



Aktualisierung des kantonalen Datenschutzrechtes

*Entwurf Änderung des Datenschutzgesetzes
und weiterer Gesetze*



Zusammenfassung

Die Europäische Union hat im April 2016 eine Reform der Datenschutzgesetzgebung verabschiedet. Die entsprechende EU-Richtlinie muss aufgrund des Schengen-Assoziierungsabkommens von der Schweiz in das innerstaatliche Recht übernommen werden. Ebenso soll das revidierte Europaratsübereinkommen zum Schutz personenbezogener Daten berücksichtigt werden. Wie das eidgenössische Datenschutzgesetz müssen auch die Datenschutzgesetze der Kantone angepasst werden. Im Kanton Luzern ist eine Teilrevision des Datenschutzgesetzes vorgesehen.

Im April 2016 beschlossen das Europäische Parlament und der Rat der Europäischen Union als Teil einer umfassenden Datenschutzreform die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, die sich auf die Strafverfolgung und die Strafvollstreckung durch die zuständigen Behörden der Staaten des Schengen-Raumes bezieht. Ferner revidierte der Europarat das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Gestützt auf die europäischen Datenschutzreformen haben die eidgenössischen Räte am 25. September 2020 die Totalrevision des Bundesgesetzes über den Datenschutz verabschiedet. Bereits mit Bundesbeschluss vom 19. Juni 2020 ermächtigten die Räte den Bundesrat, das Europaratsübereinkommen zu ratifizieren.

Das kantonale Datenschutzgesetz ist an die übergeordneten Vorgaben anzupassen. Der Anpassungsbedarf für die Kantone aus dem internationalen Recht wurde von einer Arbeitsgruppe der Konferenz der Kantonsregierungen ermittelt. Deren Leitfaden bildete die Grundlage für die Ausarbeitung des Gesetzesentwurfs.

Die Vorlage des Regierungsrates sieht Ergänzungen und Präzisierungen verschiedener Bestimmungen des geltenden luzernischen Gesetzes vor. Aktualisiert wird der Katalog der besonders schützenswerten Personendaten: Neu aufgenommen werden die genetischen und die biometrischen Daten. Gemäss der Vorlage soll auf besonderen datenschutzrechtlichen Schutz der juristischen Personen verzichtet werden, wodurch das kantonale Recht mit der vorgesehenen bundesrechtlichen Regelung in Übereinstimmung gebracht wird. Die Daten juristischer Personen, das sind insbesondere die Gesellschaften des Handelsrechts wie Aktiengesellschaften, sind durch andere Erlasse genügend geschützt.

Der Gesetzesentwurf sieht Verstärkungen bei den Informations- und Meldepflichten der öffentlichen Organe und bei den Rechten der betroffenen Personen auf Auskunft über die bearbeiteten Daten vor. Bei gewissen Datenbearbeitungen werden die dem Gesetz unterstellten öffentlichen Organe verpflichtet, Datenschutz-Folgenabschätzungen zu erstellen. Des Weiteren haben die Gerichte, die Strafverfolgungs- und die Strafvollzugsbehörden innerhalb ihrer Organisationseinheiten einen Datenschutzberater oder eine Datenschutzberaterin zu bezeichnen.

Ein wichtiger Punkt der Revision ist die Stellung und Unabhängigkeit der Aufsichtsstelle im Bereich des Datenschutzes. In Übereinstimmung mit dem höheren europäischen Standard erhält der oder die Beauftragte für den Datenschutz Verfügungsbefugnisse. Im Gesetz werden Wählbarkeitsvoraussetzungen und eine Wahl auf Amtsdauer durch den Kantonsrat vorgesehen. Bereits im Voranschlag 2020 hat der Kantonsrat die finanzielle Ausstattung der Aufsichtsstelle erhöht.

Inhaltsverzeichnis

1 Ausgangslage	4
1.1 Entwicklungen auf internationaler Ebene	4
1.2 Entwicklung in der Schweiz	5
1.3 Folgerungen	6
2 Evaluierung des Datenschutzes im Kanton Luzern im Zusammenhang mit dem Schengen-Abkommen	7
3 Datenschutzreformen in den anderen Kantonen	8
3.1 Kanton Aargau	9
3.2 Kanton St. Gallen	9
3.3 Kanton Zürich	9
3.4 Folgerungen	10
4 Ergebnis der Vernehmlassung	10
4.1 Einleitung des Vernehmlassungsverfahrens	10
4.2 Vernehmlassungsergebnis	11
4.3 Wichtige Unterschiede Vernehmlassungsbotschaft - vorliegende Botschaft ...	17
5 Grundzüge der Vorlage	18
5.1 Allgemeines	18
5.2 Geltung des Datenschutzgesetzes	19
5.3 Beschränkung auf natürliche Personen und Aktualisierung des Katalogs der besonders schützenswerten Personendaten	20
5.4 Gesetzliche Grundlage für die Datenbearbeitung	21
5.5 Informationsrechte und Auskunftspflichten	21
5.6 Datenschutz-Folgenabschätzung	21
5.7 Aufsichtsstelle	22
6 Die Gesetzesentwürfe im Einzelnen	22
6.1 Datenschutzgesetz	22
6.2 Weitere Gesetze	38
6.3 Inkrafttreten	43
7 Auswirkungen	43
8 Antrag	45

Der Regierungsrat des Kantons Luzern an den Kantonsrat

Sehr geehrter Frau Präsidentin
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen mit dieser Botschaft den Entwurf einer Änderung des Gesetzes über den Schutz von Personendaten (Datenschutzgesetz, DSG) vom 2. Juli 1990 (SRL Nr. [38](#)) sowie Folgeanpassungen in weiteren Gesetzen.

1 Ausgangslage

1.1 Entwicklungen auf internationaler Ebene

1.1.1 Europäische Union

Am 27. April 2016 verabschiedeten das Europäische Parlament und der Rat der Europäischen Union eine umfassende Reform der Datenschutzgesetzgebung. Diese Reform umfasst zwei Rechtsakte: Zum einen die [Verordnung \(EU\) 2016/679](#) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung; DSGVO) und zum anderen 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 und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (im Folgenden: Datenschutzrichtlinie; DSRL). Die beiden Erlasse haben unterschiedliche Anwendungsbereiche:

- Die DSGVO ist der grundlegende Datenschutzerlass der Europäischen Union. Sie ist für die EU-Mitgliedstaaten verbindlich und gilt in diesen unmittelbar. Insbesondere können sich die Bürgerinnen und Bürger in den EU-Mitgliedstaaten auf die eingeräumten Datenschutzrechte (Informations-, Auskunfts-, Berichtigungsrechte usw.) berufen.
- Die DSRL hat dagegen keine unmittelbare Wirkung zugunsten einzelner Personen. Sie dient der Rechtsangleichung unter den Staaten, die dem Schengen-Raum und damit dem EU-Aufgabenbereich der öffentlichen Sicherheit in Europa angeschlossen sind. Wie bereits aus dem Erlassstitel ersichtlich, hat die Datenschutzrichtlinie einen spezifischeren Inhalt als die Datenschutz-Grundverordnung: Sie muss von den Staaten des Schengen-Raums hinsichtlich ihrer Strafverfolgungs- und Strafvollzugstätigkeiten umgesetzt werden. Dabei gilt sie nicht nur für grenzüberschreitende, sondern auch für die innerstaatlichen Datenbearbeitungen der Polizei- und Strafbehörden.

Die Umsetzung der Richtlinie in der Schweiz ist aufgrund der Schengen-Assoziierungsabkommen, insbesondere des Abkommens 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](#)), erforderlich. Die Beratungen der EU-Mitgliedstaaten mit den vier assoziierten Schengen-Mitgliedern (Norwegen, Island, Schweiz, Liechtenstein) fanden in den Jahren 2012–2015 statt. Entsprechend dem vorgesehenen Verfahren wurde die Datenschutzrichtlinie

der Schweiz am 1. August 2016 als schengenrelevant notifiziert. Aufgrund der Kompetenzverteilung des schweizerischen Staatsrechts im Bereich des Datenschutzes trifft die Verpflichtung, die Richtlinie innerhalb von zwei Jahren ab der Notifikation in die innerstaatliche Rechtsordnung zu übernehmen, sowohl den Bund als auch alle Kantone der Eidgenossenschaft (vgl. Art. 5 Bundesverfassung vom 18. April 1999 [BV; SR 101] sowie Art. 9 Abs. 1 Vereinbarung zwischen Bund und Kantonen betreffend Umsetzung, Anwendung und Entwicklung des Schengen/Dublin-Besitzstands vom 20. März 2009, SR 362.1).

Die DSGVO dagegen ist insofern für die Schweiz von Bedeutung, als die Europäische Kommission gestützt darauf entscheidet, ob Drittstaaten (wie die Schweiz) ein angemessenes Datenschutzniveau haben. Nur dann ist der Datentransfer aus dem EU-Gebiet in die Schweiz ohne zusätzliche Massnahmen möglich. Dieser Angemessenheitsbeschluss dient vor allem den Unternehmungen der schweizerischen Wirtschaft. Das angemessene Datenschutzniveau wird durch die Europäische Kommission periodisch überprüft. Auch hinsichtlich der Verpflichtungen aus dem Schengen-Recht finden regelmässige Überprüfungen statt (vgl. Kap. 2).

1.1.2 Europarat

Die Schweiz ist Mitglied des Europarates. Am 2. Oktober 1997 hat sie das Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ratifiziert (SR [0.235.1](#)). Dieses Übereinkommen trat am 1. Februar 2008 in Kraft. Es 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 und das seit 1. April 2008 gilt. Im Jahr 2011 leitete der Europarat das Verfahren zur Revision der beiden völkerrechtlichen Verträge ein. Unter schweizerischer Leitung wurde ein Entwurf erarbeitet und die Arbeiten im Juni 2016 abgeschlossen. Mit Beschluss vom 18. Mai 2018 hat das Minister-Komitee des Europarates dem Änderungsprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zugestimmt. Seit dem 25. Juni 2018 steht das erneuerte Übereinkommen zur Unterzeichnung durch die Mitgliedstaaten des Europarates offen. Mit Botschaft vom 6. Dezember 2019 beantragte der Bundesrat den eidgenössischen Räten die Genehmigung des Änderungsprotokolls und die Erteilung der Ermächtigung zur Ratifizierung des Abkommens (vgl. www.parlament.ch, Rubrik Geschäfte, [Nr. 19.068](#)). Mit Bundesbeschluss vom 19. Juni 2020 ermächtigten die Räte den Bundesrat zur Ratifizierung. Wie die EU-Datenschutzrichtlinie bedarf das modernisierte Europaratsübereinkommen der Umsetzung im innerstaatlichen Recht.

1.2 Entwicklung in der Schweiz

Gemäss Artikel 13 BV hat jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten. Nach der bundesgerichtlichen Rechtsprechung ist der Schutz vor Beeinträchtigungen, die durch die Bearbeitung von persönlichen Daten entstehen, Teil des Rechts auf eine Privat- und persönliche Geheimsphäre ([BGE 138 I 331 E. 5.1](#)). Das Ziel der Datenschutzgesetzgebung ist somit nicht der Schutz von Daten an sich, sondern der Schutz der Persönlichkeitsrechte von Personen, über die Personendaten bearbeitet werden, und mithin der Schutz der Freiheiten und Rechte des Einzelnen sowie seiner Handlungsautonomie. Die Datenschutzgesetze enthalten daher Grundsätze und Regeln zur Bearbeitung von Daten, die Rückschlüsse auf (natürliche) Personen zulassen, und regeln die Ansprüche des Einzel-

nen, namentlich auf Information und Berichtigung von Daten. Nach den Grundsätzen des Datenschutzrechtes ist die Bearbeitung von Personendaten durch staatliche Organen zulässig, wenn sie gesetzlich vorgesehen, im öffentlichen Interesse liegt und verhältnismässig ist. Es kommt bei der Bearbeitung der Personendaten letztlich darauf an, wofür die Daten verwendet werden.

Wie erwähnt ist in der Schweiz die Zuständigkeit zur Rechtsetzung im Datenschutz zwischen Bund und Kantonen aufgeteilt. Im Einzelnen heisst dies Folgendes:

- Das eidgenössische Datenschutzrecht gilt für Datenbearbeitungen durch private Personen und die Bundesorgane. Die Bundeskompetenz stützt sich auf die Verfassungsbestimmungen über die Ausübung privatwirtschaftlicher Tätigkeiten im schweizerischen Wirtschaftsraum 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 Datenbearbeitungen der Organe von Kantonen und Gemeinden gilt aufgrund der Organisationsautonomie der Kantone (Art. 3 BV) das kantonale Datenschutzrecht.
- Neben die eidgenössischen und kantonalen Datenschutzerlasse, die als Querschnittserlasse konzipiert sind, treten zahlreiche bereichsspezifische Datenbearbeitungsvorschriften des eidgenössischen und des kantonalen Rechts. Solche besonderen Vorschriften regeln beispielsweise den Umgang mit Personendaten durch einzelne kantonale Verwaltungsorgane (z.B. Bekanntgabe und Löschung von Personendaten aus der polizeilichen Tätigkeit).

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 verabschiedet und den eidgenössischen Räten zugeleitet. Die Botschaft enthielt ausserdem den Entwurf eines Bundesbeschlusses über die Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der EU-Datenschutzrichtlinie. National- und Ständerat beschliessen, die Vorlage aufzuteilen und gestaffelt in Kraft zu setzen. Am 28. September 2018 stimmten die Räte dem Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz, SDSG) zu (SR [235.3](#)). Das Schengen-Datenschutzgesetz gilt nur für die Bundesbehörden und nur bis zum Inkrafttreten des totalrevidierten Datenschutzgesetzes. Gleichentags verabschiedeten die Räte auch den Bundesbeschluss über die Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Datenschutzrichtlinie. Die übrigen Teile der Totalrevision verschoben die eidgenössischen Räte in eine zweite Behandlungsrunde. Mittlerweile haben der National- und der Ständerat das totalrevidierte Datenschutzgesetz beraten und am 25. September 2020 verabschiedet (vgl. www.parlament.ch, Geschäft Nr. [17059](#), und Publikation in [Bundesblatt 2020](#), S. 7639).

1.3 Folgerungen

Auslöser der Gesetzesanpassungen im kantonalen Recht sind die Rechtsentwicklungen auf internationaler Ebene. Im Datenschutz haben Bund und Kantone parallele Gesetzgebungskompetenzen. Aufgrund der verfassungsmässigen Zuständigkeiten stehen neben dem Bund somit auch die Kantone in der Pflicht, die beschlossenen Weiterentwicklungen des Europa- und Völkerrechts, die eine Vereinheitlichung des Datenschutzes in den Rechtsordnungen anstreben, zu übernehmen. Für die gesetzgeberischen Arbeiten stellt dabei ausschliesslich die Datenschutzrichtlinie

eine Weiterentwicklung im Sinn des Schengen-Rechts dar. Diese Richtlinie enthält bemerkenswert detaillierte Vorgaben, namentlich zu den Datenschutzrechten und den Zuständigkeiten, Aufgaben und Befugnissen der behördlichen Aufsichtsstelle (vgl. Art. 12-18 und 41-49 [DSRL](#)). Bei deren Übernahme haben Bund und Kantone zu entscheiden, ob sie die für den Anwendungsbereich des Schengen-Rechts vorgesehenen, den Bereich der öffentlichen Sicherheit umfassenden Regeln in das allgemeine Datenschutzrecht übernehmen wollen. Keine rechtliche Verpflichtung besteht hingegen zur Übernahme der Regelungen der Datenschutz-Grundverordnung. Ausserhalb der Schengen-Zusammenarbeit dürfen aber zwischen den Mitgliedstaaten der Europäischen Union und Drittstaaten nach EU-Recht nur personenbezogene Daten ausgetauscht werden, wenn im Drittstaat ein angemessenes Datenschutzniveau besteht. Wie der Bundesrat in seiner Botschaft zuhanden der eidgenössischen Räte dargelegt hat, soll das Datenschutzrecht an die Schengen-relevante EU-DSLR *angepasst* und im Übrigen der EU-DSGVO *angenähert* werden. Das hiesige Schutzniveau wird nämlich durch die Europäische Kommission periodisch überprüft und mittels eines sogenannten Angemessenheitsbeschlusses anerkannt. Somit hat die Datenschutzregelung der EU und vor allem deren Weiterentwicklung in Recht und Praxis eine Bedeutung für Nichtmitgliedsländer wie die Schweiz und deren Wirtschaft. In Anbetracht des sachlichen Zusammenhangs empfiehlt sich ausserdem, das parallel zum Schengen-Recht erneuerte Europaratsübereinkommen im Rahmen der vorliegenden Revision zu berücksichtigen. Auch der Leitfaden der Konferenz der Kantonsregierungen (KdK) zur Umsetzung der EU-Datenschutzrichtlinie sowie des revidierten Europaratsübereinkommens empfiehlt dieses Vorgehen. Der Inhalt des revidierten Übereinkommens entspricht grösstenteils den EU-Datenschutzerlassen. Es enthält die gleichen datenschutzrechtlichen Instrumente, wie Melde- und Informationspflichten sowie die Datenschutz-Folgenabschätzung, und macht Vorgaben für die unabhängige Aufsichtsstelle; diese Regelungen sind im Vergleich zu diejenigen der EU lediglich etwas weniger detailliert.

2 Evaluierung des Datenschutzes im Kanton Luzern im Zusammenhang mit dem Schengen-Abkommen

In Zusammenhang mit der Anwendung des Schengen-Abkommens durch die angeschlossenen Staaten besteht ein Evaluierungs- und Überwachungsmechanismus, der verschiedene Evaluierungsprogramme vorsieht. Im Februar und März 2018 prüfte ein Expertenteam aus den anderen Schengen-Mitgliedstaaten, ob die Schweiz die Vorgaben des Abkommens einhält. Neben eidgenössischen Behörden besuchten die Expertinnen und Experten den Beauftragten für den Datenschutz des Kantons Luzern und die Luzerner Polizei. Der Bericht vom 4. Februar 2019 beurteilt Struktur, Befugnisse, Budget und Unabhängigkeit der Datenschutzbehörden in der Schweiz und im Kanton Luzern, deren Überwachung der Nutzung der Datenverarbeitungssysteme des Schengen-Rechts, die Rechte der betroffenen Personen bei solchen Datenbearbeitungen, die Bearbeitung von Personendaten in ausgewählten Datenverarbeitungssystemen sowie die Information der Öffentlichkeit und die internationale Zusammenarbeit im Schengen-Raum durch die Schweizer Behörden. Gestützt auf den Bericht hat der Rat der Europäischen Union am 7. März 2019 einen [Durchführungsbeschluss](#) zur Festlegung einer Empfehlung zur Beseitigung der bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes festgestellten Mängel angenommen und diesen samt den Empfehlungen veröffentlicht. Unser Rat hat von der entsprechenden Mitteilung des Bundesamtes

für Justiz vom 26. März 2019 Kenntnis genommen. In der Folge haben wir die Bundesbehörde über das geplante Vorgehen bei der Umsetzung der Empfehlungen, zur Hauptsache also über den laufenden Gesetzgebungsprozess, informiert.

