom 7. März 2005, SRL Nr. 26). Soweit ersichtlich, genügen die Bestimmungen dieses Gesetzes den übergeordneten Anforderungen an die sogenannte Auftragsdatenbearbeitung.

Der Nachweis für die Einhaltung der Datenschutzbestimmungen gemäss Absatz 1bis (Satz 1) kann vom verantwortlichen Organ auf der Grundlage eines Qualitätssicherungssystems in einem Datenschutzmanagementsystem erbracht werden. Der Regierungsrat regelt das Nähere, insbesondere wenn das Organ auf eine Zertifizierung nach den einschlägigen Normen verzichtet. Systeme der Datenbearbeitung sollen in technischer und organisatorischer Hinsicht so ausgestaltet werden, dass sie den Grundsätzen des Datenschutzes entsprechen. Satz 2 zählt Kriterien auf und erwähnt dabei insbesondere den risikoorientierten Ansatz. Auf Verordnungsstufe können die Kriterien und die Verantwortlichkeit für den Datenschutz bei gemeinsamer Bearbeitung durch mehrere Organe noch weiter konkretisiert werden.

§ 7

Die Sachüberschrift des geltenden § 7 lautet "Datensicherung". Dieser Begriff wird heute in technischem Sinn verstanden, nämlich als Prozess, in dem Informationen und Software in regelmässigen Abständen mittels Datensicherungskopien gesichert werden (vgl. § 18 Informatiksicherheitsverordnung vom 22. November 2016; SRL Nr. 26b). In dieser Bestimmung soll es aber um die Datensicherheit im Sinn der Vermeidung der unbefugten Bearbeitung von Personendaten gehen. Diese – umfassend verstandene – Datensicherheit ist Voraussetzung jedwelchen Datenschutzes und daher von grosser praktischer Bedeutung. In Absatz 1 soll die Pflicht der öffentlichen Organe, Personendaten durch technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten (z.B. durch Veränderung oder Verlust von Daten) zu schützen, neu umschrieben und in weiteren Absätzen die von den internationalen Recht verlangten Melde- und Mitteilungspflichten aufgenommen werden. Aus diesen Gründen ist auch die Sachüberschrift zu ändern.

Liegt eine (wesentliche) unbefugte Datenbearbeitung vor, welche die Datensicherheit verletzt und voraussichtlich zu einem hohen Risiko für Persönlichkeits- oder Grundrechtsverletzungen führt, hat das öffentliche Organ dem Beauftragten für den Datenschutz Meldung zu erstatten (Abs. 1bis). Eine solche Meldepflicht ist beispielsweise anzunehmen, wenn Datenbestände verändert oder offenbart worden oder ungesichert verloren gegangen sind und aus den Umständen dieses Vorgangs eine erhebliche Gefährdung eintreten kann. Solche Verletzungen der Datensicherheit können fahrlässig oder missbräuchlich durch einen Mitarbeiter oder eine Mitarbeiterin, aber auch durch einen Dritten, erfolgen. Im Sinn der Risikoorientierung sind jedoch qualitativ und quantitativ unbedeutende Verletzungen der Datensicherheit nicht zu melden, auch solche, die durch die nachträglichen Massnahmen behoben worden sind (z.B. Zurücksetzen der Passwörter nach Passwortdiebstahl).

Über Verletzungen der Datensicherheit sind betroffenen Personen grundsätzlich nicht zu informieren. Gemäss Absatz 1ter kann unter Umständen aber eine Information angezeigt sein. Zu denken ist an den Fall, wenn die betroffenen Personen zur Abwehr des Schadens selber Massnahmen ergreifen könnten (z.B. Zugangsdaten ändern). Jedenfalls müssen Bagatellfälle oder Verletzungen der Datensicherheit, die hinreichend eingedämmt oder beseitigt werden konnten (z.B. durch ein technisches Back-Up), nicht gemeldet werden. Die Information der Betroffenen kann trotz Meldung unterbleiben, etwa zur Wahrung der öffentlichen Sicherheit, insbesondere wenn die Information den Zweck behördlicher Untersuchungen oder Verfahren in Frage stellen würden. Auf die Information ist ausserdem zu verzichten, wenn einen unverhältnismässigen Aufwand erfordern würde oder gänzlich unmöglich ist. An Stelle der persönlichen Information kann unter Umständen eine öffentliche Bekanntgabe treten (analog § 113 Abs. 1 VRG). Das Weitere, namentlich der Inhalt der Meldung (z.B. Art der Verletzung der Datensicherheit, Folgen für betroffene Personen, Massnahmen), kann auf Verordnungsebene umschrieben werden.