Hinsichtlich des Datenschutzes lassen sich die Empfehlungen wie folgt gruppieren: Zum einen beziehen sie sich auf den Betrieb und die Nutzung zweier Datenverbände, des Visa-Informationssystems (VIS) für die Durchsetzung der europäischen Visum-Ordnung gegenüber Drittländern und des Schengener Informationssystems (SIS) für die europaweiten Personen- und Sachfahndungen, durch die eidgenössischen und kantonalen Behörden sowie die Aufsicht des Eidgenössischen Datenschutzbeauftragten und der kantonalen Datenschutzaufsichtsstellen. Zum andern umfassen die Empfehlungen institutionelle Fragen des eidgenössischen und kantonalen Datenschutzes. Zentral dabei ist, dass die Aufsichtsstellen mit einer Unabhängigkeit ausgestattet sind, die es ihnen ermöglicht, ihre Aufgaben ohne äussere Einflussnahme wahrzunehmen. Im Folgenden sind die Empfehlungen der Evaluierung aufgeführt, welche die Stellung der Datenschutzbehörden von Bund und Kantonen und insbesondere des luzernischen Beauftragten für den Datenschutz betreffen: Im Hinblick auf eine bessere Gewährleistung der vollständigen Unabhängigkeit des Datenschutzbeauftragten lautet eine Empfehlung, es sei die Möglichkeit abzuschaffen, dass der Beauftragte für den Datenschutz «aus triftigen Gründen (was andere Gründe als schwerwiegendes Fehlverhalten umfasst) entlassen werden kann». Weiter sollten die Durchsetzungsbefugnisse des Beauftragten gestärkt werden, indem ihm die Kompetenz verliehen wird, rechtsverbindliche Entscheidungen zu treffen. Der Beauftragte sollte zudem im Interesse der vollständigen Unabhängigkeit in die Lage versetzt werden, Mitarbeiterinnen und Mitarbeiter entsprechend seinen Anforderungen selbst einzustellen. Des Weiteren sollte das Finanzhaushaltsverfahren so reformiert werden, dass die Aufsichtsstelle konkreten Einfluss auf den Vorschlag für ihren eigenen Finanzhaushalt hat, bevor der Gesamtvoranschlag dem Parlament zwecks Beratung und Verabschiedung unterbreitet wird. Der Aufsichtsstelle sollte ausserdem eine sogenannte Haushaltsautonomie eingeräumt werden, sodass sie Haushaltsentscheidungen, die sie betrifft, beeinflussen und kontrollieren kann. Weitere Empfehlungen gehen schliesslich dahin, dass ausreichende finanzielle und personelle Ressourcen bereitzustellen seien, namentlich um auch Eingaben von Privatpersonen zu behandeln. Auf diese Punkte gehen wir allesamt in unseren Ausführungen zum Ergebnis des Vernehmlassungsverfahrens ein, bildeten sie doch auch Gegenstand unseres Vernehmlassungsentwurfs zur Aktualisierung des kantonalen Datenschutzgesetzes oder waren Gegenstand entsprechender Forderungen in der Vernehmlassung (vgl. Kap. 4.2).

3 Datenschutzreformen in den anderen Kantonen

In den Kantonen sind die Bemühungen um die Aktualisierung der Datenschutzerlasse unterschiedlich weit gediehen. Im Kanton Bern hat der Regierungsrat am 4. Juli 2018 eine dringliche Einführungsverordnung zur EU-Datenschutzrichtlinie (BSG Nr. 152.043) erlassen. Im Kanton Aargau ist die Gesetzesrevision bereits auf den 1. August 2018 in Kraft getreten. Im Kanton Zürich hat der Regierungsrat die Anpassungen des Gesetzes über die Information und den Datenschutz an die europäische Datenschutzreform am 4. Juli 2018 zuhanden des Kantonsparlamentes verabschiedet, und dieses hat die Gesetzesänderung am 25. November 2019 beschlossen. Die Regierung des Kantons St. Gallen hat dem Kantonsparlament am

9. Oktober 2018 Botschaft und Entwurf zum Datenschutzgesetz unterbreitet; die Gesetzesänderung ist am 25. Juni 2019 in Kraft getreten (sGS Nr. 142.1). Im Folgenden legen wir die Rechtslage in den Kantonen Aargau, St. Gallen und Zürich dar.

3.1 Kanton Aargau

Im Aargauer Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (SAR Nr. 150.700) wurden der Geltungsbereich des Gesetzes und die datenschutzrechtlichen Begriffe (u.a. Beschränkung auf Daten von natürlichen Personen) auf das internationale Recht abgestimmt. Klarer gefasst wurden im Gesetz die Informationspflicht der öffentlichen Organe bei der Beschaffung von Personendaten sowie das Recht auf Löschung der Daten, das im geltenden Recht nicht ausdrücklich erwähnt war. Aufgenommen wurden sodann das Instrument der Datenschutz-Folgenabschätzung für geplante Datenbearbeitungsvorgänge und eine erweiterte Pflicht zur Vorabkonsultation des oder der Beauftragten für Öffentlichkeit und Datenschutz. Neu aufgenommen wurden Meldepflichten bei unbefugten Datenbearbeitungen und Datenverlusten, sofern diese zu einem Risiko für die Rechte der betroffenen Personen führen. Aufgehoben wurden Bestimmungen über Pilotprojekte und Evaluationen sowie das Register der Datensammlungen, ausgenommen die Register über die Datenbearbeitungstätigkeiten der Strafbehörden, die neu in den Spezialerlassen Aufnahme fanden. Stellung und Unabhängigkeit des oder der Beauftragten für Öffentlichkeit und Datenschutz wurden durch die Gesetzesrevision gestärkt. So ist festgelegt, dass der oder die Beauftragte nach Abschluss einer Untersuchung Verfügungen erlassen kann. Vorher richtet der oder die Beauftragte in der Regel eine Empfehlung an das öffentliche Organ (z.B. eine bestimmte Datenbearbeitung einzustellen).

3.2 Kanton St. Gallen

Im Kanton St. Gallen enthält das geänderte Datenschutzgesetz (sGS Nr. 142.1) Neuerungen bei den datenschutzrechtlichen Begriffen und beim Geltungsbereich (u.a. Streichung der juristischen Personen). Des Weiteren regeln neue Vorschriften die Datenschutz-Folgenabschätzung und die Vorabkonsultation sowie die Wahrnehmung der Meldepflichten bei Verletzungen der Datensicherheit. Ausführlich geregelt wird sodann die Anlage von Verzeichnissen der Bearbeitungstätigkeiten von Justizbehörden und Polizei. Nicht aufgehoben wird dagegen das Register der Datensammlungen der öffentlichen Organe. Hinsichtlich der Organisation und der Stellung des Leiters oder der Leiterin der kantonalen Fachstelle für Datenschutz sind folgende Anpassungen an das internationale Recht vorgesehen: Wahl auf eine Amtsdauer von vier Jahren und Unvereinbarkeitsvorschriften sowie Befugnis zur Anstellung von Mitarbeiterinnen und Mitarbeitern sowie zum Erlass von Verfügungen, wenn absehbar ist, dass das öffentliche Organ eine Empfehlung ablehnen oder ihr nicht Folge leisten wird.

3.3 Kanton Zürich

Im Gesetz über die Information und den Datenschutz (IDG, LS Nr. 170.4) sind Änderungen bei den datenschutzrechtlichen Begriffen aufgenommen worden. Weitere Änderungen betreffen die Datenschutz-Folgenabschätzungen und die Vorabkontrolle sowie die Meldepflichten bei einer unbefugten Datenbearbeitung oder nach einem Datenverlust, wenn die Grundrechte der betroffenen Personen gefährdet sind. Präzisiert werden sodann die Informationspflichten der öffentlichen Organe bei der Beschaffung von Personendaten. In die Gerichts-, Straf- und Justizvollzugsgesetzgebung wurden Bestimmungen aufgenommen, welche die zuständigen kantonalen Verwaltungs- und Gerichtsbehörden verpflichten, eine für die Datenschutzberatung

innerhalb der Organe zuständige Person zu bezeichnen. Diese Person berät und unterstützt die entsprechende Behörde in Datenschutzbelangen, nimmt Datenschutz-Folgeabschätzungen vor und ist Ansprechperson des oder der Beauftragten für den Datenschutz und arbeitet mit dieser oder diesem zusammen. Der oder die Beauftragte für den Datenschutz kann bei Verletzungen von Datenschutzbestimmungen eine Verfügung erlassen und beispielsweise die Einstellung der Datenbearbeitung verlangen.

3.4 Folgerungen

Die Anpassungen der Datenschutzgesetze in den Kantonen umfassen die Einführung neuer Instrumente (insbes. Datenschutz-Folgenabschätzung) und die Verbesserungen bestehender Instrumente (u.a. Regelungen über Informationspflicht) im Sinn der europäischen Datenschutzreform. Dabei unterscheiden sich die kantonalen Entwürfe zum Teil in ihrer Regelungsdichte, was sich beispielsweise in den Bestimmungen über die Vorabkontrolle zeigt. Teilweise sehen die Kantone auch administrative Vereinfachungen vor, namentlich indem die Pflicht zur Führung des Registers über die Datensammlungen für die allgemeine Verwaltung aufgehoben wird. Die Kantone nehmen in den Aktualisierungen ihrer Datenschutzgesetze die internationalen und nationalen Entwicklungen auf. Hinsichtlich der Stellung und Organisation der kantonalen Aufsichtsstelle ist der Anpassungsbedarf unterschiedlich: Verschiedene Kantone haben bereits vor der Gesetzesrevision die erhöhten Anforderungen der europäischen Datenschutzreform erfüllt (AG und ZH hinsichtlich der Wahl auf Amtsdauer, SG und ZH hinsichtlich der Ausgabenkompetenz des oder der Beauftragten für den Datenschutz im Rahmen des entsprechenden vom Kantonsparlament verabschiedeten Voranschlags). Eine Aufteilung der Datenschutzgesetzgebung in Bestimmungen, die im Sinn der EU-Datenschutzrichtlinie für die Strafbehörden und die Organe des Strafvollzugs gelten, und in Bestimmungen, die für die übrigen Verwaltungszweige gelten, hat ausser bei einzelnen übergangsrechtlichen Festlegungen keiner der näher betrachteten Kantone vorgenommen.

4 Ergebnis der Vernehmlassung

4.1 Einleitung des Vernehmlassungsverfahrens

Die Vorarbeiten zur Aktualisierung des kantonalen Datenschutzgesetzes gehen auf das Jahr 2017 zurück. Mithilfe des Leitfadens der Konferenz der Kantonsregierungen sowie der Vernehmlassung und in der Folge der Botschaft des Bundesrates zur Totalrevision des eidgenössischen Datenschutzgesetzes erarbeitete das Justiz- und Sicherheitsdepartement die Vernehmlassungsunterlagen. Dabei wurde der damalige kantonale Beauftragte für den Datenschutz einbezogen. Im Februar 2018 ermächtigte unser Rat das Justiz- und Sicherheitsdepartement, den Entwurf einer Änderung des Datenschutzgesetzes und der damit zusammenhängenden übrigen Gesetzesanpassungen in die Vernehmlassung zu geben. Das Vernehmlassungsverfahren dauerte bis Anfang Mai 2018. Zur Vernehmlassung eingeladen waren die politischen Parteien, alle Einwohnergemeinden, der Verband Luzerner Gemeinden (VLG), der Luzerner Anwaltsverband, die Demokratischen Juristinnen und Juristen Luzern, das Kantonsgericht und die Departemente sowie die Staatskanzlei. Ihre Stellungnahmen werden im Folgenden zusammengefasst und soweit erforderlich auch bei der Kommentierung der Bestimmungen miteinbezogen (vgl. Kap. 6). Zur besseren Abgrenzung des kantonalen Datenschutzgesetzes vom Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1), die in der Gesetzessprache heute beide mit DSG abgekürzt werden, wird das kantonale Gesetz, wie mit dieser Botschaft für die künftige Anwendung beantragt, bereits mit KDSG abgekürzt.

4.2 Vernehmlassungsergebnis

4.2.1 Allgemeines

Aus den Stellungnahmen der politischen Parteien und der übrigen Organisationen vom Mai 2018 geht hervor, dass sie überwiegend und im Grundsatz die Notwendigkeit einer Aktualisierung des geltenden kantonalen Datenschutzgesetzes anerkennen oder wenigstens nicht ausdrücklich in Frage stellen. Die CVP weist die Vorlage zwar zurück, fordert indes eine gelegentliche Überarbeitung mit minimalen Anpassungen unter Berücksichtigung der Beratungen und Beschlüsse der eidgenössischen Räte. Die SVP betont ihre Grundhaltung, dass der Staat kostengünstig und effizient sein muss, und verlangt, dass er dies auch bei der Datenbearbeitung sein solle. Sie erachtet den Zeitpunkt, um das Gesetz anzupassen, insbesondere mit Verweis auf die hängige Totalrevision des eidgenössischen Datenschutzgesetzes, als zu früh und verlangt eine Sistierung der Gesetzgebungsarbeiten. Die FDP dagegen weist insbesondere darauf hin, dass es in der Verantwortung der Kantone liege, einen zum europäischen Recht als gleichwertig beurteilten Datenschutz zu schaffen, um den Zugang zum Schengen-Informationssystem nicht zu gefährden. Die heutigen rechtlichen Bestimmungen im Kanton Luzern genügten diesen Anforderungen nicht. Die SP nimmt vom Vernehmlassungsentwurf grundsätzlich positiv Kenntnis, lehnt aber auch – wie die Grünen – darin vorgesehene Lockerungen ab. Die GLP äussert sich nur zu Einzelfragen des Vernehmlassungsentwurfs und lässt somit keine grundsätzlichen Bedenken verlauten.

Ausschlaggebend für die Eröffnung des Vernehmlassungsverfahrens im Februar 2018 waren verschiedene Gründe. Mit den EU-Erlassen und dem verabschiedeten Europaratsübereinkommen, der Botschaft des Bundesrates zum Bundesgesetz sowie dem KdK-Leitfaden zur Anpassung der kantonalen Erlasse lagen die wichtigsten Grundlagen zur Ausarbeitung einer eigenen Vernehmlassungsvorlage vor. Wie in Kapitel 3 dargelegt, hatten andere Kantone ebenfalls mit gesetzgeberischen Vorarbeiten begonnen. Nach dem Schengen-Recht sind Bund und Kantone verpflichtet, innert einer zweijährigen Frist ihre Rechtsgrundlagen anzupassen. Mit der Eröffnung des Vernehmlassungsverfahrens sollten der Wille zur Aktualisierung des luzernischen Datenschutzrechts zum Ausdruck kommen und diese Bemühungen in die damals anstehende Evaluation des luzernischen Datenschutzes im Rahmen des Abkommens von Schengen einfließen. Unsere Vernehmlassungsvorlage enthielt bewusst keine Angaben zum Zeitplan der Gesetzgebung. Es sollte aufgrund der damals bereits absehbaren strittigen Punkte betreffend die finanzielle Ausstattung und die künftige Finanzierung des Datenschutzes im Kanton Luzern genügend Zeit zur Bearbeitung dieses Themas vor der Festlegung des definitiven Gesetzesentwurfs und der Botschaft eingeplant werden können. Im August 2018 beauftragte unser Rat deshalb das für die Gesetzgebungsarbeiten zuständige Justiz- und Sicherheitsdepartement und die administrativ zuständige Staatskanzlei, mit dem Verband Luzerner Gemeinden sowie der Stadt Luzern den Dialog über die künftige Organisation und Finanzierung der Datenschutzaufsichtsstelle zu führen. Dieser Prozess mündete im März 2020 in eine Anhörung der Gemeinden zu den abgeänderten Bestimmungen über die Mitfinanzierung und die Mitsprache der Gemeinden. In Anbetracht der wiederum negativen Rückmeldungen enthält der vorliegende Entwurf indes keine Bestimmungen mehr dazu (vgl. unsere Ausführungen in Kap. 4.2.3). Mittlerweile hat der Bund die Datenschutzrevision verabschiedet und auch die Evaluation der schweizerischen Datenschutzbehörden durch die Schengen-Kommission ist ab-

geschlossen (vgl. unsere Ausführungen in Kap. 1 und 2). Wir erachten den Zeitpunkt nun als gekommen, Ihrem Rat die Botschaft mit den Gesetzesänderungen zu unterbreiten. Im Folgenden gehen wir auf umstrittene Punkte der Vernehmlassung ein.

4.2.2 Befugnisse des oder der Beauftragten für den Datenschutz

Zur Befugnis des oder der Beauftragten für den Datenschutz, bei Verletzung von Datenschutzvorschriften einen Entscheid zu erlassen, wenn das für die Einhaltung der Datenschutzvorschriften verantwortliche Organ der Empfehlung des Beauftragten nicht folgt, haben sich die CVP und der VLG negativ geäußert. FDP, Grüne und SP stimmen dieser neuen Entscheidkompetenz zu. Die FDP verlangt zusätzlich ein Anzeigerecht des oder der Beauftragten. Die SP erachtet die Kann-Formulierung bei der Abgabe von Empfehlungen als unzureichend.

Eine Anforderung der eingangs erwähnten völker- und europarechtlichen Regelwerke ist, dass die Aufsichtsstellen im Bereich des Datenschutzes Entscheidungsbeziehungsweise Verfügungskompetenzen bekommen müssen. § 24 unseres Entwurfs setzt diese übergeordneten Anforderung zur Stärkung der datenschutzrechtlichen Aufsichtsbehörde um. Mit dem Erfordernis, dass der oder die luzernische Beauftragte für den Datenschutz gegenüber dem verantwortlichen Organ zunächst eine Empfehlung aussprechen soll, bevor ein formeller Entscheid ergeht, nehmen wir den zur Verfügung stehenden Spielraum insbesondere zugunsten der Gemeinden wahr (vgl. § 24 Abs. 3 und 4 KDSG-Entwurf).

Auf weiter gehende Regelungen zum Anzeigen- und Bussenrecht für den Beauftragten oder die Beauftragte für den Datenschutz wird im vorliegenden Entwurf weiterhin verzichtet, sind doch solche Instrumente innerhalb der Verwaltung wenig sinnvoll. Der oder die Beauftragte kann bei Bedarf bei Verletzungen von Bestimmungen des Datenschutzes gegenüber der Verwaltung Änderungen an der Datenbearbeitung oder deren Abbruch verfügen. Sollten die verfügten Massnahmen nicht wirksam sein, besteht nach den allgemeinen Regeln des Verfahrensrechts die Möglichkeit, an die Aufsichtsbehörde zu gelangen. Auch ist eine Strafanzeige schon nach geltendem Recht nicht ausgeschlossen (vgl. § 46a Abs. 2 Gesetz über das öffentlich-rechtliche Arbeitsverhältnis vom 26. Juni 2001 [PG; SRL Nr. 51] und § 24c KDSG).

An der teilweise kritisierten Kann-Bestimmung zum Aussprechen von Empfehlungen halten wir fest: Damit hat der oder die Beauftragte die Möglichkeit, im Rahmen seines pflichtgemässen Ermessens auf eine Empfehlung zu verzichten, wenn diese nicht nötig ist (z.B. wegen der Geringfügigkeit der Verletzung der Datenschutzvorschrift oder bei bereits erfolgter einfacher Behebung).

Bei den Befugnissen, die dem oder der Beauftragten für den Datenschutz in finanzieller Hinsicht zustehen, ist zwischen zwei Bereichen zu unterscheiden: Zum einen geht es um die Frage, ob der oder die Beauftragte Ihrem Rat, der den kantonalen Voranschlag festlegt, ein eigenes Globalbudget vorlegen darf, wie es nach geltendem Recht das Kantonsgericht und die Finanzkontrolle im Rahmen des Voranschlagsentwurfs unseres Rates unterbreiten. Zum anderen geht es darum, ob der oder die Beauftragte im Rahmen des von Ihrem Rat beschlossenen Voranschlags einerseits und der gesetzlichen Kompetenzen andererseits Ausgaben beschliessen kann (insbes. im Hinblick auf die Anstellung von eigenem Personal). Nach gelten-

dem Datenschutzrecht hat der Beauftragte für den Datenschutz keine Ausgabenkompetenzen. Das Budgetantragsrecht beziehungsweise die unveränderte Vorlage des Globalbudgets des oder der Beauftragten für den Datenschutz durch unseren Rat wurde in der Vernehmlassung von der FDP und den Grünen sowie vom damaligen Beauftragten für den Datenschutz verlangt. Die CVP lehnt ein solches Ansinnen ausdrücklich ab.

In Übereinstimmung mit unserer Beurteilung in der Teilrevision 2007 lehnen wir eine Regelung, wonach unser Rat Ihrem Rat ein vom Beauftragten oder von der Beauftragten für den Datenschutz erarbeitetes Globalbudget unverändert vorlegen muss, weiterhin ab (vgl. dazu unsere Ausführungen in der [Botschaft B 171](#) zum Entwurf von Änderungen des Datenschutzgesetzes und des Gesundheitsgesetzes vom 16. Januar 2007). Im Vergleich zu den anderen Aufgabenbereichen und zum Gesamtaufwand aller Ausgaben des Staatshaushalts weist der Aufwand für den Bereich des Datenschutzes – auch nach der im Voranschlag 2020 vorgenommenen Aufstockung – einen geringen Umfang auf. Die administrativen Aufwendungen für ein eigenes Globalbudget (Systembetreuung, Planungs-, Budget-, Rechnungsprozesse usw.) lassen sich deshalb nicht rechtfertigen. Während das Globalbudget der Gerichte per saldo Aufwendungen von rund 28 Millionen Franken umfasst und das Globalbudget der Finanzkontrolle immerhin solche von rund 1,4 Millionen Franken, sind für die Belange des Datenschutzes im Jahr 2020 340'000 Franken eingestellt. Ein eigenes Globalbudget lässt sich angesichts des geringen Umfangs nicht begründen. Zudem haben wir bereits im Aufgaben- und Finanzplan 2020–2023 eine pragmatische Lösung umgesetzt: Im Aufgabenbereich «H0-1010 Staatskanzlei» wird eine eigene Leistungsgruppe neben den bestehenden Leistungsgruppen «Kantonsrat» und «Regierungsrat» geführt. Diese Lösung gibt der unabhängigen Stellung der Datenschutzaufsichtsstelle auch bei den Staatsfinanzen besser Ausdruck, ohne dass die administrativen Nachteile eines separaten Globalbudgets beziehungsweise Aufgabenbereichs in Kauf genommen werden müssen. Die für den Datenschutz vorgesehenen Mittel sollen nun im Voranschlag und in der Rechnung separat ausgewiesen und damit die Transparenz gegenüber Parlament und Öffentlichkeit erhöht werden. Ihr Rat kann im Rahmen von Budget- und Rechnungsdebatten die Leistungen und deren Finanzierung gezielter beraten. Obwohl sich der rechtlich verbindliche Voranschlagskredit nach wie vor auf das gesamte Globalbudget der Staatskanzlei (und somit alle drei Leistungsgruppen gemeinsam) bezieht, könnten in der Jahresrechnung allfällige Ausgabenverschiebungen zwischen den einzelnen Leistungsgruppen erkannt werden und der Kantonsrat könnte bei Bedarf korrigierend Einfluss nehmen. Auch steht es der vorberatenden Kommission frei, bei der Vorberatung des Finanzhaushalts in sinngemässer Anwendung von § 25 des Kantonsratsgesetzes den Beauftragten oder die Beauftragte für den Datenschutz zu befragen. Wir gehen davon aus, dass diese auf die luzernischen Verhältnisse angepasste Lösung der Anforderung der Richtlinie, dass die Aufsichtsbehörde über eigene Haushaltspläne verfügt, zu genügen vermag.

Im Sinn der höheren Anforderungen an die Unabhängigkeit des oder der Beauftragten für den Datenschutz sieht unser Entwurf ausserdem vor, ihm oder ihr die Kompetenz zu erteilen, im Rahmen des ihm oder ihr zustehenden Voranschlagskredits Personal- und Sachausgaben zu tätigen (vgl. unsere Ausführungen zu § 22b KDSG-Entwurf in Kap. 6.1).

4.2.3 Finanzierung der Aufsichtsstelle: Beteiligung der Gemeinden?

Der im Vernehmlassungsentwurf enthaltene Vorschlag, die Aufwendungen für den Beauftragten oder die Beauftragte für Datenschutz hälftig zwischen dem Kanton und den Gemeinden zu teilen, findet bei den Gemeinden und dem Verband der Luzerner Gemeinden (VLG) keine Zustimmung. In Gesprächen mit dem VLG wurde herausgearbeitet, dass die heutige Organisationsform des luzernischen Beauftragten für den Datenschutz Vorteile für Kanton und Gemeinden hat. Letztere haben nicht die kritische Grösse, um selber eine unabhängige Aufsichtsstelle über die Datenbearbeitungen ihrer Verwaltungen zu betreiben. Auch eine Lösung auf regionaler Ebene wäre aus demselben Grund wenig geeignet. Eine Finanzierung über Gebühren wiederum wäre angesichts der unabhängigen Stellung und der Befugnisse der Aufsichtsstelle wie auch der administrativen Aufwendungen und der praktischen Anwendung eines Gebührentarifs in Aufsichts- und Kontrollangelegenheiten nicht die beste Lösung. Des Weiteren erachten wir den Einkauf von Beratungsleistungen bei Dritten durch die Gemeinden nicht als zweckmässig, zumal die Aufsichtsverantwortung nicht eingekauft werden könnte. Zu berücksichtigen ist schliesslich im Zusammenhang mit der anstehenden Gesetzesrevision, dass Aufgaben, Organisation und Kompetenzen der Aufsichtsstelle vermehrt internationalen Vorgaben genügen müssen. Wir sind überzeugt, dass hinsichtlich der künftigen Aufsicht der gemeinsame Datenschutzbeauftragte von Kanton und Gemeinden die beste Lösung ist, verbunden mit der Möglichkeit für Gemeinden mit grösseren Verwaltungen, für sich bedarfsgerecht eine organisationsinterne Datenschutzberatung einzurichten, welche keine Anforderungen an die institutionelle Unabhängigkeit erfüllen muss.

Der oder die Beauftragte für den Datenschutz kann wegen der institutionellen Stellung nicht mit den Fachstellen der kantonalen Verwaltung verglichen werden, die Aufsichtstätigkeiten wahrnehmen; er oder sie hat eine spezielle und eigenständige Rolle. Nach Rücksprache mit dem VLG hat unser Rat deshalb das Justiz- und Sicherheitsdepartement beauftragt, die Gemeinden in einer zusätzlichen Anhörung mit diesen Überlegungen zur Stellung des Beauftragten für den Datenschutz vertraut zu machen. Dabei wurde vorgeschlagen, den Gemeinden insofern entgegenzukommen, als die Mitfinanzierung der Gemeinden auf den Anteil von einem Drittel reduziert und ihnen Mitspracherechte eingeräumt werden sollen. Auch dieser Vorschlag stiess indes nicht auf Zustimmung. Unser Rat verzichtet daher in dieser Botschaft auf die Vorlage einer Bestimmung zur Mitfinanzierung der Aufsichtsstelle durch die Gemeinden. Dies hat unweigerlich zur Folge, dass ein weiterer Ausbau der Stelle und damit auch der Ausbau der Leistungen für die Gemeinden in nächster Zeit nicht im Vordergrund stehen kann, obwohl das Gesetz Neuerungen einführt.

4.2.4 Parlamentarische Zuständigkeiten und Abläufe

4.2.4.1 Wahl durch den Kantonsrat auf Amtsdauer

Die Wahl des oder der Beauftragten für den Datenschutz durch den Kantonsrat auf Antrag des Regierungsrates wird im Vernehmlassungsverfahren von FDP, SVP und GLP ausdrücklich befürwortet. Die anderen Parteien haben sich dazu nicht geäussert. Die FDP und der damalige Beauftragte für den Datenschutz regen zusätzlich an, die Zuständigkeit bei einer allfälligen Kündigung zu regeln.

In unserem Entwurf ist – wie schon im Vernehmlassungsentwurf – die Wahl des oder der Beauftragten für den Datenschutz durch den Kantonsrat auf Antrag des Regierungsrates vorgesehen. Auch ist eine Amtsdauer von vier Jahren vorgesehen, ohne Einschränkungen bei der Wiederwahl. Mit der Parlamentswahl und

dem Amtsdauersystem wird die Unabhängigkeit des oder der Beauftragten für den Datenschutz gestärkt, dies im Sinn der Bestrebungen auf internationaler und nationaler Ebene. Dabei bleibt der oder die Beauftragte für den Datenschutz dem kantonalen Personalgesetz unterstellt. Gemäss diesem gelten die Bestimmungen über die Auflösung des Arbeitsverhältnisses auch für die auf Amtsdauer gewählten Angestellten des Kantons (§ 23 Abs. 3 i.V.m. §§ 19–22 PG). Deren Arbeitsverhältnis kann aus wichtigen Gründen ohne Einhaltung von Fristen jederzeit aufgelöst werden; als wichtiger Grund gilt namentlich jeder Umstand, bei dessen Vorhandensein die Fortsetzung des Arbeitsverhältnisses nach Treu und Glauben nicht mehr zugemutet werden darf (§ 9 Abs. 2 PG). Bei Angestellten, die von einem gesetzgebenden Organ gewählt werden, ist hierfür die Aufsichtsbehörde zuständig (§ 19 Abs. 3 PG). Wir schlagen vor, die für die Auflösung aus wichtigen Gründen geltende Regelung des Finanzkontrollgesetzes in das Kantonale Datenschutzgesetz zu übernehmen. Demnach kann der Regierungsrat das Arbeitsverhältnis des oder der Beauftragten für den Datenschutz aus wichtigen Gründen vor Ablauf der Amtsdauer zwar auflösen, muss jedoch dafür die Genehmigung der Geschäftsleitung des Kantonsrates einholen (§ 22 Abs. 1^{ter} KDSG-Entwurf; vgl. § 3 Abs. 4 Finanzkontrollgesetz vom 8. März 2004, SRL Nr. 615). Mit dieser Lösung wird die Handlungsfähigkeit bei Vorliegen ausserordentlicher Umstände gewahrt und der Wahlkompetenz des Kantonsrates Rechnung getragen. Wir gehen davon aus, dass die Kombination der personalrechtlichen Auflösungsregel mit der parlamentsrechtlichen Zustimmung eine allfällige Entlassung vor Ablauf der Amtsdauer nur bei schwerwiegenden Verfehlungen zulässt.

Die Datenschutzrichtlinie verpflichtet die Schengen-Staaten zur Regelung des Ernennungsverfahrens, lässt ihnen jedoch die Wahl zwischen Ernennung der Mitglieder der Aufsichtsstelle durch das Parlament, die Regierung, das Staatsoberhaupt oder ein unabhängiges Organ. Zur Stärkung der Unabhängigkeit sind ausserdem Wählbarkeitsvoraussetzungen und eine Wahl auf Amtsdauer vorzusehen sowie eine Beschränkung der Amtsenthebung gestützt nur auf Gründe einer schweren Verfehlung oder fehlender Voraussetzungen bei der Aufgabenerfüllung. Eine wesentliche Anforderung ist, dass die Aufsichtsstellen im Bereich des Datenschutzes über institutionelle Garantien zur erforderliche Unabhängigkeit verfügen müssen. In Übereinstimmung mit unserer Stellungnahme zum (inzwischen zurückgezogenen) [Postulat P 251](#) von Rosy Schmid-Ambauen über eine Überprüfung der Legislaturdauer ist die übliche vierjährige Amtsdauer vorgesehen. 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. § 22a KDSG-Entwurf).

4.2.4.2 Abläufe in Kommission und Kantonsrat

Im Zusammenhang mit der Aufgabenerfüllung und Finanzierung der Aufsichtsstelle sieht unser Entwurf neu eine Verbesserung in der parlamentarischen Begleitung vor. Inskünftig soll der Kantonsrat die Möglichkeit haben, den (politisch) erwünschten Rahmen für den Datenschutz im Kanton Luzern im direkten Dialog mit dem oder der Beauftragten für den Datenschutz – und unter Achtung der vom Gesetz garantierten fachlichen Unabhängigkeit der Aufsichtsstelle – zu klären. Wie die Finanzkontrolle soll der oder die Beauftragte für den Datenschutz den jährlichen Tätigkeitsbericht inskünftig der Aufsichts- und Kontrollkommission (AKK) und der Planungs- und Finanzkommission (PFK) vorlegen (§ 23 Abs. 3 KDSG-Entwurf; vgl. § 17 Abs. 1 Finanzkontrollgesetz). Letztere Kommission könnte sich inskünftig im Rahmen der

Behandlung des politischen Leistungsauftrags als Teil des Aufgaben- und Finanzplans wie auch bei der Behandlung des Tätigkeitsberichtes, der sich beispielweise zu Schwerpunkten der Aufsichtstätigkeiten und zu einem Ausblick äussern könnte, näher mit Datenschutzanliegen befassen. Sofern nötig, kann die mit der Datenschutzgesetzgebung befasste Kommission Justiz und Sicherheit einen Mitbericht zuhanden der PFK oder auch der AKK verfassen. Aufwendigere Alternativlösungen wie eine Milizkommission (wie im Kanton Freiburg) oder eine parlamentarische Sonderkommission haben wir verworfen. Ebenfalls abzusehen ist von einer formellen Genehmigung des Tätigkeitsberichtes durch den Kantonsrat. Im Kantonsratsgesetz ist eine solche Genehmigung nur bei den Jahresberichten gemäss Gesetz über die Steuerung der Finanzen und Leistungen (FLG; SRL Nr. 600) und den besonderen Rechenschaftsberichten von Regierungsrat und Kantonsgericht vorgesehen (§ 80 Kantonsratsgesetz, KRG; SRL Nr. 30). Die Kenntnisnahme ist beispielsweise bei den Geschäftsberichten von Universität und Pädagogischer Hochschule Luzern üblich. Mit dieser Lösung erachten wir die Unabhängigkeit des oder der Beauftragten für den Datenschutz in fachlicher Hinsicht als am besten gewährleistet.

4.2.5 Datenschutzrechtliche Instrumente

4.2.5.1 Katalog der besonders schützenswerten Personendaten

In Übereinstimmung mit den Zielen des europäischen Rechts und des revidierten Datenschutzgesetzes 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 heikel ist und die nach einem qualifizierten Schutz verlangen. Neu werden genetische Daten und die sogenannten biometrischen Daten in die Kategorie der besonders schützenswerten Daten aufgenommen. Im Vernehmlassungsverfahren begrüssen FDP, GLP, Grüne und SP die geplante Aktualisierung des Katalogs der besonders schützenswerten Daten. Die FDP regte an, die Daten über das Sexualleben und die sexuelle Orientierung ebenfalls besonders zu schützen. Die GLP wünschte sich einen abschliessenden Katalog der besonders schützenswerten Personendaten.

Wir erachten den im geltenden Recht verwendeten Begriff der Intimsphäre als genügend klar. Angaben zum Sexualleben oder zur sexuellen Orientierung sind darin zweifellos mitenthalten. Deshalb sehen wir keinen Grund, den Katalog der besonders schützenswerten Personendaten weiter zu ergänzen. Auch der KdK-Leitfaden sowie die Änderungserlasse der anderen Kantone gehen nicht von der Notwendigkeit einer solchen Ergänzung aus. Die Aufnahme der genetischen und der biometrischen Daten in die Kategorie der besonders schützenswerten Personendaten zeigt, dass eine nicht abschliessende Liste inskünftig Vorteile bei der Anwendung des Datenschutzgesetzes mit sich bringen könnte und die Anwendung des Gesetzes flexibler macht. Zu den Anforderungen an die gesetzlichen Grundlagen des Bearbeitens von Personendaten verweisen wir auf unsere Ausführungen in Kapitel 5.4 und die Kommentierung von § 5 in Kapitel 6.1.

4.2.5.2 Register der Datensammlungen

In der Vernehmlassung hat die Aufhebung des [Registers der Datensammlungen](#) unterschiedliche Einschätzungen erfahren. Die FDP erachtet den Verzicht als unproblematisch, wenn die Polizei der Registerpflicht unterstellt bleibt. Grüne und SP ver-

mochte die knappe Begründung in der Vernehmlassungsbotschaft nicht zu überzeugen. Eine Anzahl Gemeinden hat den Verzicht auf das Register begrüsst. Die übrigen Vernehmlassungsteilnehmer haben sich nicht ausdrücklich dazu geäußert.

Die Datenschutzrichtlinie verlangt in ihrem Anwendungsbereich, somit für die Strafgerichts-, Strafverfolgungs- und Strafvollzugsbehörden, dass ein Verzeichnis der Datenbearbeitungen geführt wird, und knüpft damit praxisbezogen an die Tätigkeit der entsprechenden Behörden an. Es ist vorgesehen, diese Anforderung an die kantonale Datenschutzgesetzgebung mit einer offenen Grundsatznorm aufzunehmen, ohne – wie im Vernehmlassungsentwurf vorgesehen – die bisherige Norm auch in formeller Hinsicht gänzlich zu streichen (vgl. § 14 KDSG-Entwurf). In der Sache wollen wir aber auf das allgemeine Register der Datensammlungen verzichten. Aufgrund der seit der Entstehungszeit des kantonalen Datenschutzgesetzes auf breiter Front aufkommenden elektronischen Datenverarbeitung in den Verwaltungen von Kanton und Gemeinden müssen interessierte Personen davon ausgehen, dass die Verwaltungsorgane im Rahmen ihrer Aufgabenerfüllung Personendaten erfassen und bearbeiten. Bei den einzelnen Verwaltungsorganen kann jederzeit nachgefragt werden, ob und wenn ja welche Personendaten gespeichert sind. Die Bewirtschaftung des Registers ist aufwendig. Deswegen konnte das Register die Erwartungen an ein aktuelles Inhaltsverzeichnis der Datensammlungen aller der Meldepflicht unterstellten Gemeinwesen nicht mehr vollständig erfüllen. Auch sind gewisse Eintragungen von beschränktem Informationsnutzen (z.B. wenn bei der Kategorie Personalakten einer Dienststelle die Selbstverständlichkeit ausgewiesen wird, dass Geburtsdaten, Geschlecht oder Arbeitsort erfasst werden). Nicht zuletzt mit der vorliegenden Gesetzesrevision werden der Geltungsbereich des Gesetzes sowie die Auskunfts- und Informationsrechte ausgebaut. In den genannten Bereichen mit erhöhten Anforderungen an den Grundrechtsschutz, namentlich im Polizeibereich, sind im Rahmen der Einführungsphase verbesserte Register in Form von Verzeichnissen der Datenbearbeitungstätigkeiten zu erstellen. Die Verzeichnisse können von den betroffenen Behörden im Sinn einer Selbstregulierung direkt verwaltet werden und bedürfen keiner besonderen Datenbank.

4.3 Wichtige Unterschiede Vernehmlassungsbotschaft - vorliegende Botschaft

Nebst Ergänzungen und redaktionellen Bereinigungen unterscheidet sich unser Gesetzesentwurf inhaltlich in folgenden Punkten vom Vernehmlassungsentwurf:

Thema	Vernehmlassungsentwurf	Gesetzesentwurf
Geltung des Gesetzes: Anpassung an § 2 Abs. 8, Verhältnis zur Aufsicht	§ 3 Abs. 2b	§ 3 Abs. 1d und Abs. 4
Bearbeiten von Personendaten: Klarstellung bei Umschreibung der Voraussetzungen	§ 5	§ 5
Verantwortlichkeit der Organe für Datenschutz und Datensicherheit: Zusammenführung zweier Bestimmungen	§ 6 Abs. 1 ^{bis} § 7 Abs. 1	§ 6 Abs. 1 ^{bis}

Verzeichnis der Datenbearbeitungstätigkeiten: Einführung durch Verordnung oder auch durch Gemeinden	§ 7b Abs. 1	§ 14
Datenschutzberater/in: Einführung durch Verordnung und auch in Gemeinden	§ 7b Abs. 2 und 4	§ 7b Abs. 1 und 3
Beauftragte/r für den Datenschutz: personalrechtliche Regelungen	–	§ 22 Abs. 1 ^{bis} und 1 ^{ter}
Finanzierung: keine Kostenbeteiligung der Gemeinden	§§ 22 Abs. 3 und 22a	–

Ausserdem enthält die Botschaft die Anpassungen und die begrifflichen Nachführungen in den Spezialerlassen, die im Vernehmlassungsentwurf noch nicht im Einzelnen ausgewiesen waren.