§ 7a

Die neuen europäischen Rechtsgrundlagen verlangen eine Datenschutz-Folgenabschätzung durch das verantwortliche Organ. Mittels Datenschutz-Folgeabschätzungen sollen Risiken identifiziert und bewertet werden, die durch den Einsatz von Technologien und Systemen im Rahmen der Datenverarbeitung entstehen. Eine solche Abschätzung ist nicht generell erforderlich. Vielmehr soll sie nötig sein, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt (Abs. 1). Diese Voraussetzung ist relativ offen formuliert und muss in der Praxis konkretisiert werden. Dabei muss es auch möglich, mehrere ähnliche Bearbeitungsvorgänge in einer Untersuchung zu beurteilen. Je umfangreicher die Bearbeitung oder je umfassender der Bearbeitungszweck oder je sensibler die bearbeiteten Daten, umso eher ist ein hohes Risiko anzunehmen. Ein hohes Risiko kann sich aber auch aus der Art der Bearbeitung ergeben, hauptsächlich wenn neue Technologien oder Mechanismen verwendet werden, und in den meisten Fällen beim Profiling. Dieser risikoorientierte Ansatz liegt bereits dem geltenden § 7 Absatz 1 zugrunde ("angemessene Massnahmen") und wird durch die neue Bestimmung verstärkt. Das verantwortliche öffentliche Organ ist verpflichtet, eine Prognose darüber zu machen, welche Folgen eine geplante Datenbearbeitung für die Betroffenen aufweist. Die Abschätzung enthält zumindest eine allgemeine Beschreibung der geplanten Datenbearbeitung (z.B. Zweck, Bearbeitungsvorgänge und verwendete Technologie, Aufbewahrungsdauer der

Daten), eine Bewertung der genannten Risiken sowie eine Darstellung und Bewertung der geplanten Abhilfemassnahmen und anderen Vorkehren und Verfahren, durch die der Schutz der Grundrechte sichergestellt werden soll. Die Abschätzung kann dem Organ der Vorbereitung zum verlangten Nachweis der Einhaltung der Datenschutzvorschriften gemäss § 6 dienen. Einzelheiten zur Datenschutz-Folgeabschätzung können durch Verordnung geregelt werden.

Auf der Grundlage der Datenschutz-Folgeabschätzung kann der Beauftragte für den Datenschutz Stellung nehmen und innert Frist Massnahmen zur Verbesserung des Datenschutzes vorschlagen (Abs. 2). Die Empfehlungen des Beauftragten sollen sicherstellen, dass die Risiken bei den Datenbearbeitungsvorhaben hinreichend abgeklärt werden und gegebenenfalls mit verhältnismässigen rechtlichen, organisatorischen oder technischen Massnahmen weiter reduziert werden können. Bei Rechtsetzungsvorhaben kann sich der Beauftragte mittels Stellungnahmen in Vernehmlassungsverfahren des Kantons eingeben, damit die datenschutzrechtlichen Vorgaben Berücksichtigung finden mögen (vgl. § 23 Abs. 1e Entwurf). Die Risikoabschätzung schliesst damit an die übliche verfassungsmässige Prüfung von Recht- und Angemessenheit eines Erlasses an.

§ 7b
Für den Justiz- und Polizeibereich verlangt die EU-Richtlinie, dass die Gerichts- und Strafverfolgungsbehörden ein Register der Datenbearbeitungen führen. Das Register schliesst praxisbezogen an die Tätigkeit an. Auf ein allgemeines Register der Datensammlungen gemäss § 14 KDSG wird inskünftig verzichtet. Der Aufwand für die Registerführung rechtfertigt sich nicht mehr. Vgl. unsere Ausführungen in Kapitel 2.4.

Die EU-Richtlinie verlangt für die Schengen-Umsetzung die Ernennung eines Datenschutzberaters oder einer Datenschutzberaterin im Gerichts- und Strafverfolgungsbereich. Wie beim Bund soll diese Funktion indes nicht als Datenschutzbeauftragter bezeichnet werden, um Verwechslungen mit der ordentlichen Aufsichtsstelle zu vermeiden. Bei dieser Person soll es um eine Angehörigen des bestehenden Personals handeln, der besondere Kenntnisse auf dem Gebiet des Datenschutzes hat, und sich so neben seiner Haupttätigkeit einbringen kann, soweit diese sich damit verträgt. Im Vordergrund dürfte eine Stabstätigkeit, ausgenommen die Informationstätigkeit, sein. Der Datenschutzberater oder die Datenschutzberaterin soll die Mitarbeitenden, die Personendaten bearbeiten, unterstützen, indem er sie hinsichtlich der Datenschutzbelange unterrichtet und berät. Zudem nimmt der Datenschutzberater oder die Datenschutzberaterin die Datenschutzfolgeabschätzungen vor oder lässt sie vornehmen und ist Ansprechperson des oder der Beauftragten für den Datenschutz.

Das Kantonsgericht und der Regierungsrat können für ihre Organisationseinheiten das Weitere zur Registerführung und die interne Datenschutzberatung regeln. Wir gehen davon aus, dass je ein Datenschutzberater oder eine Datenschutzberaterin innerhalb des Gerichtswesens, innerhalb der Staatsanwaltschaft und innerhalb der Luzerner Polizei den Anforderungen und Bedürfnissen genügt.