5 Grundzüge der Vorlage

5.1 Allgemeines

Bei den vorliegenden Änderungen geht es im Wesentlichen darum, das kantonale Datenschutzrecht an die Entwicklungen, wie sie in Kapitel 1 erläutert sind, anzupassen. Insbesondere die EU-Datenschutzrichtlinie ist darauf ausgerichtet, dass die Staaten, die dem Schengen-Assoziierungsübereinkommen angeschlossen sind, ihre Datenschutzerlasse vereinheitlichen. Die Richtlinie stellt in ihrem Regelungsbereich – dem Schutz natürlicher Personen bei der Bearbeitung von Personendaten durch die Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten sowie der Strafvollstreckung – eine umfassende und relativ detaillierte Ordnung des Datenschutzes auf. Es soll ein hohes Schutzniveau gewährleistet werden. Aufgrund der Regelungsdichte der Datenschutzrichtlinie muss das luzernische Datenschutzgesetz in all seinen Bestimmungen überprüft werden. Dabei ist abzuwägen, ob die Vorgaben der Richtlinie für das ganze Datenschutzrecht oder nur im engeren Anwendungsbereich der öffentlichen Sicherheit im Sinn des Schengen-Rechts angewendet werden sollen. Als Beispiel für den Verzicht auf die Ausdehnung einer Schengen-Bestimmung auf das allgemeine Datenschutzrecht kann die neu einzuführende amtsinterne Datenschutzberatung erwähnt werden: Wir sehen ausdrücklich davon ab, diese Funktion für die gesamte Verwaltung obligatorisch zu erklären. Entsprechend sollen in der Verordnung nur die Strafverfolgungsbehörden (inkl. Luzerner Polizei) und die Strafvollzugsbehörden verpflichtet werden, eine Datenschutzberaterin oder einen Datenschutzberater zu bezeichnen. Bei der Beurteilung solcher Anwendungsfragen müssen allerdings in einer Gesamtschau auch das neue Europaratsübereinkommen und die EU-Datenschutz-Grundverordnung beachtet werden.

In diesem Vieleck der Anforderungen umfasst die Anpassung des kantonalen Datenschutzrechtes zunächst einmal verschiedene terminologische Modernisierungen und Vereinheitlichungen. So sind Definitionen zu erweitern oder zu präzisieren (z.B. Nennung der genetischen Daten bei der Umschreibung der Personendaten), und auf gewisse Begriffe (z.B. Datensammlung) ist zu verzichten. Beim Geltungsbereich müssen Ausnahmen von der Anwendung des Gesetzes wegfallen. Mit allen diesen Anpassungen sollen Abweichungen oder Unklarheiten vermieden und insgesamt eine Vereinfachung des Datenschutzrechtes erreicht werden (vgl. im Einzelnen die

Kommentierung in Kap. 6.1). Zur Klarstellung dient auch die vorgeschlagene Änderung des Erlasstitels: In Abgrenzung zum Bundesgesetz über den Datenschutz beziehungsweise zum eidgenössischen Datenschutzgesetz (DSG) schlagen wir den Kurztitel Kantonales Datenschutzgesetz und die Abkürzung KD SG vor.

Neben eher formellen und technischen Anpassungen enthält der Änderungsentwurf aber durchaus auch Verstärkungen beim präventiven Datenschutz, dies wiederum ausschliesslich aufgrund des übergeordneten Rechts. Zu erwähnen sind insbesondere die formalisierte Datenschutz-Folgenabschätzung und die Vorabkonsultation in § 7a unseres Entwurfs. Bei der Aktualisierung des Luzerner Datenschutzgesetzes will unser Rat aber mit Augenmass vorgehen und die Grundsätze der luzernischen Gesetzestchnik, die auf eine verständliche und möglichst knappe Normierung zielen und Einzelheiten des Vollzugs im Verordnungsrecht regeln oder der Praxis überlassen, nicht aufgeben. Das geltende kantonale Gesetz hat sich nämlich im Grossen und Ganzen bewährt. Die im Gesetz genannten Grundsätze der Datenbearbeitung – insbesondere Recht- und Verhältnismässigkeit, Integrität (Richtigkeit), Zweckbindung (§ 4) – und die Kontrollrechte der betroffenen Person hinsichtlich der Daten, die in der Verwaltung über sie bearbeitet werden (§§ 15 ff.), sowie die Organisation des Aufsichtsorgans selbst (§§ 22 ff.) bleiben in den wesentlichen Zügen unverändert.

Bei der Kommentierung der Bestimmungen in Kapitel 6 wird, soweit erforderlich, auf die Anforderungen der übergeordneten Erlasse an das kantonale Recht im Einzelnen eingegangen, oder es werden mindestens Hinweise auf die entsprechenden Normen gegeben.

5.2 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 öffentliche Organe, unabhängig von den angewandten Mitteln, Verfahren und Organisationsformen, Anwendung finden. Die §§ 1–3 KD SG waren deshalb in dieser Hinsicht zu überprüfen und Ausnahmen nur unter engen Voraussetzungen vorzusehen (vgl. die Kommentierung in Kap. 6). Gemäss unserem Entwurf soll das KD SG in den Gemeinwesen und deren Behörden und Verwaltungseinheiten allgemein anwendbar sein. Die hierfür 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. Beispielsweise sind in Verfahren der Einbürgerung in Kanton und Gemeinden die besonderen Bestimmungen der Bürgerrechtsgesetzgebung anwendbar (vgl. §§ 33 und 34 Kantonales Bürgerrechtsgesetz vom 15. Mai 2017; SRL Nr. 2). Beim Grundbuch gehen die im eidgenössischen Grundbuchrecht geregelten Auskunftsrechte dem kantonalen Recht vor. Beispielsweise wäre eine auf kantonales Datenschutzrecht gestützte Datensperre gar nicht möglich (vgl. Art. 26 ff. Grundbuchverordnung; SR 211.432.1). Für die kantonalen Anstalten hat unser Rat die Geltung des kantonalen Datenschutzgesetzes bereits durch Verordnung ausgeweitet (vgl. § 3 Verordnung zum Datenschutzgesetz; SRL Nr. 38b).

Die Regeln der Datenbearbeitung widerspiegeln letztlich die Anforderungen an staatliches Handeln auf der Grundlage von Treu und Glauben und der Grundsätze

des öffentlichen Interesses, der Recht- und der Verhältnismässigkeit (vgl. § 2 Kantonsverfassung). Unter diesem Aspekt erscheint die möglichst breite Anwendung des Datenschutzrechtes zweckmässig.

5.3 Beschränkung auf natürliche Personen und Aktualisierung des Katalogs der besonders schützenswerten Personendaten

Aus der Definition der Personendaten im geltenden Datenschutzgesetz ergibt sich, dass dieses Gesetz nicht nur den Schutz von natürlichen Personen vor unbefugtem Bearbeiten ihrer Daten durch öffentliche Organe, sondern auch den Schutz von juristischen Personen und Personengesellschaften des Handelsrechts bezweckt (vgl. § 2 Abs. 1). Dagegen sehen das Europaratsübereinkommen, die für die Schengen-Staaten geltende Datenschutzrichtlinie, die Datenschutzgesetzgebung der meisten europäischen Staaten und das totalrevidierte eidgenössische Datenschutzgesetz die Anwendung der Datenschutzbestimmungen auf die 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. Die Kantone sind zwar nicht verpflichtet, die bundesrechtliche Anpassung an das internationale Recht zu vollziehen, doch hat sich aus der Praxis des Beauftragten für den Datenschutz kein Bedürfnis für ein spezifisches Datenschutzrecht der juristischen Personen ergeben. Diese sind durch andere, gesamtschweizerische Regelwerke umfassend geschützt: Bei Persönlichkeitsverletzungen, soweit sie keine physische Existenz voraussetzen, kommen die Bestimmungen des Schweizerischen Zivilgesetzbuches (SR 210) zum Tragen. Bei Vertragsverletzungen (z.B. Vertraulichkeitsabreden) ist das Obligationenrecht (SR 220) massgebend, vor Verletzungen von Berufs-, Geschäfts- und Fabrikationsgeheimnissen und bei zahlreichen weiteren Tatbeständen, die für die Wirtschaftsunternehmen von Bedeutung sind, schützt das Schweizerische Strafgesetzbuch (SR 311) vor Datenmissbrauch. Im Wirtschaftsverkehr gelten ausserdem die Bestimmungen des Urheber- und des Wettbewerbsrechts, im Rechtsverkehr die Regeln des Prozess- und Verfahrensrechts. Des Weiteren sind die Verwaltungsbehörden zur Wahrung des allgemeinen Amtsgeheimnisses wie auch zur Wahrung spezifischer Geheimhaltungspflichten verpflichtet, namentlich bei den Steuerdaten (vgl. § 134 Steuergesetz, SRL Nr. 620). Es wird daher auch für das kantonale Datenschutzgesetz vorgeschlagen, auf die Unterstellung der Daten juristischer Personen unter das Gesetz zu verzichten und den Erlass auf den Schutz der Daten von natürlichen Personen zu beschränken. Dadurch soll eine Einheitlichkeit mit der bundesrechtlichen Regelung geschaffen werden. Weitere Ausführungen dazu können den Erläuterungen zum DSG-Entwurf in der Botschaft des Bundesrates entnommen werden (dort in Kap. 9.1.2 zu Art. 2 Abs. 2; in rechtlicher Hinsicht vgl. auch Drechsler, Plädoyer für die Abschaffung des Datenschutzes für juristische Personen, in: AJP 2016 S. 80). Der Bund sieht für die Daten von juristischen Personen überhaupt keine Anwendung des eidgenössischen Datenschutzgesetzes mehr vor, beabsichtigt jedoch im Regierungs- und Verwaltungsorganisationsgesetz eine separate rechtliche Grundlage für die Bearbeitung von Daten von juristischen Personen durch die Verwaltung zu schaffen. Entsprechend sieht auch unser Entwurf eine Ergänzung des Organisationsgesetzes vom 13. März 1995 (SRL Nr. 20) vor (vgl. Kap. 6.2). Zugleich werden Bestimmungen in den Spezialerlassen angepasst, damit in diesen Bereichen die gesetzliche Grundlage zur Datenbearbeitung erhalten bleibt (z.B. im Statistikrecht).

Wie in Kapitel 4.2.5.1 erläutert, wird der Katalog der besonders schützenswerten Personendaten aktualisiert und flexibilisiert. Die Angaben, welche zu dieser Kategorie von Personendaten gehören, haben sich schon bisher zur Hauptsache auf die natürlichen Personen bezogen.

5.4 Gesetzliche Grundlage für die Datenbearbeitung

In der Formulierung des geltenden Rechts dürfen Personendaten zur Erfüllung von *Aufgaben* bearbeitet werden, *für die* eine Rechtsgrundlage besteht (§ 5 Abs. 1 KDSG). Er steht dem Gesetzgeber aber frei, nicht nur die Verwaltungsaufgabe, sondern bereits die Datenbearbeitung an sich unmittelbar in einem Gesetz zu regeln. Da dies in den letzten Jahren in verschiedenen Spezialgesetzen so gehandhabt wurde, soll das Datenschutzgesetz entsprechend nachgeführt werden. Die Möglichkeit zur Bearbeitung von Personendaten gestützt auf eine mittelbare Rechtsgrundlage, die ohne Nennung der Datenbearbeitung lediglich die Aufgabe klar umschreibt, bleibt damit weiter bestehen. Zur Bearbeitung von besonders schützenswerten Daten ist ein Gesetz im formellen Sinn nötig. Auch die völker- und europarechtlichen Grundlagen für den Datenschutz setzen «geeignete Sicherheiten» beziehungsweise «geeignete Garantien im Gesetz» für die Bearbeitung von besonders schützenswerten Personendaten voraus.

5.5 Informationsrechte und Auskunftspflichten

Überarbeitet werden die Bestimmungen über die Informationspflichten beim Erheben von Personendaten und über die Auskunftsrechte hauptsächlich in den §§ 8 und 15 KDSG. Dabei wird die Informationspflicht nicht grundlegend geändert, deren Anwendung jedoch verbessert, indem klarer aufgeführt wird, über was das erhebende Organ die betroffenen Personen von sich aus 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 soll weiterhin grundsätzlich kostenlos ausgeübt werden können.

In Ergänzung zu diesen grundsätzlich schon bestehenden Rechten und Pflichten ist eine Melde- und Informationspflicht bei unbefugten Datenbearbeitungen festzulegen (vgl. § 7 KDSG-Entwurf): Sind beispielsweise Personendaten ungesichert verloren gegangen und kann aus den Umständen dieses Vorgangs eine erhebliche Gefährdung der Persönlichkeits- und Grundrechte eintreten, sind die betroffenen Personen zu informieren. Solche Verletzungen der Datensicherheit können fahrlässig oder missbräuchlich von Verwaltungsmitarbeiterinnen und -mitarbeitern, aber auch von Dritten, verursacht werden. Die Informationspflicht ist dabei nicht um ihrer selbst willen zu erfüllen. Im Sinn der Risikoorientierung werden in der Praxis Kriterien aufzustellen sein, bei deren Erfüllung eine Information sinnvoll ist. Eine Informationspflicht ist insbesondere dann anzunehmen, wenn die betroffenen Personen zur Abwehr des Schadens selber Massnahmen ergreifen können (z.B. die Zugangsdaten ändern).

5.6 Datenschutz-Folgenabschätzung

Die neuen europäischen Rechtsgrundlagen verlangen bei geplanten Datenbearbeitungen eine vorgängige Datenschutz-Folgenabschätzung. Dieses Instrument ist auch im totalrevidierten Datenschutzgesetz des Bundes vorgesehen. Es dient dazu, den Datenschutz bereits in der Planungsphase eines Vorhabens besser zu verankern. Künftig soll bei heiklen Vorhaben eine etwas formale Beurteilung des Daten-

schutzes als bisher durchgeführt und dokumentiert werden. Dabei soll ein risikobasierter Ansatz gelten: Eine Datenschutz-Folgenabschätzung ist nötig, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeits- oder die Grundrechte der betroffenen Personen führt. In der Sache selbst geht es um nichts Neues. Bei kantonalen Gesetzes- und Informatikprojekten werden solche Abschätzungen schon heute vorgenommen. Mit der Abschätzung ist eine Prognose darüber zu machen, welche Folgen eine geplante Datenbearbeitung für die betroffenen Personen oder Personengruppen hat. 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 Vorkehrungen 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. Die Prüfung möglicher Auswirkungen einer geplanten Datenbearbeitung ist ein Beitrag zur Qualitätssicherung bei den organisatorischen und technischen Prozessen innerhalb der Verwaltung. Die Datenschutz-Folgenabschätzung kann ausserdem die Grundlage für eine effiziente Durchführung der Vorabkontrolle sein, zu welcher der oder die Beauftragte für den Datenschutz schon nach heutigem § 23 Absatz 1h ermächtigt ist.

5.7 Aufsichtsstelle

Mit einlässlichen Vorgaben wird in den neuen völker- und europarechtlichen Regelwerken die Unabhängigkeit der Aufsichtsbehörden, die für die Einhaltung der Datenschutzvorschriften und die Überwachung zuständig sind, europaweit vereinheitlicht und gestärkt. Dabei muss der kantonalen Aufsichtsstelle die Befugnis zukommen, selber Entscheide zu fällen. Weitere Bestimmungen betreffen die institutionelle Ausgestaltung als unabhängige Fachstelle. Die Möglichkeit zur Schaffung von kommunalen oder regionalen Aufsichtsstellen (im geltenden Gesetz § 22 Abs. 3, im Vernehmlassungsentwurf § 22a) wird im Zuge der Massnahmen zur Stärkung der Aufsichtsstelle wie auch zur Vermeidung allfälliger Doppelspurigkeiten gestrichen. Im Kanton Luzern soll die Aufsichtsstelle weiterhin mit der geläufigen Bezeichnung «Beauftragter oder Beauftragte für den Datenschutz» bezeichnet werden, auch wenn die EU-Datenschutzrichtlinie den Begriff des Datenschutzbeauftragten für den organisationsinternen Datenschutzberater verwendet. Zur Funktion des Datenschutzberaters oder der Datenschutzberaterin verweisen wir auf die Kommentierung des § 7b KDSG-Entwurf im nachstehenden Kapitel. Zur Stellung des oder der kantonalen Beauftragten für den Datenschutz verweisen wir auf unsere Ausführungen in Kapitel 4.2.2 und 4.2.4 sowie auf die Erläuterungen zu den §§ 22–22b im nachstehenden Kapitel.

6 Die Gesetzesentwürfe im Einzelnen

6.1 Datenschutzgesetz

Erlassstitel und -abkürzung

Das luzernische Gesetz über den Schutz von Personendaten trägt seit dessen Erlass am 2. Juli 1990 den Kurztitel «Datenschutzgesetz» und die Abkürzung «DSG». Die gleiche Abkürzung bezeichnet seit dem 19. Juni 1992 das Bundesgesetz über den Datenschutz. Das am 25. September 2020 totalrevidierte Bundesgesetz über den Datenschutz führt ebenfalls den Kurztitel «Datenschutzgesetz» und die Abkür-

zung «DSG» im Erlassstitel. In Abgrenzung zum eidgenössischen Datenschutzgesetz soll das luzernische Gesetz über den Schutz von Personendaten den Kurztitel «Kantonales Datenschutzgesetz» und die Abkürzung «KDSG» erhalten. Diese Abkürzung wird in dieser Botschaft bereits für den geltenden Erlass verwendet.

§ 2

Internationales Recht: Art. 2 Europaratsübereinkommen,
Art. 3 DSRL

In dieser Bestimmung werden Begriffe des Datenschutzes definiert. Verschiedene davon sind an das übergeordnete Recht anzupassen, damit Unklarheiten ausgeräumt und Widersprüche aufgehoben werden, die sich aus der Gegenüberstellung der verschiedenen Regelwerke ergeben. Dabei verzichten wir allerdings wie der Bund und voraussichtlich sämtliche Kantone zum einen auf den Ersatz der allgemein eingeführten und bewährten Begriffe «Personendaten» und «Bearbeiten von Personendaten», wofür im internationalen Kontext die Begriffe «personenbezogene Daten» und «Verarbeiten von Daten» gebraucht werden, und zum andern auf den weiteren Ausbau der Legaldefinitionen, wo es nicht erforderlich ist. Insbesondere werden Datenverantwortlichkeit und Datensicherheit in den materiellen Schutznormen des Gesetzes umschrieben (vgl. §§ 6 Abs. 1 und 7 Abs. 1).

Absatz 1: Aus der Definition der Personendaten im geltenden Gesetz ergibt sich, dass dieser Begriff nicht nur die natürlichen Personen, sondern auch die juristischen Personen und Personengesellschaften des Handelsrechts umfasst. Wie in Kapitel 5.3 erläutert, sollen die Personendaten inskünftig nur noch als Angaben über bestimmte oder bestimmbare *natürliche* Personen verstanden werden. Eine redaktionelle Folgeanpassung ist in Absatz 3 vorzunehmen. Dagegen bleibt die Zweckumschreibung in § 1 unverändert. Die Beschränkung auf die natürlichen Personen im KDSG schliesst die Beibehaltung der bisherigen Begriffsbestimmung in anderen Erlassen nicht aus (vgl. unsere Ausführungen zum Informatik- und zum Statistikgesetz, Kap. 6.2.4 und 6.2.5). Es soll nämlich die bisherige Bearbeitung von Daten juristischer Personen und von Personengesellschaften des Handelsrechts durch die Verwaltung sichergestellt sein (vgl. dazu die Anpassungen im Organisations-, Statistik- und Archivgesetz). Wie bisher sind Personendaten Angaben, mit denen eine Person direkt oder – beispielsweise durch die AHV-Nummer – indirekt identifiziert werden kann. Es kann insbesondere auf den bundesrechtlichen Datenbegriff verwiesen werden.

Absatz 2: In diesem Absatz werden neu die genetischen Daten unter der Kategorie der besonders schützenswerten Personendaten aufgeführt, dies mit dem Begriff der Daten «über das Erbgut». 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](#)). Wie bei anonymisierten Daten findet das Datenschutzgesetz keine Anwendung, wenn eine Re-Identifikation nicht möglich ist.

Im Sinn der Aktualisierung des Datenschutzrechtes ist zudem vorgesehen, die mit dem Begriff «biometrische Daten» umschriebenen Personendaten 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 (insbes. durch Gesichtserkennungsprogramme gewonnene Daten zu einem Gesicht, daktyloskopische Daten der Polizei, Stimmuster, Irismuster der Augen einer Person). Dabei gilt es festzuhalten, dass keineswegs jede Fotografie unter die Definition im Sinn des Gesetzes fällt. Dies wird mit der differenzierten Umschreibung der biometrischen Daten klar signalisiert.

Die genetischen wie die biometrischen Daten wurden auch in die Liste der besonders schützenswerten Daten des neuen eidgenössischen Datenschutzgesetzes aufgenommen. Die Begriffe sollen gleich ausgelegt werden wie im Bundesrecht. Weitergehende Änderungen drängen sich nicht auf (vgl. zu vereinzelt Eingaben im Vernehmlassungsverfahren Kap. 4.2.5.1).

Die Kategorie der besonders schützenswerten Personendaten ist für die Beurteilung der Zulässigkeit der Datenbearbeitung durch die öffentlichen Organe von Bedeutung (vgl. § 5 Abs. 2). Im Unterschied zum geltenden Recht soll diese Kategorie im Gesetz nicht mehr in abschliessender Form umschrieben werden. Damit werden die Konzepte neuerer kantonaler Datenschutzerlasse (u.a. AG, BS und ZH) übernommen, womit die Anwendung des Gesetzes flexibler wird. Wir verweisen auf unsere Ausführungen in Kapitel 4.2.5.1. 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 anstelle der administrativen Massnahmen und Sanktionen. In der Sache ändert sich nichts, geht es doch wie bisher nur um den engeren Verwaltungsvollzug mittels Massnahmen und Sanktionen. Auf Anregung des Beauftragten für den Datenschutz wird trotz der Generalklausel und der nicht abschliessenden Aufzählung die bisherige Unterkategorie «Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der natürlichen Person erlaubt (Persönlichkeitsprofil)» weiterhin erwähnt. Der Begriff des Persönlichkeitsprofils hat in der Praxis eine gewisse Bedeutung erhalten; auch kann das Persönlichkeitsprofil vom Profiling (Abs. 4^{bis}) genügend klar abgegrenzt werden. Damit sind besonders schützenswerte Personendaten gemeint, bei den aufgrund der Bedeutung oder der Art ihrer Bearbeitung oder der Möglichkeit der Verknüpfung mit anderen Daten die besondere Gefahr einer Persönlichkeits- und Grundrechtsverletzung besteht.

Absatz 4: Als Bearbeitungsformen sollen aufgrund der Rückmeldungen aus der Vernehmlassung zusätzlich das Aufbewahren, das Löschen und das Speichern aufgeführt (Satz 1) aufgeführt werden. Diese Bearbeitungen sind von hoher Praxisrelevanz für die Gewährleistung eines ausreichenden Datenschutzes und finden sich auch im DSG des Bundes. Ausserdem soll in dieser Bestimmung der Begriff des Bekanntgebens von Personendaten konkretisiert werden als Übermitteln (z.B. durch telefonische oder EDV-Mittel) und als Zugänglichmachen, wobei in Satz 2 das Einsichtgewähren, Weitergeben und Veröffentlichen als Arten des Zugänglichmachens genannt werden. Die Aufzählung der Bearbeitungsformen ist indes nicht abschliessend und der Begriff des Bearbeitens von Personendaten muss umfassend verstanden werden. Er entspricht wie erwähnt dem im internationalen Kontext bevorzugten Begriff der Verarbeitung personenbezogener Daten.

Absatz 4^{bis}: In diesem neuen Absatz wird der Begriff des Profilings (als besondere Art des Bearbeitens von Personendaten) definiert. Profiling ist jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte zu bewerten, was dazu dienen soll, 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 das neue DSGVO. Im internationalen Datenschutzrecht wird der Begriff des Profilings lediglich in der Datenschutzrichtlinie verwendet, dies aufgrund des Sachzusammenhangs zur Strafverfolgung, der im öffentlichen Bereich im Vordergrund steht. Das Profiling stellt einen besonderen Datenbearbeitungsvorgang dar: Aus dem «Datenbild» einer Person wird eine Schlussfolgerung mit Bezug auf persönliche Aspekte einer Person gezogen. Der Begriff des Persönlichkeitsprofils (Abs. 2e) knüpft dagegen an die Art der Daten an. Soweit die aufgrund eines Profilings entstandenen Daten Personendaten oder besonders schützenswerte Personendaten sind, gelangt das Datenschutzgesetz zur Anwendung; dient es zur Erzeugung von anonymisierten Daten, sind die Resultate des Profilings 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 wird zunehmend darauf abgestellt, ob Personendaten bearbeitet werden. Zudem kann bei der Methode des Profilings auf Quellen zurückgegriffen werden, die keine Datensammlungen darstellen. Bereits in unserer Botschaft B 82-1989 haben wir Zweifel an der Tauglichkeit des Begriffs der Datensammlung angebracht (vgl. Verhandlungen des Grossen Rates [GR] 1989, S. 713 f.). Der Begriff soll nun gestrichen werden. Konsequenterweise ist auch vom Begriff des Inhabers einer Datensammlung abzusehen (vgl. Abs. 7), zumal bei zentralen Datenbanken im Sinn des § 5 des Informatikgesetzes (SRL Nr. 26), bei denen mehrere Organe Personendaten in eine einzige Datensammlung einbringen und gemeinsam bearbeiten, Schwierigkeiten bei der Definition der Inhaberefunktion bestehen. Mit dieser Begriffsbereinigung folgt unser Entwurf dem DSGVO.

Absatz 7: In diesem Absatz wird der Begriff des für die Datenbearbeitung verantwortlichen Organs eingeführt. Damit kann die gleiche Terminologie wie im neuen DSGVO und wie in den internationalen Rechtsgrundlagen Verwendung finden. Im Übrigen fand der Begriff des verantwortlichen Organs schon im geltenden Erlass Verwendung (vgl. §§ 6 Abs. 1 und 3, 18 Abs. 2a und 2c, 23 Abs. 1b, 24 Abs. 1 und 3). Verantwortlich ist das Organ, das allein oder zusammen mit anderen Organen über den Zweck oder die Mittel der Datenbearbeitung (z.B. über die verwendete Software) entscheidet. Demgegenüber gilt als Auftragsdatenbearbeiter die private Person oder das andere Organ, das im Auftrag des datenverantwortlichen Organs Personendaten bearbeitet (vgl. § 6 Abs. 2).

Aus der Ersetzung der Begriffe «Datensammlung» und «Inhaber der Datensammlung» in den Absätzen 6 und 7 ergeben sich redaktionelle Folgeanpassungen in weiteren Paragraphen, in denen die Begriffe verwendet werden, und es sind weitere Erlasse formell anzupassen. Insgesamt erhöht sich dadurch aber die Verständlichkeit und Durchgängigkeit des Datenschutzrechtes.

Ausschlüsse von der Geltung des Datenschutzgesetzes sind auch aufgrund der Vorgaben des übergeordneten Rechts problematisch. In § 3 werden daher Ausnahmen ganz oder teilweise reduziert oder anders umschrieben, um den Anforderungen zu genügen

Absatz 1: Im Sinn der Einheit des kantonalen öffentlichen Rechts soll das KDSG für die Gemeinwesen und sämtliche Personen und Organisationen, die öffentliche Aufgaben erfüllen, angewendet werden. Schon bisher hat der Regierungsrat die kantonalen Anstalten durch Verordnung dem Datenschutzgesetz unterstellt, dies gestützt auf die Kompetenzdelegation des Absatzes 1c (vgl. § 3 Verordnung zum Datenschutzgesetz, SRL Nr. 38b).

Absatz 2: Statt des bestehenden weiten Ausschlusses wird hier ein enger Ausschluss vorgeschlagen. Notizen und Agenden, die den Mitarbeiterinnen und Mitarbeitern der Verwaltung in handschriftlicher oder schriftlicher Form oder heutzutage auch in einem elektronischen Format als Hilfsmittel bei der Aufgabenerfüllung dienen, sollen von den Kontrollrechten des Teils 3 des Gesetzes, namentlich dem Auskunftrecht, ausgenommen bleiben. Notizen dienen insbesondere als Gedankenstützen in der Sachbearbeitung in der Verwaltung und sind nicht Teil der amtlichen Akten. Das Führen von sogenannten Schattendossiers ist hingegen schon aus rechtsstaatlichen Gründen nicht erlaubt. Agenden dienen der Arbeitsorganisation.

Absatz 3: Dieser Absatz schliesst an den bisherigen Absatz 2a an, der aufgehoben wird. Geregelt wird das Verhältnis der Prozess- und Verfahrensordnungen zum Datenschutzrecht. Das Datenschutzgesetz wird auf sämtliche Verfahren vor kantonalen Gerichten nicht angewendet, insbesondere die verwaltungsgerichtlichen Verfahren. Eingeschlossen in dieser Ausnahme sind die Verfahren nach den kantonalen Verfahrensordnungen, sowohl die allgemeine Verfahrensordnung gemäss Gesetz über die Verwaltungsrechtspflege (SRL Nr. 40) wie auch besondere Verfahrensordnungen und -regelungen, wie sie sich aus dem Justizgesetz (SRL Nr. 260) oder auch etwa dem kantonalen Enteignungsgesetz (SRL Nr. 730) ergeben können. 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 Verfahrensakten erscheinen. Selbstverständlich können solche Erlasse auch auf die Regelungen im Datenschutzrecht verweisen. Aus Absatz 3 ergibt sich im Umkehrschluss, dass das Datenschutzgesetz auf Datenbearbeitungen angewendet wird, welche von den Gerichtsbehörden in administrativer Hinsicht vorgenommen werden, beispielsweise von einer Gerichtskanzlei über Daten des eigenen Personals.

Absatz 4: Dieser Absatz nimmt parlamentarische und Rechtsprechungstätigkeiten von Überwachungsmaßnahmen im Sinn des § 23 Absatz 1a aus. Dieser Ausschluss sichert insbesondere die parlamentarische Oberaufsicht des Kantonsrates (§ 50 KV) wie auch die Tätigkeit der unabhängigen Justizbehörden. Im Übrigen kommen bei Parlamentsgeschäften die Verfahrensbestimmungen des Kantonsratsgesetzes (SRL Nr. 30) zum Zuge, in justiziellen Verfahren die besonderen Prozessregelungen, die als besondere Verfahrensordnungen gelten (vgl. Abs. 6).

Absatz 5: Öffentliche Organe können am wirtschaftlichen Wettbewerb teilnehmen und dabei privatrechtlich handeln (vgl. §§ 33a und 45 Organisationsgesetz, SRL Nr. 20). Im Sinn der Gleichbehandlung sollen bei solchen Leistungen die Bestimmungen des eidgenössischen Datenschutzrechtes zur Anwendung gelangen, welche für die Privaten gelten. Auch wenn die dem Gesetz unterstellten Organe wie Private handeln, bleiben sie als öffentliche Organe der Aufsicht des oder der kantonalen Beauftragten für den Datenschutz unterstellt.

Absatz 6: Das Datenschutzgesetz gilt als Querschnittsgesetz und regelt den Datenschutz im Allgemeinen. Im Anwendungsbereich kantonaler Spezialgesetze können besondere Normen über den Umgang mit Daten oder auch amtlichen Dokumenten (z.B. Protokollen) sowie Verfahrensrechte (insbes. Akteneinsichtsrechten) bestehen, die vorgehen. In diesem Absatz wird dies klargestellt. Soweit kantonale Behörden bei der Datenbearbeitung Bundesgesetze anwenden, gelten ohnehin die Sachnormen des bereichsspezifischen Bundesrechts (z.B. bei der Erfassung von und der Einsichtnahme in Daten des Grundbuchs, bei der Datenbearbeitung durch die Ausländerbehörde des Kantons, bei Datenüberprüfungen im elektronischen Zivilstandsregister, beim Informationsaustausch in Strafverfahren).

Zwischentitel vor § 5

Mit dem neuen Zwischentitel wird die Übersichtlichkeit verbessert.

§ 5

Internationales Recht: Art. 5 und 6 Europaratsübereinkommen,
Art. 8 und 10 DSRL

Das Datenschutzrecht unterscheidet mit Blick auf die Anforderungen an die Rechtsgrundlage für die Datenbearbeitung zwischen besonders schützenswerten Personendaten (Abs. 2) und anderen Personendaten (Abs. 1). Zur Umschreibung dieser Kategorien vergleiche die Kommentierung von § 2 Absätze 1 und 2. Allgemein bedarf es zur Bearbeitung von Personendaten einer generell-abstrakten Norm. Der Rechtssatz muss dabei genügend bestimmt sein, denn das staatliche Handeln soll im Einzelfall voraussehbar sein (zu den Erfordernissen des Rechtssatzes vgl. Häfelin/Müller/Uhlmann, Allgemeines Verwaltungsrecht, 8. Auflage 2016, N 338 ff.). Bereits nach geltendem luzernischem Recht dürfen öffentliche Organe gewöhnliche Personendaten, das heisst nicht besonders schützenswerte Daten im Sinn des § 2 Absatz 2, im Rahmen ihrer Aufgabenerfüllung bearbeiten, wenn *für die Aufgabe* eine Rechtsgrundlage besteht. Der Gesetzgeber erachtet somit eine mittelbare gesetzliche Grundlage für diese Datenbearbeitung als ausreichend. Es genügt jede im Rahmen der Rechtsordnung erlassene generell-abstrakte Norm, insbesondere auch eine solche im Verordnungsrecht. Gemäss den Ausführungen in unserer Botschaft B 82-1989 muss das Bearbeiten von Personendaten in der Rechtsgrundlage nicht einmal zum Ausdruck kommen. Die Rechtsgrundlage statuiere lediglich die zu erfüllende Aufgabe. Ob zur Erfüllung dieser Aufgabe Personendaten zu bearbeiten sind, beurteile sich nach den Grundsätzen des § 4 KDSG (vgl. GR 1989 S. 718). Im neu gefassten Absatz 2 wird zunächst das Bearbeiten von Personendaten aufgrund der unmittelbaren Rechtsgrundlage genannt. Eine solche Rechtsgrundlage kann eine ausdrückliche Verpflichtung oder nur eine Ermächtigung zu einer bestimmten Datenbearbeitung sein. Je nach Art der Datenerhebung (z.B. durch neue Technologien), der Ausgestaltung der Zugriffsrechte auf die erhobenen Personendaten oder des Verwendungszwecks kann sich eine Bearbeitung als so wichtig oder grundlegend erweisen, dass sie selbst in einem Gesetz im formellen Sinn geregelt werden

muss. Anschliessend nimmt die Wendung «oder dies zur Erfüllung von Aufgaben erforderlich ist, für die eine Rechtsgrundlage besteht» die bisherige Anforderung der mittelbaren Gesetzesgrundlage auf. Mit der vorgenommenen Änderung des Absatzes 1 werden die Voraussetzungen für die zulässige Bearbeitung von Personendaten verdeutlicht und der Klarheit halber aufgrund der Fragen und Bemerkungen im Vernehmlassungsverfahren und zur Vermeidung von Missverständnissen die bisherige Formulierung möglichst beibehalten.

Für die Vornahme eines Profilings im Sinn des neuen § 2 Absatz 4^{bis} gelten die gleichen Voraussetzungen wie beim Bearbeiten von besonders schützenswerten Personendaten, nämlich dass sich die Zulässigkeit aus dem Gesetz selbst ergibt oder dieses zur Erfüllung einer im Gesetz umschriebenen (und damit konkreten) Aufgabe unentbehrlich ist (Abs. 2a und 2b). Der Einleitungssatz von Absatz 2 wird entsprechend ergänzt.

§ 5a

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

§ 6

Internationales Recht: Art. 7 Ziff. 1 und 10 Ziff. 1 Europaratsübereinkommen, Art. 19 DSRL

Die neuen internationalen Rechtsgrundlagen betonen die klare Zuordnung der Verantwortung für Datenbearbeitungen und verlangen insbesondere, dass das öffentliche Organ gegenüber der Aufsichtsstelle nachweisen kann, dass es die Datenschutzbestimmungen bei der Datenbearbeitung einhält. Der neue Absatz 1^{bis} und die Änderungen des Absatzes 2 nehmen diese Anforderungen auf. Die verlangten Nachweise für die Einhaltung der Datenschutzbestimmungen können die kantonalen und kommunalen Verwaltungen und die Gerichte insbesondere durch organisatorische Festlegungen, Konzepte und andere Führungsmittel leisten (z.B. spezifische Informatiksicherheits- und Zugriffskonzepte, allgemeine Organisationskonzepte). Generell kann der Nachweis vom verantwortlichen Organ auf der Grundlage eines Qualitätssicherungssystems in einem Datenschutzmanagementsystem erbracht werden. Systeme der Datenbearbeitung sollen in technischer und organisatorischer Hinsicht so ausgestaltet werden, dass sie den Grundsätzen des Datenschutzes entsprechen. Von zentraler Bedeutung bleibt dabei das datenschutzrechtliche Verhältnismässigkeitsprinzip (§ 4 Abs. 3 KDSG), aus dem weitere Leitplanken für die Datenbearbeitung abgeleitet werden können (insbes. Datenschutz durch Technikgestaltung und Datenschutz durch Voreinstellung, vgl. Art. 20 EU-Datenschutzrichtlinie). Für eine Ausformulierung dieses technischen Datenschutzes im Gesetz besteht kein Bedarf. Absatz 1^{bis} Satz 2 führt spezifische Konkretisierungen auf und erwähnt neben dem Stand der Technik insbesondere den zunehmend wichtigeren risikoorientierten Ansatz (vgl. auch unsere Ausführungen zu § 7a). Damit und mit dem Kriterium der Angemessenheit der technischen und organisatorischen Massnahmen wird die Bedeutung einer konkreten Interessen- und Nützlichkeitsabwägung bei den einzelnen Vorhaben von Kanton und Gemeinden zum Ausdruck gebracht.

Wie bisher darf das Datenbearbeiten auch einem anderen Organ oder Dritten übertragen werden (Abs. 2). Zentral bleibt die Vorschrift, wonach Personendaten nur so

bearbeitet werden dürfen, wie es das verantwortliche Organ selber darf. Das verantwortliche Organ hat insbesondere um den erforderlichen Datenschutz und die ausreichende Datensicherheit besorgt zu sein, weshalb schon aus diesem Grund eine schriftliche Vereinbarung für diese Art von Datenbearbeitung nötig ist. Für ausgelagerte kantonale Informatikdienstleistungen sei auch auf die §§ 13 ff. des Informatikgesetzes vom 7. März 2005 (SRL Nr. 26) verwiesen.