§ 8
Transparenz und Information sind wichtige Anliegen des Datenschutzrechtes. Die öffentlichen Organe stehen in der Pflicht, die betroffenen Personen über die Erhebung von Personendaten zu informieren. Dem geltenden § 8 liegt der Transparenzgedanke ebenfalls zugrunde, Absatz 4 über die Informationspflicht bei der Datenerhebung ist jedoch zu überarbeiten und ergänzen. Dabei gilt es zu beachten, dass der Begriff des Erhebens von Personendaten in anderen kantonalen Datenschutzgesetzen als Beschaffen von Personendaten bezeichnet und nach heutigem Wortgebrauch etwas breiter verstanden wird als bei der Entstehung des kantonalen Datenschutzgesetzes Ende der 1980er-Jahre.

Die Information über die Datenerhebung soll Angaben über das verantwortliche Organ samt dessen Kontaktdaten umfassen sowie Angaben über die bearbeiteten Daten oder Datenkategorien, die Rechtsgrundlage und der Zweck des Bearbeitens, allfällige Dritte als Datenempfänger und die

Rechte der betroffenen Personen. Werden die Daten (auf Papier oder mittels Internet elektronisch) auf Formular erhoben, können die Angaben auf oder mit dem Formular und standardisiert angegeben werden. Bei anderen Datenerhebungen sind die betroffenen Personen individuell zu informieren, ausser es greifen die Gründe gemäss Absatz 5. Gemäss diesem Absatz kann unter bestimmten Umständen von der Information abgesehen werden, beispielsweise wenn die betroffenen Personen in einer früheren Phase der Datenerhebung bereits einmal informiert worden sind oder die betroffenen Personen aus den gesetzlichen Grundlagen, insbesondere solchen des Verfahrensrechts, mit hinreichender Deutlichkeit herauslesen können, welche Daten über sie zu welchem Zweck bearbeitet werden. Ausserdem entfällt die Informationspflicht, wenn dadurch die Erfüllung der öffentlichen Aufgaben ernstlich gefährdet oder verunmöglicht würde, wie im geltenden Absatz 2 festgehalten (z.B. bei polizeilichen Ermittlungen).

§ 9

Die Voraussetzungen für die Bekanntgabe von Personendaten in § 9 Absatz 1a folgen denjenigen für die Bearbeitung von Personendaten gemäss § 5 Absatz 1; entsprechend ist dieser Absatz zu ergänzen (Abs. 1a^{bis}). Besondere Geheimhaltungsvorschriften wie das medizinische Berufsgeheimnis können einer Bekanntgabe von Daten weiterhin entgegenstehen. Dies wird im Einleitungssatz von Absatz 1 bereits heute klargestellt. Gegebenenfalls ist in solchen Fällen die Zustimmung der betroffenen Person einzuholen.

§ 13

Satz 2 von Absatz 1 wie auch Absatz 2 sind überflüssig und aufzuheben. Für Personendaten, die von der Polizei erhoben werden, verweisen wir auf das Spezialrecht (vgl. Änderung des Gesetzes über die Luzerner Polizei vom 30. Oktober 2017, in: Kantonsblatt 2017 S. 3049, und unsere Ausführungen in der Botschaft B 74 über die Aktualisierung des Polizeirechts vom 21. März 2017).

Zur Datenbearbeitung nach dem Verhältnismässigkeitsprinzip gehört die Löschung von Personendaten beziehungsweise die regelmässige Überprüfung, ob die Datenbestände zur Aufgabenerfüllung noch erforderlich sind. Absatz 3 ermächtigt den Regierungsrat ausdrücklich, im Verordnungsrecht Löschfristen und Massnahmen zur Sicherstellung der regelmässigen Überprüfung sicherzustellen.

Gemäss den redaktionellen Leitlinien der luzernischen Gesetzgebung entfällt die Sachüberschrift dieser Bestimmung, da im Unterabschnitt kein weiterer Paragraph enthalten ist.

§ 14

Wie in Kapitel 2.4 und zum neuen § 7b ausgeführt, wird auf das Register der Datensammlungen inskünftig verzichtet. Die Bestimmung ist aufzuheben.

§§ 15 und 17–19

Das Recht jeder Person, Auskunft zu erhalten, ob Daten über ihre eigene Person von einem Organ bearbeitet werden, und gegebenenfalls auch die direkte Einsicht in deren Datenbestände, ist ein Kernpunkt des Datenschutzrechts. Das Auskunftsrecht hat den Zweck, der betroffenen Person zu ermöglichen, die über sie bearbeiteten Daten zu kontrollieren mit dem Ziel, die Einhaltung der datenschutzrechtlichen Grundsätze, wie Beschaffung der Daten mit rechtmässigen Mitteln und nicht in gegen Treu und Glauben verstossender Weise oder Gewährleistung der Richtigkeit der Daten und der Verhältnismässigkeit ihrer Bearbeitung, in der Rechtswirklichkeit zu überprüfen und durchzusetzen (BGE 138 III 425 E. 5.3) Die Änderungen nehmen Präzisierungen am Umfang des Auskunftsrechts vor und orientieren sich an der entsprechenden Bestimmung des DSG-Entwurfes des Bundes beziehungsweise den Anforderungen des internationalen Rechts.

Der Umfang des Auskunftsrechts ergibt sich grundsätzlich aus der Informationspflicht der Organe. Inhaltlich orientiert sich § 15 Absatz 2 am neuen § 8 Absatz 4 und zusätzlich werden die Angaben

über die Herkunft der Personendaten und über deren Aufbewahrungsdauer angeführt. Die Aufzählung ist nicht abschliessend zu verstehen. Das Auskunftsrecht ist hingegen kein Einsichtsrecht in amtliche Dokumente und kein Editionsrecht für Urkunden; so umfasst es die lediglich Personendaten als solche. Schon bei der Datenerhebung nach § 8 wurden die betroffenen Personen über das datenerhebende Organ und dessen Kontaktdaten informiert. Wir gehen davon aus, dass sich diese Angaben bei der Erteilung der Auskunft durch das angefragte Organ ergeben (insbesondere bei schriftlichen Auskünften durch den Briefkopf) und hier nicht noch einmal aufzuführen sind. Werden Daten systematisch erhoben (z.B. auf einem Formular im Internet oder auf Papier), sollten sämtliche Angaben auf dem Formular oder einem Beiblatt angebracht werden.

In verschiedenen Absätzen ist aufgrund der Änderung von § 2 Absatz 7 der Begriff des Inhabers der Datensammlung durch "verantwortliches Organ" oder "Organ" zu ersetzen. In § 18 Absatz 1b wird die Löschung der Daten explizit aufgenommen, wie es der DSG-Entwurf des Bundes beziehungsweise die Anforderungen des internationalen Rechts vorsehen. Mit der gleichen Begründung wird in § 18 Absatz 2c der Anspruch etwas allgemeiner gefasst und § 19 Absatz 2 gestrichen. Zu letzterem sei bemerkt, dass in den Fällen, in denen die Auskunft mit dem Grund der Auskunftsverweigerung kollidiert, die Anforderungen an die Begründung inhaltlich und umfangsmässig reduziert werden können, ohne dass auf einen formellen Entscheid nach dem Verwaltungsrechtspflegegesetz verzichtet werden müsste.

Mit der erwähnten Ergänzung von § 18 können Organe flexibel auf berechtigte Bearbeitungsforderungen eingehen. Beispielsweise könnte das Staatsarchiv oder ein Museum – nach einer umfassenden Interessenabwägung von unbeschränktem Zugangsinteresse und Persönlichkeitsschutz – auf eine Internetpublikation verzichten.

Festzuhalten bleibt, dass das Auskunfts- und Einsichtsverfahren nach § 15, die Berichtigung von Personendaten nach § 17 Absatz 1, das Nachweisverfahren für die Richtigkeit und die Aufnahme des Bestreitungsvermerks nach § 17 Absatz 2 sowie die Verfahren nach § 18 unverändert kostenlos zu gewähren sind (§ 20), dies in Übereinstimmung mit den internationalen Rechtsgrundlagen.

§ 21
Erlass und Anfechtung von Entscheiden in Datenschutzangelegenheiten (z.B. von Dienststellen der Verwaltung) richten sich nach dem Gesetz über die Verwaltungsrechtspflege vom 3. Juli 1972 (VRG, SRL Nr. 40). Dieses Verfahrensrecht regelt auch die Kostenfolge. In Absatz 2 kann deshalb der zweite Teilsatz gestrichen werden.

Aufgrund der internationalen Rechtsgrundlagen soll die unabhängige Aufsichtsstelle Entscheidbefugnisse erhalten, weshalb Absatz 2 entfällt. Vgl. unsere Ausführungen zu § 24.

Gemäss Absatz 3 sollen Entscheide des Beauftragten für den Datenschutz unmittelbar mit Verwaltungsgerichtsbeschwerde beim Kantonsgericht angefochten werden können; das Verfahren vor Gericht richtet sich nach VRG. Da der Beauftragte für den Datenschutz Entscheidbefugnisse hat, sollen die betroffenen Organe seine Entscheide anfechten dürfen und dementsprechend vor Gericht als Partei auftreten (vgl. § 18 Abs. 1 VRG).

§ 22 / § 22a (Variante)
Wie in Kapitel 2.5.3 erläutert, soll die Finanzierung der Aufsichtsstelle auf neue Grundlagen gestellt werden. In der bevorzugten Hauptvariante wird die Aufsichtsstelle, welche – wie heute – die Aufsicht über die Organe von Kanton und Gemeinden ausübt, hälftig durch Kanton und Gemeinden finanziert (Abs. 3). Die Hauptvariante trägt den hohen fachlichen Anforderungen wie auch der notwendigen Unabhängigkeit der Aufsicht Rechnung.