§ 7

Internationales Recht: Art. 7 Ziff. 2 Europaratsübereinkommen,
Art. 29–31 DSRL

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). Die Datensicherheit, verstanden als Ensemble von Massnahmen zur Vermeidung unbefugten Bearbeitens von Personendaten, ist Voraussetzung jedwelen Datenschutzes. Sie wird in unserem Entwurf im neuen § 6 Absatz 1^{bis} angesprochen. In § 7 sollen die im Zusammenhang mit der Datensicherheit vom internationalen Recht verlangten Melde- und Informationspflichten aufgenommen werden.

Liegt eine unbefugte Datenbearbeitung vor, welche die Datensicherheit verletzt und voraussichtlich zu einem hohen Risiko für Persönlichkeits- oder Grundrechtsverletzungen führt, hat das verantwortliche Organ dem oder der Beauftragten für den Datenschutz Meldung zu erstatten. 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 betroffener Personen eintreten kann. Verletzungen der Datensicherheit können fahrlässig oder missbräuchlich durch einen Mitarbeiter oder eine Mitarbeiterin der Verwaltung, 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 nachträgliche Massnahmen behoben worden sind (z.B. Zurücksetzen der Passwörter nach Passwortdiebstahl).

Gemäss Absatz 1^{bis} kann unter Umständen die Information der betroffenen Personen über eine Verletzung der Datensicherheit angezeigt sein. Zu denken ist an den Fall, wenn diese Personen zur Abwehr des Schadens selber Schutzmassnahmen ergreifen können (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 aber auch trotz Meldung an den Beauftragten oder die Beauftragte für den Datenschutz unterbleiben, etwa zur Wahrung der öffentlichen Sicherheit, insbesondere wenn die Information den Zweck behördlicher Untersuchungen oder Verfahren in Frage stellen würde. Auf die Information ist ausserdem zu verzichten, wenn sie einen unverhältnismässigen Aufwand erfordern würde oder gänzlich unmöglich ist. An die Stelle der persönlichen Information kann unter Umständen eine öffentliche Bekanntgabe treten (vgl. § 30 Abs. 1c Gesetz über die Verwaltungsrechtspflege [VRG] vom 3. Juli 1972). Das Weitere, namentlich der Inhalt der Meldung (z.B. Art der Verletzung der Datensicherheit, Folgen für betroffene Personen, Massnahmen), soll in der Verordnung umschrieben werden.

Die neuen europäischen Rechtsgrundlagen verlangen eine Beurteilung der wahrscheinlichen Auswirkungen der beabsichtigten Datenbearbeitungen. Mittels sogenannter Datenschutz-Folgenabschätzungen sollen Risiken identifiziert und bewertet werden, die durch den Einsatz von Technologien und Systemen im Rahmen der Datenverarbeitung entstehen. Nach unserem Entwurf, welcher sich an die spezifischere EU-Datenschutzrichtlinie und das neue eidgenössische DSG anlehnt, ist eine formelle Datenschutz-Folgenabschätzung 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). Der risikoorientierte Ansatz liegt bereits dem geltenden § 7 Absatz 1 zugrunde («angemessene Massnahmen») und wird durch die neue Bestimmung verstärkt. Diese Voraussetzung ist relativ offen formuliert und muss durch Praxis und Rechtsprechung konkretisiert werden. Dabei muss es auch möglich sein, 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. Das verantwortliche Organ ist verpflichtet, die Folgen einer geplanten Datenbearbeitung für die Betroffenen abzuschätzen. 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 dient auch dem Nachweis der Sicherstellung der Datenschutzvorschriften gemäss § 6 Absatz 2. Die Einzelheiten zur Datenschutz-Folgenabschätzung können durch Verordnung geregelt werden.

Auf der Grundlage der Abschätzungen nach Absatz 1, insbesondere einer Datenschutz-Folgenabschätzung, kann der Beauftragte für den Datenschutz Stellung nehmen und innert angemessener Frist allenfalls nötige Nachbesserungen beim Datenschutz vorschlagen (Abs. 2). Die Empfehlungen des Beauftragten sollen sicherstellen, dass die Risiken bei den Datenbearbeitungsvorhaben rechtzeitig und hinreichend abgeklärt werden und gegebenenfalls mit verhältnismässigen rechtlichen, organisatorischen oder technischen Massnahmen weiter reduziert werden können. Bei Rechtsetzungsvorhaben des Kantons, welche die Bearbeitung von Personendaten betreffen, kann sich der Beauftragte bei Bedarf mittels Stellungnahmen in das Vernehmlassungsverfahren einbringen (vgl. § 23 Abs. 1e KDSG-Entwurf).

Im Anwendungsbereich der EU-Datenschutzrichtlinie müssen die verantwortlichen Organe einen eigenen «Datenschutzbeauftragten oder eine Datenschutzbeauftragte» bestimmen. Wie im Bundesrecht ist für diese organisationsinterne Funktion in unserem Entwurf die Bezeichnung «Datenschutzberater oder -beraterin» vorgesehen, um Verwechslungen mit dem oder der Beauftragten für den Datenschutz als unabhängiger Aufsichtsstelle auszuschliessen. In der kantonalen Verwaltung und den Gerichten soll es sich bei den entsprechenden Personen um Angestellte handeln, die sich Kenntnisse auf dem Gebiet des Datenschutzes angeeignet haben und

diese neben ihrer Haupttätigkeit einbringen können. Im Vordergrund dürfte für die Angestellten in der Verwaltung eine Stabstätigkeit, ausgenommen die Informativität, stehen. Die Datenschutzberaterinnen und -berater sollen die Mitarbeitenden, die Personendaten bearbeiten, amts- beziehungsweise gerichtsintern unterstützen, indem sie diese hinsichtlich der Datenschutzbelange unterrichten und beraten. Zudem sorgen sie für die Datenschutz-Folgenabschätzungen (z.B. durch Begleitung) und sind erste Ansprechpersonen des Beauftragten für den Datenschutz (Abs. 2). Dem verantwortlichen Organ bleibt es unbenommen, seinem Datenschutzberater oder seiner Datenschutzberaterin weitere Aufgaben zu übertragen (z.B. als Kontaktstelle für Datenerhebungen nach § 8 Abs. 4a oder für Datenbekanntgaben nach § 9 ff.). Die Pflicht zur Bezeichnung des Datenschutzberaters oder der Datenschutzberaterin soll im kantonalen Bereich die Strafverfolgung und den Strafvollzug, das heisst die Strafverfolgungsbehörden (Polizei, Staatsanwaltschaft), die Strafvollzugsbehörden und die Strafgerichte betreffen. Den übrigen Gemeinwesen steht es frei, einen Datenschutzberater oder eine Datenschutzberaterin zu bezeichnen, sei es inner- oder ausserhalb der Verwaltung. Bei Bedarf soll der Regierungsrat ein Gemeinwesen dazu verpflichten können, damit eine hilfreiche Koordinationsstelle mit Scharnierfunktion zu dem oder der Beauftragten für den Datenschutz geschaffen werden kann.

§ 8

Internationales Recht: Art. 8 Europaratsübereinkommen,
Art. 13 DSRL

Transparenz und Information sind wichtige Anliegen des Datenschutzrechtes. Die öffentlichen Organe stehen in der Pflicht, die betroffenen Personen über die Erhebung von Personendaten aktiv zu informieren. Dem geltenden § 8 liegt der Transparenzgedanke ebenfalls zugrunde. Die Bestimmung soll im Hinblick auf die neuen internationalen Rechtsgrundlagen aktualisiert werden. 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 den Zweck des Bearbeitens, die Aufbewahrungsdauer, allfällige Dritte als Datenempfänger und die Rechte der betroffenen Personen (Abs. 4). Neu soll über diese Angaben nicht nur informiert werden, wenn die befragte Person dies ausdrücklich verlangt. Werden die Daten mit Formularen (auf Papier oder mittels Internet in einem elektronischen Format) erhoben, können die Angaben selbstverständlich weiterhin 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 (insbes. gesetzliche Regelung).

Gemäss Absatz 5 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).

§ 12a

In dieser Bestimmung wird lediglich Absatz 3 in sprachlicher Hinsicht präzisiert (insbes. wird der bisherige Satz 2 als eigenständiger Absatz 4 gefasst und dadurch in der Anwendung flexibler).

§ 13

Diese Bestimmung ist gesetzestechnisch zu bereinigen: Für Personendaten, die von der Luzerner Polizei erhoben werden, verweisen wir auf die von Ihrem Rat geänderten Bestimmungen des Gesetzes über die Luzerner Polizei (vgl. dazu §§ 4-4a PolG; SRL Nr. 350, und unsere Ausführungen in der [Botschaft B 74-2017](#) über die Aktualisierung des Polizeirechts). Absatz 2 wie auch der Vorbehalt dieses Absatzes in Absatz 1 sind deshalb zu streichen. Mit diesen Streichungen kann im gleichen Zug auf den Verweis auf § 18 Absatz 1 verzichtet werden.

Zur Datenbearbeitung nach dem Grundsatz der Verhältnismässigkeit gehört die Löschung von Personendaten beziehungsweise die regelmässige Überprüfung, ob die Datenbestände zur Aufgabenerfüllung noch erforderlich sind. Absatz 3 ermächtigt unseren Rat, im Verordnungsrecht Löschfristen und Massnahmen zur Sicherstellung der regelmässigen Überprüfung vorzusehen.

Gemäss den Luzerner Richtlinien über die Gesetzestechnik entfällt die Sachüberschrift dieser Bestimmung, da der Zwischentitel («Archivieren und Vernichten von Personendaten») den Inhalt der Bestimmung bereits festhält und der Abschnitt keine weitere Bestimmung umfasst.

§ 14

Internationales Recht: Art. 24 DSRL

Wie in Kapitel 4.2.5.2 erläutert, wird auf das allgemeine Register der Datensammlungen inskünftig verzichtet. Indes müssen gemäss EU-Datenschutzrichtlinie die Gerichts- und Verwaltungsorgane, die in den Bereichen der Strafverfolgung und der Strafvollstreckung tätig sind, ein Verzeichnis aller Kategorien ihrer Datenbearbeitungstätigkeiten führen. Dieses Verzeichnis schliesst praxisbezogen an die entsprechenden Tätigkeiten an und umfasst insbesondere Angaben zum Bearbeitungszweck, zu den Kategorien von Empfängern der Personendaten und den Kategorien der betroffenen Personen. Die Erstellung eines solchen Verzeichnisses kann als Massnahme der Selbstregulierung im Datenschutz angesehen werden. Zur Durchsetzung dieser Anforderung des übergeordneten Rechts wird unser Rat das Nähere durch Verordnung regeln. Über die minimale Regelung hinaus ist es dem Beauftragten für den Datenschutz ein Anliegen, dass alle Dienststellen ein Bearbeitungsverzeichnis führen. Im Rahmen der Umsetzung des Datenschutzgesetzes werden wir diesen Antrag prüfen. Die Gemeinden können über die Führung eines oder mehrerer Verzeichnisse selber entscheiden.

Vorbemerkung zu den §§ 15–19

Das Recht jeder Person, Auskunft zu erhalten, ob Daten über sie von einem Organ bearbeitet werden, und gegebenenfalls auch die Einsicht in die Personendaten, 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](#)) Mit den vorgesehenen Änderungen werden Präzisierungen am Umfang des Auskunftsrechts vorgenommen. Diese orientieren sich an der entsprechenden Bestimmung des DSGVO und an den Anforderungen des internationalen Rechts. 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 zu anderen Ansprüchen nach § 18 müssen kostenlos gewährt werden, dies aufgrund des unveränderten § 20 und in Übereinstimmung mit Artikel 12 der EU-Datenschutzrichtlinie.

§ 15

Internationales Recht: Art. 8 Europaratsübereinkommen,
Art. 14 DSRL

Aufgrund der Änderung von § 2 Absatz 7 ist der Begriff des Inhabers der Datensammlung durch «verantwortliches Organ» beziehungsweise «Organ» zu ersetzen (Abs. 1 und 2).

Der Umfang des Auskunftsrechts ergibt sich grundsätzlich aus der Informationspflicht der Organe. Inhaltlich orientiert sich § 15 Absatz 2 an § 8 Absatz 4. Zusätzlich werden Angaben über die Herkunft der Personendaten als Teil des Informationsanspruchs angeführt. Die Aufzählung ist nicht abschliessend zu verstehen. Das Auskunftsrecht ist hingegen kein allgemeines Einsichtsrecht in amtliche Dokumente und kein Editionsrecht für Urkunden; so umfasst es lediglich die Auskunft über und die Einsicht in die eigenen 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 erschliessen (insbes. bei schriftlichen Auskünften durch den Briefkopf der Mitteilung) und hier nicht noch einmal aufzuführen sind. Werden Daten systematisch erhoben (z.B. auf einem Formular im Internet oder auf Papier), sollten möglichst alle Angaben auf dem Formular oder dem zugehörigen Beiblatt angebracht werden.

§ 17

Aufgrund der Änderung von § 2 Absatz 7 ist der Begriff des Inhabers der Datensammlung durch «verantwortliches Organ» beziehungsweise «Organ» zu ersetzen (Abs. 1 und 2).

§ 18

Internationales Recht: Art. 9 Europaratsübereinkommen,
Art. 16 DSRL

Nach den Auskunfts- und Berichtigungsansprüchen der §§ 15 und 17 handelt diese Bestimmung von den sogenannten anderen Ansprüchen. Die von einer unrechtmässigen Datenbearbeitung betroffene Person verfügt insbesondere über Unterlassungs- und Beseitigungsansprüchen. In Absatz 1 soll die Löschung der Daten ausdrücklich aufgenommen werden. Dies aufgrund der praktischen Bedeutung in der elektronischen Datenverwaltung, aber auch weil der Anspruch auf Löschung in den internationalen Rechtsgrundlagen und auch im eidgenössischen Datenschutzgesetz

(Art. 41) ausdrücklich genannt wird. Als «sonstige» Beseitigungsform im Sinn des Absatzes 1b kann in einem IT-System die Ergänzung von Daten mittels eines verknüpften Eintrags angesehen werden, beispielweise wenn in einem Rapportsystem der ursprüngliche Eintrag nicht korrigiert werden darf.

In Absatz 2 wird der Anspruch der betroffenen Person bei Datenbekanntgaben etwas allgemeiner gefasst. Dadurch können die Organe flexibler und damit bürgerfreundlicher auf berechnigte Bearbeitungsfordernngen eingehen. Beispielsweise könnte das Staatsarchiv oder ein kantonales Museum – nach einer umfassenden Interessenabwägung zwischen Zugangsinteresse und Persönlichkeitsschutz – auf eine Internetpublikation verzichten (Einschränkung gemäss Abs. 2c).

§ 19

Internationales Recht: Art. 9 Europaratsübereinkommen,
Art. 16 DSRL

In einem Fall, in dem die Auskunft mit dem Grund der Auskunftsverweigerung kollidiert, kann das zuständige Organ die Anforderungen an die Begründung inhaltlich und umfangsmässig reduzieren, ohne auf einen formellen Entscheid nach dem Verwaltungsrechtspflegegesetz zu verzichten. Es wird vorgeschlagen, die singuläre Regelung des geltenden Absatzes 2 zu streichen.

Zwischentitel nach § 20, § 21

Unter Ziffer 4 enthält das geltende Gesetz die Bestimmungen über den Rechtsschutz und die Aufsicht sowie eine Strafbestimmung. Dieser Teil soll auf zwei Teile aufgeteilt werden. Da der oder die Beauftragte für den Datenschutz in § 24 die Kompetenz erhält, verbindliche Anordnungen in Form von Verfügungen zu treffen, wird die Bestimmung über den Rechtsschutz verschoben und im neuen Teil 4a als § 24b neu gefasst. § 21 ist aus diesem Grund aufzuheben.

§ 22

Internationales Recht: Art. 15 Europaratsübereinkommen, Art. 41–44 DSRL

Absatz 1: Neu soll der Kantonsrat den Beauftragten oder die Beauftragte für den Datenschutz wählen, dies auf Antrag des Regierungsrates und auf eine Amtsdauer von vier Jahren (Abs. 1). Die Wahl auf Amtsdauer entspricht den internationalen Anforderungen. Sie soll die Unabhängigkeit des oder der Beauftragten für den Datenschutz stärken. Zum Wechsel der Wahlkompetenz verweisen wir auf unsere Ausführungen in Kapitel 4.2.4.1.

Absatz 1^{bis}: Entsprechend der Regelung in § 3 Absatz 3 des Finanzkontrollgesetzes soll der Entscheid über die Besoldungseinreihung beim Regierungsrat liegen. Dieser stellt sicher, dass die Einreihung des oder der Beauftragten ins Gesamtgefüge der Besoldungen der anderen Funktionen in der Funktionsgruppe Ia der kantonalen Verwaltung passt.

Absatz 1^{ter}: Das Personalgesetz (PG) vom 26. Juni 2006 (SRL Nr. 51) gilt auch für die von einem gesetzgebenden Organ auf Amtsdauer gewählten kantonalen Mitarbeiterinnen und Mitarbeitern. Bei fristloser Auflösung des Arbeitsverhältnisses, insbesondere bei vorsätzlicher schwerer Amtspflichtverletzung, gilt somit § 19 PG. Wie in § 4 Absatz 4 des Finanzkontrollgesetzes vom 8. März 2004 (SRL Nr. 615) soll indes die Spezialregelung gelten, dass die Auflösung aus wichtigen Gründen zwar

durch den Regierungsrat ausgesprochen, aber von der Geschäftsleitung des Kantonsrates genehmigt werden muss.

§ 22a

Internationales Recht: Art. 15 Europaratsübereinkommen, Art. 41–44 DSRL

Der oder die Beauftragte für den Datenschutz muss über die erforderlichen Qualifikationen, Erfahrung und Sachkunde verfügen, um die vorgeschriebenen Aufgaben erfüllen zu können. Die Aufsichtsstelle ist keine politische Behörde und deshalb mit einer Fachperson zu besetzen, was Absatz 1 verdeutlicht.

Eine Unvereinbarkeit soll bestehen zwischen dem Amt des oder der Beauftragten für den Datenschutz und einem anderen öffentlichen Amt (Abs. 2). Bei einem Teilpensum muss dem Beauftragten oder der Beauftragten aber eine andere (privatrechtliche) Erwerbstätigkeit bewilligt werden können (Abs. 3).

§ 22b

Internationales Recht: Art. 15 Europaratsübereinkommen, Art. 41–44 DSRL

Diese Bestimmung regelt die Finanz- und Personalkompetenzen des oder der Beauftragten für den Datenschutz als Leiter beziehungsweise Leiterin der Aufsichtsstelle. Die Verfügungsbefugnis umfasst im Rahmen des Voranschlags alle Ausgaben, die einer Dienststelle nach § 32 Absatz 2 der Verordnung zum Gesetz über die Steuerung der Finanzen und Leistungen (SRL Nr. 600a) zukommen. Der oder die Beauftragte kann im Rahmen der verfügbaren Ausgaben Anschaffungen tätigen und falls nötig auch Sachverständige beiziehen. Er oder sie verfügt über die für Anstellungen nötigen personalrechtlichen Befugnisse wie auch der oder die Beauftragte grundsätzlich dem kantonalen Personalrecht unterstellt bleibt.