Der Variantenvorschlag zu Absatz 3 würde es den Gemeinden ermöglichen, einzeln oder gemeinsam mit anderen Gemeinden eine Aufsichtsstelle zu betreiben (vgl. § 22a Variante). Für solche kommunalen oder überkommunalen (d.h. regionalen) Aufsichtsstellen würden die kantonalen wie

auch die völker- und europarechtlichen Anforderungen ebenfalls gelten. Nur in wenigen Kantonen gibt es aber überhaupt kommunale Aufsichtsstellen (vgl. die entsprechenden Regelungen in BE, SG und ZH). Sollten sich eine Gemeinde in diesem Modell dafür entscheiden, sich mittels Vereinbarung mit dem Kanton an der kantonalen Aufsichtsstelle zu beteiligen, müsste sie diese ebenfalls mitfinanzieren.

Würde in der Vernehmlassung der Variantenvorschlag bevorzugt, müsste § 22 redaktionell überarbeitet werden (Sachüberschrift: Kantonale Aufsicht, Absatz 1: kantonale Aufsichtsstelle, Absatz 3: Streichung). Allenfalls wäre im Sinn einer Übergangsbestimmung eine Regelung zu treffen, was passiert, wenn die Gemeinden die eigene Aufsichtsstelle nicht oder nicht rechtzeitig bezeichnen. Im Vollzug wäre die Variante auch unter diesem Gesichtspunkt aufwendiger.

§ 22b
Wie bisher bedarf die behördliche Datenbearbeitung einer unabhängigen Aufsicht. Der Beauftragte oder die Beauftragte für den Datenschutz muss über die erforderlichen Qualifikationen, Erfahrung und Sachkunde verfügen, um die gesetzlich vorgeschriebenen Aufgaben zu erfüllen. Die Aufsichtsstelle ist keine politische Behörde und deshalb mit einer Fachperson zu besetzen, was Absatz 1 verdeutlicht. Ausserdem ist eine Wahl durch den Kantonsrat auf Amtszeit festzulegen (vgl. Kap. 2.5.2). Diese Regelungen über das Wahlverfahren und die institutionelle Unabhängigkeit entsprechen den internationalen Anforderungen.

Eine Unvereinbarkeit soll bestehen zwischen dem Amt des oder der Beauftragten für Datenschutz und einem anderen öffentlichen Amt (Abs. 2). Bei einem Teilpensum muss dem Beauftragten oder der Beauftragten eine andere (privatrechtliche) Erwerbstätigkeit bewilligt werden (Abs. 3). Zur fristlosen Auflösung des Arbeitsverhältnisses, insbesondere bei vorsätzlicher schwerer Amtspflichtverletzung, vgl. § 19 des Personalgesetzes vom 26. Juni 2006 (SRL Nr. 51).

§ 22c
Diese Bestimmung regelt die Finanz- und Personalkompetenzen. Die Verfügungsbefugnis umfasst auch Ausgaben für Anstellungen. Der oder die Beauftragte verfügt über die für Anstellungen nötigen personalrechtlichen Befugnisse wie auch der oder die Beauftragte grundsätzlich dem kantonalen Personalrecht unterstellt bleibt.

§ 23
Der oder die Beauftragte für den Datenschutz überwacht unabhängig die Einhaltung der Vorschriften über den Datenschutz. Er oder sie soll die massgeblichen Entwicklungen in der Informations- und Kommunikationstechnologie, soweit sie sich für den Datenschutz auswirken, verfolgen, damit die öffentlichen Organe beraten werden können. Entsprechend den internationalen Rechtsgrundlagen wird Absatz 1b in diesem Sinn ergänzt.

Die Kontrolle nach § 23 Absatz 1a ist eine anlassfreie und nach einem eigenen Prüfprogramm. Eine anlassbezogene Kontrolle auf eine konkrete Beanstandung hin muss jedoch auch möglich sein. Dem aufgrund des internationalen Rechts nötigen Recht auf Beschwerdemöglichkeit soll mit einer Ergänzung des Absatzes 1c Rechnung getragen werden.

Neu wird dem Beauftragten in Übereinstimmung mit den internationalen Rechtsgrundlagen die Möglichkeit zu (förmlichen) Empfehlungen zu Datenbearbeitungen der öffentlichen Organe gegeben; das Organ, an das die Empfehlung gerichtet ist, hat zu erklären, ob es der Empfehlung folgen wird (Abs. 1c^{bis}).

Zu Absatz 1d schlagen wir die ersatzlose Streichung vor. Die Vermittlung zwischen Organen und Personen wird nicht nachgefragt, würde im Bedarfsfall erhebliche Ressourcen binden und kann mit

dem Beratungsauftrag nach Absatz 1b in Konflikt geraten, da nach einer Beratung eine unvoreingenommene Schlichtung kaum mehr möglich wäre. Eine Vermittlungstätigkeit ist auch vom internationalen Recht nicht verlangt.

Absatz 1e wird mit der Möglichkeit ergänzt, dass der oder die Beauftragte zu Rechtsetzungsvorhaben, welche das Bearbeiten von Personendaten betreffen, eine Vernehmlassung abgeben kann. Damit kann der oder die Beauftragte insbesondere zu Risiken für die Grundrechte beispielweise aufgrund der Verwendung neuer Technologien in der Verwaltung Stellung nehmen.

In Absatz 1f wird aufgrund des internationalen Rechts die Sensibilisierung der Öffentlichkeit für den Datenschutz aufgenommen.

§ 24
Der Aufsichtsstelle muss aufgrund der internationalen Rechtsgrundlagen die Befugnis zukommen, bei Verstössen gegen Datenschutzrecht verbindliche Anordnungen (in Form einer Verfügung) zu treffen. Ein anfechtbarer Entscheid soll insbesondere nach Ablehnung einer Empfehlung erlassen werden. Das bisherige System, dass das öffentliche Organ eine Verfügung erlässt, welche der oder die Beauftragte für den Datenschutz anfechten musste, ist umzukehren. Neu muss die Verfügung des oder der Beauftragten vom Gemeinwesen beziehungsweise von dessen berechtigtem Organ (z.B. Gemeinderat) beim Kantonsgericht angefochten werden. Zeichnet sich ab, dass eine Behörde die Empfehlung nicht befolgt, kann der oder die Beauftragte eine vorsorgliche Verfügung im Sinn des Verwaltungsrechtspflegegesetzes treffen, was ausdrücklich erwähnt soll (Abs. 4). Eine mögliche Massnahme könnte die Einschränkung oder Einstellung der Datenbearbeitung bis zum Urteil des Kantonsgerichtes sein.

§ 26
Für die Umstellung auf das Amtsdauersystem (§ 22 Abs. 1) wird eine Übergangsfrist vorgesehen. Damit kann der Kantonsrat die Wahlgenehmigung jeweils im zweiten Jahr der Legislatur aussprechen.

3.2 Organisationsgesetz
Mit dem neuen § 21b wird für das GEVER-System der kantonalen Verwaltung eine Grundlage im Gesetz geschaffen. In diesem elektronischen Geschäftsverwaltungssystem erhalten die Departemente Zugriff auf Dokumente zur Abwicklung aller Geschäftsprozesse und insbesondere zur Bearbeitung von Regierungsgeschäften zwischen den Departementen und der Staatskanzlei (z.B. Vernehmlassungen). Entsprechend greifen innerhalb eines Departementes auch die einzelnen Verwaltungseinheiten auf das System zu. Durch die elektronische Dokumentenablage (z.B. aus einem Schriftverkehr) oder bei der Erstellung von Dokumenten werden Daten von natürlichen Personen oder von juristischen Personen, einschliesslich besonders schützenswerter Personendaten, bearbeitet. Der verwaltungsinterne Zugriff in GEVER-Geschäften stellt letztlich ein Abrufverfahren dar. Absatz 2 stellt die gesetzliche Grundlage zur Datenbearbeitung für die Regierungsgeschäfte im Sinn des § 20 dar. Vorbehalten bleiben die spezialgesetzlichen Grundlagen für die den Verwaltungszweigen und -einheiten übertragenen Verwaltungsaufgaben (§ 20 Unterabs. d).

3.3 Verwaltungsrechtspflegesetz
Wie in Kapitel 3.1 zu § 3 Absatz 3 KDSG-Entwurf ausgeführt, regeln die Prozess- und Verfahrensordnungen den Datenschutz in Gerichts- und Verwaltungsverfahren. Das Justizgesetz vom 10. Mai 2010 enthält die Ausführungsbestimmungen zum Vollzug der gesamtschweizerisch geltenden Prozessordnungen (Zivilprozessordnung vom 19. Dezember 2008, ZPO, SR 272; Strafprozessordnung, vom 5. Oktober 2007, StPO, SR 312.0; Jugendstrafprozessordnung vom 20. März 2009, JStPO, SR 312.1), stellt aber keine eigenen datenschutzrechtlichen Regeln auf. Die Prozessordnungen selbst enthalten Bestimmungen über die Parteiöffentlichkeit und die Justizöffentlichkeit und regeln damit auch den Umgang mit Personendaten (z.B. Akteneinsichtsrecht der Prozessparteien).

Im verwaltungsrechtlichen Verfahren gelangt – abgesehen von den allgemeinen Verfahrensgrundrechten der Bundesverfassung – die kantonale Verfahrensordnung zur Anwendung, mithin das Gesetz über die Verwaltungsrechtspflege vom 3. Juli 1972 (SRL Nr. 40). Das Gesetz regelt das Recht der Parteien auf Akteneinsicht in hängigen oder abgeschlossenen eigenen Angelegenheiten (§§ 48 ff. VRG) und die Verhandlungen vor den Verwaltungs- und Gerichtsbehörden. In Verwaltungssachen verhandeln und beraten die Behörden grundsätzlich unter Ausschluss der Parteien und der Öffentlichkeit (§ 38 VRG). Das Gesetz über die amtlichen Veröffentlichungen (Publikationsgesetz) vom 20. März 1984 (PubG; SRL Nr. 27) stellt die Rechtsgrundlage für die Veröffentlichung von Leitentscheiden und weiteren Entscheiden der Gerichts- und Verwaltungsbehörden ("Luzerner Gerichts- und Verwaltungsentscheide") mittels einer im Internet zugänglichen Datenbank dar (vgl. § 13 PubG).