§ 23

Internationales Recht: Art. 15 Europaratsübereinkommen, Art. 46 und 47 DSRL

Der oder die Beauftragte für den Datenschutz überwacht 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 Absatz 1a erfolgt anlassfrei und nach einem eigenen Prüfprogramm. Eine anlassbezogene Kontrolle auf eine konkrete Beanstandung hin muss jedoch auch möglich sein. Dieser Anforderung des internationalen Rechts soll mit der Ergänzung des Absatzes 1c, wonach der oder die Beauftragte aufsichtsrechtliche Anzeigen behandelt, Rechnung getragen werden. Mit der Wendung «innert angemessener Frist» wird auf die EU-Datenschutzrichtlinie Bezug genommen, die eine Information über den Stand oder das Ergebnis der Abklärungen zuhanden des Eingabestellers innerhalb von drei Monaten postuliert.

Zu den vom internationalen Recht verlangten wirksamen Befugnissen ist auch die Möglichkeit zu (förmlichen) Empfehlungen zu Datenbearbeitungen der öffentlichen

Organe zu zählen. Der neue Absatz 1c^{bis} nimmt dieses Instrument auf. Zu Empfehlungen und Verfügungen im Fall von Datenschutzverletzungen verweisen wir auf § 24.

Absatz 1d wird zur ersatzlosen Streichung vorgeschlagen. 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 erkannten Risiken beispielweise im Zusammenhang mit der Verwendung von neuen Technologien in der Verwaltung Stellung beziehen.

In Absatz 1f wird aufgrund des internationalen Rechts die Sensibilisierung der Öffentlichkeit für den Datenschutz aufgenommen. Namentlich im Rahmen der jährlichen Berichterstattung (bisher Abs. 1k, neu Abs. 2) wurde bereits Öffentlichkeitsarbeit in diesem Sinn betrieben.

In Absatz 1h findet die vorgängige Stellungnahme zu Datenbearbeitungen mit hohem Risiko Erwähnung. Soweit die Vorabkonsultation des oder der Beauftragten für den Datenschutz im Rahmen der Abklärungen der Datenschutz-Folgenabschätzung erfolgt, ist auf § 7a Absatz 2 zu verweisen.

Wie in Kapitel 4.2.5.2 und zu § 14 ausgeführt entfällt die Pflicht zur Führung des Registers über die Datensammlungen. Absatz 2 ist deshalb zu streichen.

Absatz 3 tritt anstelle von Absatz 1k. Geregelt werden die Pflicht zur Berichterstattung und die Behandlung des Tätigkeitsberichts durch Regierung und Parlament. Die internationalen Rechtsgrundlagen verlangen eine Berichterstattung in jährlicher (EU-Datenschutzrichtlinie) beziehungsweise periodischer (Europaratsübereinkommen) Abfolge. Zum verbesserten parlamentarischen Verfahren sei auf unsere Ausführungen in Kapitel 4.2.4.2 verwiesen.

§ 24

Internationales Recht: Art. 15 Europaratsübereinkommen,
Art. 47 DSRL

In allen Absätzen dieser Bestimmung wird der Begriff «der Beauftragte» durch «der oder die Beauftragte» sowie in Absatz 2 der Begriff «Datensammlung» durch «Daten» ersetzt.

Absätze 3 und 4: Dem oder der Beauftragten für den Datenschutz muss aufgrund der internationalen Rechtsgrundlagen die Befugnis zukommen, bei Verstößen gegen Datenschutzrecht verbindliche Anordnungen (in Form von Verfügungen) zu treffen. Das heutige System, bei dem das öffentliche Organ eine Verfügung erlässt, welche der oder die Beauftragte anfechten muss, ist umzukehren. Neu muss die Verfügung des oder der Beauftragten vom Gemeinwesen beziehungsweise von dessen berechtigtem Organ vor Gericht angefochten werden. Ein anfechtbarer Ent-

scheid soll gemäss unserem Entwurf in der Regel erst nach einer – unter Umständen bloss faktischen – Ablehnung einer Empfehlung erlassen werden. Inhalt einer Empfehlung wie einer Verfügung kann die Einschränkung oder Einstellung einer bestimmten Datenbearbeitung und die Löschung oder Vernichtung von bereits erhobenen Personendaten sein (vgl. § 18). Zeichnet sich ab, dass ein Organ die entsprechende Empfehlung nicht befolgt, ist der oder die Beauftragte ausserdem befugt, um den bestehenden Zustand zu erhalten oder bedrohte rechtliche Interessen einstweilen zu schützen, eine vorsorgliche Verfügung zu treffen. Massgebend ist in einem solchen Fall § 45 VRG, da für das Verfahren das Gesetz über die Verwaltungsrechtspflege zur Anwendung gelangt (§ 21 Abs. 1 KDSG). Eine vorsorgliche Massnahme könnte die Einschränkung oder Einstellung der Datenbearbeitung bis zur Umsetzung der Empfehlung beziehungsweise bis zur richterlichen Klärung sein.

Zwischentitel nach § 24

Im Teil 4a unseres Entwurfes werden die bisherige Straf- und die geänderte Rechtsschutzbestimmung gefasst.

§ 24b

Internationales Recht: Art. 9, 12, 15 Ziff. 9 Europaratsübereinkommen, Art. 53 DSRL

Während der unveränderte § 24a das Strafverfahren zum Gegenstand hat, regelt diese Bestimmung den Rechtsschutz im Verwaltungsverfahren. Vom geltenden § 21 wird Absatz 1 übernommen, dessen Absatz 2 hingegen fällt ersatzlos weg, dies aufgrund der Änderung von § 24 Absatz 4.

Gemäss Absatz 2 sollen Entscheide des oder der Beauftragten für den Datenschutz unmittelbar mit Verwaltungsgerichtsbeschwerde beim Kantonsgericht angefochten werden können (vgl. § 148 Abs. 1d VRG). Dabei soll das vom Entscheid betroffene Organ den Entscheid des oder der Beauftragten mit Verwaltungsgerichtsbeschwerde anfechten und dementsprechend vor Gericht als Partei auftreten dürfen (§ 129 Abs. 2 VRG). Das Kantonsgericht hätte als erstes Rechtsmittel die Verwaltungsbeschwerde an den Regierungsrat bevorzugt. Aufgrund der unabhängigen Stellung des oder der Beauftragten für den Datenschutz bei der Aufsicht über die Verwaltung ist indes vom Regierungsrat als Beschwerdeinstanz abzusehen. Wir erachten die Einsetzung des Kantonsgerichtes als angemessen und zweckmässig, zumal es in den Fällen von Beanstandungen privater Personen um persönlichkeits- oder grundrechtliche Aspekte von Datenbearbeitungen geht. Eine Aufteilung des Rechtsmittelweges je nach Inhalt der Beschwerde wäre ineffizient und unübersichtlich. Auch die EU-Datenschutzrichtlinie verlangt ein «wirksames» gerichtliches Rechtsmittel und der KdK-Leitfaden empfiehlt deshalb, den direkten Weg an das Kantonsgericht vorzusehen.

§§ 26 und 26a

Die bisherige Übergangsbestimmung (§ 26) ist schon längst obsolet. Es braucht allerdings eine neue Übergangsregelung. Wegen der Umstellung auf das Amtsdauersystem (§ 22 Abs. 1) ist eine Übergangsfrist vorzusehen. Damit kann Ihr Rat die Wahl jeweils im zweiten Jahr der Legislatur, erstmals auf den 1. Januar 2022 für den Rest der Amtsdauer 2019–2023, vornehmen (§ 26a).

6.2 Weitere Gesetze

6.2.1 Gesetz über die Niederlassung und den Aufenthalt

§ 12

In dieser Bestimmung des Gesetzes über die Niederlassung und den Aufenthalt vom 1. Dezember 1948 (SRL Nr. 5) ist der geänderte Erlassstitel («Kantonales Datenschutzgesetz») zu berücksichtigen (Abs. 2).

6.2.2 Organisationsgesetz

§ 21b

Zur Erfüllung ihres Auftrages nach den Bestimmungen des Gesetzes über die Organisation von Regierung und Verwaltung (Organisationsgesetz, OG; SRL Nr. 20) setzt die Verwaltung elektronische Informations-, Geschäftsverwaltungs- und Dokumentationssysteme ein. Im elektronischen Geschäftsverwaltungssystem bereiten die Verwaltungsorgane ihre eigenen Geschäfte vor und gestalten die Geschäftsprozesse. Angesichts der weiteren Digitalisierung der Verwaltung gibt Absatz 3 dem Regierungsrat die Kompetenz für weitere Vorschriften, mit denen diese Prozesse koordiniert werden können.

Im KDSG-Entwurf ist vorgesehen, den Begriff der Personendaten auf natürliche Personen zu beschränken (vgl. unsere Ausführungen in Kap. 5.3). Entsprechend dem bisherigen § 5 Absatz 1 KDSG bildet Absatz 2 die gesetzliche Grundlage dafür, dass die Verwaltungsorgane weiterhin Angaben über juristische Personen und Personengesellschaften des Handelsrechts bearbeiten dürfen, wenn dies zur Aufgabenerfüllung erforderlich ist. Die Bearbeitung dieser Daten ist rechtmässig, wenn sie zur Erfüllung der Verwaltungsaufgabe erforderlich ist, für die eine Rechtsgrundlage besteht, oder wenn die Datenbearbeitung ausdrücklich in der Rechtsgrundlage geregelt ist. Im Anwendungsgebiet des Organisationsgesetzes gehört insbesondere die in § 20 verankerte Aufgabe der Verwaltung dazu, die Geschäfte des Regierungsrates vorzubereiten. Im elektronischen Geschäftsverwaltungssystem bereiten die Departemente die Geschäfte des Regierungsrates vor oder haben Zugang zu Regierungsgeschäften, die sie von der Staatskanzlei zur Vorbereitung zugeteilt erhalten (z.B. Vernehmlassungen des Bundes). Entsprechend greifen innerhalb eines Departementes die einzelnen Verwaltungseinheiten auf die elektronische Dokumentenablage zu. Im Übrigen gelten für die Verwaltungsorgane die Bestimmungen des Spezialrechts, beispielweise bei der Erhebung von Daten für Statistiken oder die Archivierung von Verwaltungsunterlagen.

6.2.3 Registergesetz

§§ 18 und 19

In diesen beiden Bestimmungen des Gesetzes über die Harmonisierung amtlicher Register (Registergesetz) vom 25. Mai 2009 (SRL Nr. 25) ist aufgrund des geänderten Erlassstitels der Verweis auf das Kantonale Datenschutzgesetz anzupassen.

6.2.4 Informatikgesetz

§ 3

Diese Bestimmung des Informatikgesetzes vom 7. März 2005 (SRL Nr. 26) verweist hinsichtlich verschiedener Begriffsdefinitionen auf das Kantonale Datenschutzgesetz. In Absatz 1 ist aufgrund des geänderten Erlassitels der Verweis anzupassen, und es sind die neueren Begriffe einzusetzen. Auch in Absatz 4 ist ein Begriff anzupassen.

Da sich der Begriff der Personendaten laut § 2 Absatz 1 KDSG-Entwurf auf die natürlichen Personen beschränkt und im Informatikrecht der bisherige, umfassendere Datenbegriff, der sich auch auf juristische Personen sowie Personengesellschaften des Handelsrechts bezieht, beibehalten werden soll, ist in Absatz 1 eine klärende Ergänzung nötig.

§§ 4 und 5

Bei den Techniken der Datenherstellung wie auch der versuchsweisen Bewilligung von zentralen Datenbanken wird das Profiling ergänzt (§§ 4 und 5, jeweils Abs. 3). Aufgrund der Systematik des KDSG gehören Persönlichkeitsprofile zu den besonders schützenswerten Personendaten, weshalb sie in diesen Bestimmungen nicht mehr gesondert erwähnt werden müssen.

§§ 6 und 7

In den §§ 6 Absatz 5 und 7 Absatz 1 ist lediglich der Erlassitel in den Verweisen anzupassen.

§§ 10 und 11

Diese Bestimmungen sind auf das Kantonale Datenschutzgesetz anzupassen (Begriffe, Verzeichnis der Datenbearbeitungstätigkeiten).

§ 15

In Absatz 2 wird aus Gründen der Klarheit der im Kantonalen Datenschutzgesetz eingeführte und auch im Informatikgesetz (§§ 10 und 11) bereits benützte Begriff der Aufsichtsstelle verwendet.

§§ 16 und 18

In verschiedenen Absätzen dieser Bestimmungen wird der im Datenschutz verwendete Begriff des verantwortlichen Organs eingesetzt.

6.2.5 Statistikgesetz

§ 3

In dieser Bestimmung des Statistikgesetzes vom 13. Februar 2006 (SRL Nr. 28a), welcher hinsichtlich der Definition der Personendaten auf das Kantonale Datenschutzgesetz verweist, ist aufgrund des geänderten Erlassitels der Verweis anzupassen (Abs. 8 Satz 1). Da sich der Begriff der Personendaten laut § 2 Absatz 1 KDSG-Entwurf auf die natürlichen Personen beschränkt und im Statistikrecht der bisherige, umfassendere Datenbegriff, der sich auch auf juristische Personen sowie Personengesellschaften des Handelsrechts bezieht, beibehalten werden soll, sind klärende Ergänzungen nötig (Abs. 8 Satz 2, Abs. 9).

§ 16

In Absatz 2 ist lediglich der Begriff der Datensammlung zu ersetzen (vgl. im KDSG-Entwurf aufgehobener § 2 Abs. 6).

§ 22

In Absatz 3 ist die Wendung «im Sinn des Datenschutzgesetzes» zu streichen, da sich die Bestimmung nicht nur auf Daten von natürlichen Personen beziehen soll, wie sie im Kantonalen Datenschutzgesetz definiert werden.

6.2.6 Geoinformationsgesetz

§§ 3, 9 und 20

In diesen Bestimmungen des Gesetzes über die Geoinformation und die amtliche Vermessung (Geoinformationsgesetz, GIG) vom 8. September 2003 (SRL Nr. 29) ist der Begriff des Inhabers oder der Inhaberin einer Datensammlung zu ersetzen (vgl. § 2 Abs. 7 KDSG-Entwurf).

6.2.7 Gesetz über die Videoüberwachung

§ 6

In dieser Bestimmung des Gesetzes über die Videoüberwachung vom 20. Juni 2011 (SRL Nr. 39) ist aufgrund des geänderten Erlassitels lediglich der Verweis auf das Kantonale Datenschutzgesetz anzupassen.

6.2.8 Gesetz über die Verwaltungsrechtspflege

§ 141a

Im verwaltungsrechtlichen Verfahren gelangt – abgesehen von den allgemeinen Verfahrensgrundrechten der Bundesverfassung – die kantonale Verfahrensordnung zur Anwendung, mithin das Gesetz über die Verwaltungsrechtspflege (VRG) 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). Der neue § 141a regelt den Umgang mit persönlichen Daten nach Abschluss der Gerichtsverfahren insoweit, 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. Vorbehältlich weiter gehender Anonymisierungen und anderweitiger Einschränkungen aufgrund überwiegender öffentlicher 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 [BGE 133 I 106](#) E. 8.3). Auf eine weiter gehende Regelung im Verwaltungsverfahren 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). 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, und § 36 Abs. 1 Justiz-Kostenverordnung vom 26. März 2013, SRL Nr. 265). 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 in einer im Internet zugänglichen Datenbank dar ("Luzerner Gerichts- und Verwaltungsentscheide", vgl. § 13 PubG).

6.2.9 Personalgesetz

§ 67

Mit dieser Bestimmung wird eine schon längere bestehende Gesetzeslücke im Personalgesetz geschlossen (Abs. 3 Satz 3). Für die der Staatskanzlei administrativ zugeordneten Organisationseinheiten soll der Staatsschreiber oder die Staatsschreiberin als zuständig erklärt werden, die sogenannten übrigen personalrechtlichen Entscheide zu treffen. Im vorliegenden Sachzusammenhang bezieht sich diese Zuständigkeit auf die vom Kantonsrat als gesetzgebendem Organ gewählte Funktion des oder der Beauftragten für den Datenschutz, nicht aber auf die weiteren Mitarbeiterinnen und Mitarbeiter der kantonalen Aufsichtsstelle (§ 22b Abs. 2 KDSG-Entwurf; vgl. § 4 Absatz 2 Finanzkontrollgesetz).

6.2.10 Gesetz über den Justizvollzug

§ 22

In dieser Bestimmung des Gesetzes über den Justizvollzug (JVG) vom 14. September 2015 (SRL Nr. 305) ist lediglich klarzustellen, dass die Einsicht von Fachpersonen in Vollzugsakten auch die Ergebnisse von Profilings umfassen kann. Die Justizvollzugsbehörden müssen berechtigt sein, die Vollzugsakten der Strafbehörden über die eingewiesene Person einzusehen, soweit dies für ihre Aufgabenerfüllung erforderlich ist, und befugt sein, die Vollzugsakten an berechnigte Fachpersonen weiterzugeben. Nicht Regelungsgegenstand der Norm ist hingegen die Vornahme eines Profilings zum Zwecke des Justizvollzugs. Führungsberichte, Verlaufsberichte von Therapien, neu erstellte Gutachten und Ähnliches bilden die Grundlagen für die Massnahmen der Vollzugseinrichtungen.

6.2.11 Gesetz über die Luzerner Polizei

§§ 4 und 4^{bis}

In diesen Bestimmungen des Gesetzes über die Luzerner Polizei (PoIG) vom 27. Januar 1998 (SRL Nr. 350) sind verschiedene Begriffe anzupassen. Der spezifische datenschutzrechtliche Begriff der «Datensammlung» wird aufgehoben (vgl. § 2 Abs. 6 KDSG; er geht in den Begriffen der Personendatenbearbeitung beziehungsweise der Datenbearbeitungssysteme auf. Neu wird die gesetzliche Grundlage für Profilings im Sinn des neuen § 2 Absatz 4^{bis} KDSG geschaffen (§ 4 Abs. 2d), welche

hauptsächlich für die Belange der Kriminalpolizei von Nutzen sind. In zwei Absätzen ist der geänderte Erlassartikel des KDSG bei den Verweisen zu berücksichtigen.

6.2.12 Archivgesetz

§ 3

Da sich der Begriff der Personendaten laut § 2 Absatz 1 KDSG-Entwurf auf die natürlichen Personen beschränkt und im Gesetz über das Archivwesen (Archivgesetz) vom 16. Juni 2003 (SRL Nr. 585) der bisherige, umfassendere Datenbegriff, der sich auch auf juristische Personen sowie Personengesellschaften des Handelsrechts beziehen kann, beibehalten werden soll, ist eine Ergänzung nötig (Abs. 5). Ausserdem ist der geänderte Erlassartikel des KDSG zu berücksichtigen.

§ 6

Das Staatsarchiv berät gemäss § 4 Absatz 2a die öffentlichen Organe bei der Verwaltung ihrer Unterlagen und unterstützt sie bereits bei der Vorbereitung von Ablieferungen. Setzt die Verwaltung elektronische Informations-, Geschäftsverwaltungs- und Dokumentationssysteme ein, muss das Staatsarchiv die Möglichkeit haben, schon vor der Ablieferung der Daten Zugriff auf die Systeme zu erhalten, um die sachgemässe Vorbereitung der Übernahme zu sichern. Die öffentlichen Organe sind für die Zugriffsverwaltung verantwortlich (Abs. 2).

6.2.13 Steuergesetz

§ 137

Da sich der Begriff der Personendaten laut § 2 Absatz 1 KDSG-Entwurf auf die natürlichen Personen beschränkt und im Steuerrecht der bisherige, umfassendere Datenbegriff, der sich auch auf juristische Personen sowie Personengesellschaften des Handelsrechts beziehen kann, beibehalten werden soll, ist eine begriffliche Anpassung in Absatz 5 dieser Bestimmung des Steuergesetzes (StG) vom 22. November 1999 (SRL Nr. 620) nötig.

6.2.14 Gesundheitsgesetz

§ 53h

In dieser Bestimmung des Gesundheitsgesetzes (GesG) vom 13. September 2005 (SLR Nr. 800) ist der geänderte Erlassartikel des KDSG im Verweis zu berücksichtigen (Abs. 4).