Im Entwurf wird nun vorgeschlagen, den Umgang mit persönlichen Daten nach Abschluss der Gerichtsverfahren in einem neuen § 141a insoweit zu regeln, als es um die Veröffentlichung und den – von der Bundesverfassung garantierten – Zugang zu Rechtsmittelentscheiden geht. Im Sinn des Datenschutzes ist mindestens zu verlangen, dass die Namen der Parteien unkenntlich gemacht werden (Abs. 1). Vorbehältlich weitergehender Anonymisierungen und anderweitiger Einschränkungen aufgrund überwiegender öffentlicher Interessen oder besonderer schützenswerter privater Interessen in Einzelfällen wird den Interessen der Parteien am Persönlichkeitsschutz durch Unkenntlichmachung ihrer Namen in der Regel genügend Rechnung getragen (BGE 139 I 129 und 133 I 106 E. 8.3). Im Übrigen gewähren die Gerichte bereits heute Zugang zu abgeschlossenen Verfahren und erheben hierfür moderate Gebühren (vgl. §§ 120 f. Justizverordnung vom 26. März 2013, SRL Nr. 262; § 36 Abs. 1 Justiz-Kostenverordnung vom 26. März 2013; SRL Nr. 265).

Auf eine weitergehende Regelung im Verwaltungsbeschwerdeverfahren soll zum heutigen Zeitpunkt verzichtet werden. Der Europäische Gerichtshof für Menschenrechte hat in seinem Urteil vom 8. November 2016 festgehalten, dass die Einsichtsverweigerung alleine aufgrund der Tatsache, dass darin Personendaten enthalten sind, und ohne eine Interessenabwägung durchzuführen, gegen die Meinungs- und Informationsfreiheit verstösst und ein Zugangsrecht auf amtliche Akten nach Interessenabwägung bereits aus Artikel 10 der Europäischen Menschenrechtskonvention abgeleitet werden kann (EGMR-Urteil Nr. 18030/11 vom 18. November 2016 i.S. Magyar Helsinki Bizottság contra Ungarn).

3.4 Personalgesetz

Wurde ein Angestellter oder eine Angestellte im Sinn des Personalgesetzes vom 26. Juni 2001 (PG; SRL Nr. 51) von einem gesetzgebenden Organ gewählt, ist die oberste Dienstaufsichtsbehörde für die übrigen personalrechtlichen Entscheide gemäss § 67 PG zuständig; ist der Regierungsrat oberste Dienstaufsichtsbehörde und wählt – wie im Falle des oder der Beauftragten für Datenschutz – den Angestellten, gilt Absatz 2 von § 67 PG. In diesem Absatz 2 ist nun die Zuständigkeit des Staatsschreibers oder der Staatsschreiberin aufzunehmen, da der oder die Beauftragte für Datenschutz administrativ der Staatskanzlei zugeordnet ist. In der geltenden Bestimmung werden nur die Departementsvorsteher und -vorsteherinnen erwähnt, da bei der Entstehung des Personalgesetzes weder die Organisationseinheit für Datenschutzbelange noch diejenige für Finanzkontrolle der Staatskanzlei zugeordnet waren. Die fristlose Aufkündigung des Arbeitsverhältnisses aus wichtigen Gründen während der Amtszeit bleibt gemäss § 67 Absatz 2 (Satz 2) PG dem Regierungsrat vorbehalten.

3.5 Gesetz über die Steuerung der Finanzen und Leistungen

Die Ergänzung von § 11 Absatz 2 (Satz 2) des Gesetzes über die Steuerung der Finanzen und Leistungen vom 13. September 2010 (SRL Nr. 600) ist eine Folgeanpassung aus § 22 Absatz 3 KDSG-Entwurf. Wie bei der Finanzkontrolle übernimmt der Regierungsrat die vom Beauftragten oder von der Beauftragten für den Datenschutz vorgelegten (Global-)Budgets unverändert in den kantonalen Voranschlag zuhanden des Kantonsrates.

3.6 Weitere Gesetze

Weitere Gesetze sind hinsichtlich der Verwendung der datenschutzrechtlichen Terminologie zu überprüfen und anzupassen. Sie seien im Folgenden lediglich aufgezählt:

Gesetz	§§
Informatikgesetz vom 7. März 2005 (SRL Nr. 26)	3 Abs. 1 und 4, 4 Abs. 3, 5 Abs. 3, 10 Abs. 1, 16 Abs. 1, 18
Statistikgesetz vom 13. Februar 2006 (SRL Nr. 28a)	13 Abs. 2a, 22 Abs. 3
Geoinformationsgesetz vom 8. September 2003 (SRL Nr. 29)	3 Unterabs. h, 9 Abs. 1 und 2, 20 Abs. 1
Gesetz über den Justizvollzug vom 14. September 2015 (SRL Nr. 305)	22 Abs. 1
Gesetz über die Luzerner Polizei (SRL Nr. 350) in der Fassung gemäss der Änderung vom 30. Oktober 2017 (Kantonsblatt Nr. 44/4. November 2017, S. 3049)	4 Abs. 1b und 1c
Steuergesetz vom 22. November 1999 (SRL Nr. 620)	137 Abs. 5 (Satz 2)

Stand: 29.12.2017

4 Auswirkungen

Mit der vorliegenden Revision des kantonalen Datenschutzgesetzes wird die Entwicklung des übergeordneten Völker- und Europarechts sowie die Totalrevision des eidgenössischen Datenschutzgesetzes aufgenommen. Neue Begrifflichkeiten werden in das Gesetz aufgenommen und verschiedene Bestimmungen ergänzt und präzisiert. Es sollen jedoch wo immer möglich Vereinfachungen vorgesehen werden (z.B. Verzicht auf Register über Datensammlungen auf Stufe der Gemeinwesen). Mit der Datenschutz-Folgeabschätzung und der Vorabkonsultation müssen entsprechend den internationalen Vorgaben neue Instrumente eingeführt werden. Durch die Bezeichnung von Datenschutzberatern bei den Gerichts- und Strafverfolgungsbehörden erwarten wir nur eine geringfügige Entlastung für den Beauftragten für den Datenschutz. Hingegen erwachsen den Strafbehörden dadurch Aufwendungen im Umfang von mehreren Tausend Franken, da sie intern Fachwissen aufbauen müssen. Durch den Verzicht auf das Register über Datensammlungen entfallen beim Beauftragten jährlich wiederkehrende Kosten für den Betrieb der Datenbank und des Webhosting von jährlich rund 3'800 Franken.

Auswirkungen hat die Revision auf die Stellung und Unabhängigkeit der Aufsichtsstelle im Bereich des Datenschutzes. Der oder die Beauftragte für den Datenschutz verfügt künftig über die Befugnisse, verbindliche Anordnungen in Form eines Entscheides nach den Bestimmungen des Gesetzes über die Verwaltungsrechtspflege zu erlassen. Bisher konnte er lediglich datenschutzrechtliche Entscheide von Behörden mit Verwaltungsbeschwerde beziehungsweise Verwaltungsgerichtsbeschwerde anfechten. Wir erwarten aus diesem Systemwechsel keine Mehraufwendungen. Jedoch wird die Aufsicht dadurch gestärkt. Eine formale Stärkung erhält die Aufsicht auch durch die Wahl des oder der Beauftragten durch den Kantonsrat

Wie in der derzeitigen kantonalen Finanzplanung aufgezeigt, soll die Aufsichtsstelle künftig über mehr Finanzen verfügen, um ihre Aufgaben zu erfüllen. Mit der Beteiligung der Gemeinden schlagen wir vor, die Finanzierung der Aufsicht auf eine neue, faire Grundlage zu stellen (§ 22 Abs. 3 des Gesetzesentwurfs). Damit kann auf den Grundlagen der bisherigen Planung das Ressourcenproblem bei der Aufsichtsstelle wesentlich entschärft werden (vgl. Kap. 2.5.3). Insgesamt hängen die Kosten des Datenschutzes nicht von der Ausgestaltung dieser Gesetzesrevision, sondern davon ab, wie stark die Bevölkerung von ihren Auskunfts- und Kontrollrechten Gebrauch macht und wie die Verwaltungen von Kanton und Gemeinden weiter digitalisiert werden. Mit der Aktualisierung des kantonalen Datenschutzgesetzes ändert am System des Datenschutzrechtes nichts Grundlegendes. Die Revision stellt sicher, dass den Verpflichtungen des Schengen-Übereinkommens nachgekommen werden kann und ein angemessenes Datenschutzniveau im Sinn der europarechtlichen Anforderungen gewährleistet ist.

5 Weiteres Vorgehen

Im Rahmen der Erarbeitung der Botschaft an den Kantonsrat und der weiteren Bearbeitung des Entwurfs sind neben den internationalen Entwicklungen des Datenschutzrechtes die Beratungen in den eidgenössischen Räten zu beobachten.

Sodann ist die Verordnung zum kantonalen Datenschutzgesetz zu überarbeiten und die Anpassungen im übrigen Verordnungsrecht, hauptsächlich im Hinblick auf eine einheitliche datenschutzrechtliche Terminologie, vorzunehmen.

Luzern, 2. Februar 2018

KANTON LUZERN

Justiz- und Sicherheitsdepartement
Bahnhofstrasse 15
6002 Luzern

Telefon 041 228 59 17
vernehmlassungen.jsdds@lu.ch
www.lu.ch