6.2.15 Spitalgesetz

§ 6g

In dieser Bestimmung des Spitalgesetzes vom 11. September 2006 (SRL Nr. 800a) ist der geänderte Erlassartikel des KDSG im Verweis zu berücksichtigen (Abs. 1).

6.2.16 Einführungsgesetz zum Bundesgesetz über die Krankenversicherung

§ 5a

In dieser Bestimmung des Einführungsgesetzes zum Bundesgesetz über die Krankenversicherung vom 23. März 1998 (SRL Nr. 865) ist der geänderte Erlassstitel des KDSG zu berücksichtigen (Abs. 8).

6.2.17 Sozialhilfegesetz

§ 52a

In dieser Bestimmung des Sozialhilfegesetzes (SHG) vom 16. März 2015 (SRL Nr. 892) ist der Verweis auf § 7 KDSG zu streichen, da dessen Wortlaut geändert wird (vgl. Kap. 6.1).

6.2.18 Kantonales Landwirtschaftsgesetz

§ 6

In dieser Bestimmung des Kantonalen Landwirtschaftsgesetz vom 12. September 1995 (KLwG; SRL Nr. 902) ist der geänderte Erlassstitel des KDSG zu berücksichtigen (Abs. 3). Soweit Betriebsdaten Personendaten umfassen, gelten die Datenschutzvorschriften.

6.3 Inkrafttreten

Nach dem Beschluss Ihres Rates kann die Gesetzesänderung frühestens auf den 1. September 2021 in Kraft treten. Die Gesetzesanpassung ist auf Dauer ausgelegt. Eine Befristung der Änderung wäre zudem auch aufgrund des übergeordneten Rechts und wegen der zahlreichen organisatorischen Bestimmungen nicht sinnvoll.

7 Auswirkungen

Das kantonale Datenschutzgesetz enthält die Grundsätze zur Bearbeitung von Personendaten durch die Verwaltung, regelt die Kontrollrechte der davon betroffenen Personen und legt die Aufsicht über die Datenbearbeitungstätigkeit fest. Die Gesetzesänderungen umfassen alle diese Teile: Legaldefinitionen (Begriff der Personendaten und insbesondere der besonders schützenswerten Personendaten, Profiling), Informations- und Meldepflichten der öffentlichen Organe und Datenschutz-Folgenabschätzung, die Einführung der Funktion des Datenschutzberaters sowie die Tätigkeit und Organisation der Aufsichtsstelle. Die Wahlzuständigkeit des Kantonsrates, die festgelegten Wählbarkeitsvoraussetzungen und Unvereinbarkeitsbestimmungen sowie die im Gesetz vorgesehenen Kompetenzen des oder der Beauftragten für den Datenschutz (Möglichkeit zum Erlass von Verfügungen bei Verletzung von Datenschutzvorschriften, Finanz- und Personalkompetenzen) sollen die Unabhängigkeit der Aufsichtsstelle stärken. Hauptsächlich handelt es sich bei diesen Änderungen um rechtstechnische Anpassungen in dem Sinn, als mit der Teilrevision des kantonalen Datenschutzgesetzes die Entwicklungen des übergeordneten Völker- und Europarechts sowie die Totalrevision des eidgenössischen Datenschutzgesetzes aufgenommen wird. Die Notwendigkeit zur Abstimmung ergibt sich aus der bundes-

staatlichen Ordnung, welche den Kantonen Kompetenzen, aber auch die Verantwortung zur Regelung des Datenschutzes belässt. Da aufgrund der Bestrebungen um Rechtsvereinheitlichung zahlreiche terminologische Anpassungen und Regelungen mit höherem Detaillierungsgrad nötig sind, erscheinen die Anpassungen im kantonalen Recht bei äusserlicher Betrachtung recht umfangreich. Mit der formalen Verankerung von datenschutzrechtlichen Instrumenten wie der Datenschutz-Folgenabschätzung halten sich die Auswirkungen der Gesetzesrevision für die kantonale Verwaltung in Grenzen, sind diese Instrumente doch schon bekannt. Auch ist davon auszugehen, dass nach einer Umstellungsphase bei vollzugsfreundlicher Handhabung der Gesetzesänderungen in den meisten Dienststellen keine Kostenfolgen entstehen. In der Informatik kann die hinreichende Ermittlung und Eindämmung der Datenschutzrisiken die Projektarbeit erleichtern. Für die Aufsichtsstelle geht der Beauftragte für den Datenschutz hingegen davon aus, dass insbesondere die Handhabung der Meldungen und der Mitteilungspflichten bei unbefugten Datenbearbeitungen, die von der Aufsichtsstelle innert angemessener Frist vorzunehmenden Vorabkontrollen, die Wahrnehmung der Verfügungskompetenz (z.B. hinsichtlich der Entscheidungsvorbereitung, der Wahrung der Formvorschriften beim rechtlichem Gehör usw.) bei der Aufsichtsstelle Mehrbelastungen verursachen, die nicht im Voraus beziffert werden können, wie auch die Praxis der Gemeinden nur schwer einschätzbar sei.

In unserem Entwurf nehmen wir daher zur Entlastung auch Handlungsspielräume wahr, wo es das übergeordnete Recht zulässt. Im Sinne eines guten Umgangs zwischen den Behörden, insbesondere auch der Gemeindebehörden, und nicht zuletzt einer effizienten Umsetzung des Datenschutzes sieht unser Entwurf vor, dass weiterhin das «weichere» Instrument der Empfehlungen im Vordergrund stehen soll, wenn es die Verwaltungstätigkeit auf die Belange des Datenschutzes abzustimmen gilt, bevor zum Instrument der Verfügung gegriffen werden soll. Bei der Funktion des Datenschutzberaters gehen wir davon aus, dass je ein Datenschutzberater oder eine Datenschutzberaterin innerhalb des Gerichtswesens, innerhalb der Staatsanwaltschaft, innerhalb der Dienststelle Militär, Zivilschutz und Strafvollzug sowie der Luzerner Polizei den Anforderungen und Bedürfnissen genügt. Diese Verwaltungseinheiten sollen in bestimmten Umfang ein internes Fachwissen aufbauen, wodurch ihnen Aufwendungen in geringem Umfang entstehen. Dabei handelt es sich nicht um neue Stellen, sondern um eine Zusatzaufgabe für bewährte Mitarbeiterinnen und Mitarbeiter. Damit stehen aber dem oder der Beauftragten für den Datenschutz Ansprechpersonen in den Dienststellen und im Gerichtswesen zur Verfügung und können zu seiner beziehungsweise ihrer Entlastung beitragen. Durch den Verzicht auf das Register über Datensammlungen wird die Einsparung für den Betrieb der Datenbank und des Webhostings abgesichert.

Wir wollen mit diesen Lösungen das kantonale Datenschutzgesetz den Entwicklungen im Europa- und im Völkerrecht, die eine Rechtsvereinheitlichung anstreben und die Stellung des Datenschutzes stärken, Rechnung tragen und ein angemessenes Datenschutzniveau im Sinn der europaweiten Anforderungen gewährleisten, aber gleichzeitig auch den Bedürfnissen im spezifischen, im Vergleich zum restlichen Europa kleinräumigen kantonalen Umfeld genügen. 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, welche Vorgaben und Praktiken sich aus dem internationalen und eidgenös-

sischen Datenschutzrecht insbesondere bei der Handhabung des datenschutzrechtlichen Instrumentariums ergeben und in welchem Umfang – auch auf kantonaler Ebene – staatliche Verwaltungen weiter digitalisiert werden.

8 Antrag

Sehr geehrte Frau Präsidentin, sehr geehrte Damen und Herren, wir beantragen Ihnen, dem Entwurf zur Aktualisierung des kantonalen Datenschutzrechtes zuzustimmen.

Luzern, 17. November 2020

Im Namen des Regierungsrates
Der Präsident: Reto Wyss
Der Staatsschreiber: Vincenz Blaser

Entwurf RR vom 17. November 2020

Gesetz über den Schutz von Personendaten (Datenschutzgesetz, DSG)

Änderung vom

Betroffene SRL-Nummern:

Neu: –

Geändert: 5 | 20 | 25 | 26 | 28a | 29 | 38 | 39 | 40 | 51 | 305 | 350 | 585 |
620 | 800 | 800a | 865 | 892 | 902

Aufgehoben: –

Der Kantonsrat des Kantons Luzern,

gestützt auf die Botschaft des Regierungsrates vom 17. November 2020,

beschliesst:

I.

Gesetz über den Schutz von Personendaten (Datenschutzgesetz, DSG) vom 2. Juli 1990¹ (Stand 1. Januar 2012) wird wie folgt geändert:

Titel (*geändert*)

Kantonales Gesetz

über den Schutz von Personendaten (Kantonales Datenschutzgesetz, KDSG)

§ 2 Abs. 1 (*geändert*), **Abs. 2** (*geändert*), **Abs. 3** (*geändert*), **Abs. 4** (*geändert*), **Abs. 4^{bis}** (*neu*), **Abs. 6** (*aufgehoben*), **Abs. 7** (*geändert*)

¹ Personendaten sind Angaben über eine bestimmte oder bestimmbare natürliche Person.

² Besonders schützenswerte Personendaten sind Angaben über natürliche Personen, bei welchen eine besondere Gefahr für Persönlichkeits- und Grundrechtsverletzungen besteht, insbesondere

- a. (*neu*) Daten über die religiöse, weltanschauliche oder politische Haltung,
- b. (*neu*) Daten über die Gesundheit, die Intimsphäre, das Erbgut oder die ethnische Zugehörigkeit,
- c. (*neu*) mit speziellen technischen Verfahren gewonnene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten),
- d. (*neu*) Daten über verwaltungs- und strafrechtliche Massnahmen und Sanktionen sowie die Massnahmen der Sozialhilfe,
- e. (*neu*) Zusammenstellungen von Daten, die eine Beurteilung wesentlicher Aspekte der natürlichen Person erlaubt (Persönlichkeitsprofil).

³ Betroffene Person ist die Person, von der Personendaten bearbeitet werden.

⁴ Bearbeiten von Personendaten ist, unabhängig von den angewendeten Mitteln und Verfahren, jeder Umgang mit Daten, wie das Erheben, Beschaffen, Aufbewahren, Aufzeichnen, Sammeln, Speichern auf elektronischen Datenträgern, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen und Vernichten. Bekanntgeben ist das Übermitteln oder das Zugänglichmachen von Personendaten, insbesondere durch Einsichtgewähren, Weitergeben oder Veröffentlichung.

¹ SRL Nr. [38](#)

^{4bis} Profiling ist jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um die Arbeitsleistung, die wirtschaftlicher Lage, die Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

⁶ aufgehoben

⁷ Verantwortliches Organ ist das Organ, das, allein oder zusammen mit anderen Organen, über den Zweck und die Mittel der Bearbeitung von Personendaten entscheidet.

§ 3 Abs. 1, Abs. 2 (geändert), Abs. 3 (neu), Abs. 4 (neu), Abs. 5 (neu), Abs. 6 (neu)

¹ Das Gesetz gilt für

- c. (geändert) andere Gemeinwesen gemäss § 1 des Gesetzes über die Verwaltungspflege vom 3. Juli 1972²,
- d. (neu) die übrigen Personen und Organisationen des öffentlichen und des privaten Rechts, denen kantonale Aufgaben übertragen sind.

² Der Teil 3 dieses Gesetzes gilt nicht für Notizen und Agenden, die als Hilfsmittel bei der Aufgabenerfüllung dienen.

- a. aufgehoben
- b. aufgehoben
- c. aufgehoben
- d. aufgehoben

³ Die Prozess- und Verfahrensordnungen regeln das Bearbeiten von Personendaten und die Rechte der betroffenen Personen in Gerichts- und Verwaltungsverfahren. Auf erstinstanzliche Verwaltungsverfahren sind die Bestimmungen dieses Gesetzes anwendbar.

⁴ Soweit Organe parlamentarische oder gerichtliche Befugnisse ausüben, unterliegen sie der Überwachung durch die zuständige Aufsichtsstelle gemäss § 22 nicht.

⁵ Soweit ein Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt, sind auf seine Datenbearbeitungen die Bestimmungen des Bundesgesetzes über den Datenschutz vom 25. September 2020³ anwendbar. Die Aufsicht richtet sich nach den Bestimmungen des Teils 4 dieses Gesetzes.

⁶ Vorbehalten bleiben besondere Vorschriften, die das Bearbeiten von Daten und insbesondere die Rechte der betroffenen Personen regeln.

Titel nach § 3 (neu)

1a Bearbeiten von Personendaten

§ 5 Abs. 1 (geändert), Abs. 2 (geändert)

¹ Organe dürfen Personendaten bearbeiten, wenn

- a. (neu) dafür eine Rechtsgrundlage besteht oder
- b. (neu) dies zur Erfüllung von Aufgaben erforderlich ist, für die eine Rechtsgrundlage besteht.

² Sie dürfen besonders schützenswerte Personendaten bearbeiten oder ein Profiling vornehmen, wenn es

Aufzählung unverändert.

§ 5a Abs. 2 (geändert)

² In Einzelfällen können Daten entweder bei der zugriffsberechtigten Person oder über ein automatisiertes Abrufverfahren beschafft werden, sofern der Zugriff protokolliert und vom verantwortlichen Organ sowie von dem oder der Beauftragten für den Datenschutz überprüft werden kann.

² SRL Nr. 40

³ SR ...

§ 6 Abs. 1^{bis} (neu), Abs. 2 (geändert), Abs. 3 (geändert), Abs. 4 (neu)

^{1bis} Das verantwortliche Organ stellt mit technischen und organisatorischen Massnahmen die Einhaltung des Datenschutzes sicher. Die Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Rechte der betroffenen Personen mit sich bringt, angemessen sein.

² Es kann das Bearbeiten von Personendaten einem anderen Organ oder Dritten übertragen, wenn

- a. (neu) keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht,
- b. (neu) sichergestellt ist, dass die Personendaten nur so bearbeitet werden, wie es das verantwortliche Organ selbst tun dürfte; insbesondere darf das Bearbeiten von Personendaten nicht ohne vorgängige schriftliche Zustimmung des verantwortlichen Organs weiteren Auftragsdatenbearbeitern übertragen werden.

³ Bearbeiten mehrere Organe Personendaten aus einem Datenbestand oder mehreren Datenbeständen, regeln sie die Verantwortlichkeit.

⁴ Der Regierungsrat regelt das Nähere durch Verordnung.

§ 7 Abs. 1 (geändert), Abs. 1^{bis} (neu)

Melde- und Informationspflichten bei unbefugter Datenbearbeitung (*Überschrift geändert*)

¹ Die verantwortlichen Organe melden dem oder der Beauftragten für den Datenschutz unverzüglich unbefugte Datenbearbeitungen, insbesondere durch Verlust, Fälschung, Entwendung und Kenntnisnahme durch nicht berechtigte Dritte, wenn diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führen.

^{1bis} Sie informieren die betroffenen Personen, wenn es zu deren Schutz erforderlich ist oder der oder die Beauftragte für den Datenschutz es verlangt, und soweit erforderlich andere Organe und Dritte. Die Information kann eingeschränkt oder aufgeschoben oder es kann darauf verzichtet werden, wenn überwiegende öffentliche Interessen dies erfordern oder wenn die Information einen unverhältnismässigen Aufwand verursacht.

§ 7a (neu)

Datenschutz-Folgenabschätzung und Vorabkonsultation

¹ Das verantwortliche Organ prüft bei Vorhaben zur Datenbearbeitung die Auswirkungen auf den Datenschutz. Besteht voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen, führt das Organ eine Datenschutz-Folgenabschätzung durch.

² Ergibt sich aus den Abklärungen, dass die vorgesehene Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der Betroffenen zur Folge hätte, obwohl Massnahmen vorgesehen sind, holt das Organ die Stellungnahme des oder der Beauftragten für den Datenschutz ein. Dieser gibt innert angemessener Frist eine Empfehlung ab und schlägt geeignete Massnahmen vor.

³ Der Regierungsrat regelt das Nähere durch Verordnung.

§ 7b (neu)

Datenschutzberater oder -beraterin

¹ Die vom Regierungsrat durch Verordnung bestimmten weiteren Organe und das Kantonsgericht bezeichnen einen Datenschutzberater oder eine Datenschutzberaterin.

² Der Datenschutzberater oder die Datenschutzberaterin

- a. unterstützt die Mitarbeiterinnen und Mitarbeiter der Organisationseinheiten, die Personendaten bearbeiten, bei der Einhaltung der Vorschriften über den Datenschutz,
- b. sorgt für die notwendigen Datenschutz-Folgenabschätzungen gemäss § 7a,
- c. ist Ansprechperson des oder der Beauftragten für den Datenschutz.

³ Der Regierungsrat kann die übrigen Gemeinwesen verpflichten, einen Datenschutzberater oder eine Datenschutzberaterin zu bezeichnen.

§ 8 Abs. 3 (geändert), Abs. 4 (geändert), Abs. 5 (neu)

³ Das Organ weist die Person auf das Bestehen einer Auskunftspflicht und gegebenenfalls auf die Folgen einer Verletzung der Auskunftspflicht hin.

⁴ Es informiert die Person über

- a. *(geändert)* das für die Erhebung verantwortliche Organ und gibt dessen Kontaktdaten bekannt,
- b. *(geändert)* die Rechtsgrundlage und den Zweck der Datenerhebung,
- c. *(neu)* die bearbeiteten Personendaten oder die Kategorien der bearbeiteten Daten,
- d. *(neu)* die Dauer der Aufbewahrung der Personendaten oder die Kriterien für die Festlegung der Aufbewahrungsdauer,
- e. *(neu)* die Empfänger der Personendaten oder die Kategorien der Empfänger, falls die Daten Dritten bekannt gegeben werden sollen,
- f. *(neu)* die Rechte der betroffenen Person.

⁵ Auf die Information kann verzichtet werden, wenn

- a. die Datenbearbeitung im Gesetz vorgesehen ist oder
- b. die betroffene Person bereits über die Angaben gemäss Absatz 4 verfügt oder
- c. die Information der betroffenen Person nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

§ 12a Abs. 3 (geändert), Abs. 4 (neu)

³ Der oder die Beauftragte für den Datenschutz muss über die Garantien nach Absatz 2a informiert werden.

⁴ Der Regierungsrat kann weitere Vorschriften erlassen.

§ 13 Abs. 1 (geändert), Abs. 2 (aufgehoben), Abs. 3 (geändert)

(Überschrift geändert)

¹ Benötigt ein Organ Datenbestände voraussichtlich nicht mehr, werden sie nach den dafür geltenden Vorschriften archiviert oder vernichtet.

² *aufgehoben*

³ Der Regierungsrat kann weitere Vorschriften erlassen. Insbesondere kann er Löschfristen und Massnahmen zur regelmässigen Überprüfung der Notwendigkeit von Personendatenbeständen festlegen.

§ 14 Abs. 1 (geändert), Abs. 2 (geändert), Abs. 3 (geändert)

Verzeichnis der Datenbearbeitungstätigkeiten *(Überschrift geändert)*

¹ Die von der obersten Verwaltungsbehörde des Gemeinwesens bezeichneten Organe führen ein Verzeichnis über die Datenbearbeitungstätigkeiten in ihrem Zuständigkeitsbereich.

² Das Verzeichnis ist öffentlich. Es nennt mindestens

- a. *(geändert)* die Kontaktdaten,
- b. *(geändert)* den Zweck der Datenbearbeitung,
- c. *(neu)* die Kategorien der betroffenen Personen und der bearbeiteten Personendaten,
- d. *(neu)* die Kategorien der Empfängerinnen und Empfänger.

³ Der Regierungsrat regelt das Nähere durch Verordnung.

§ 15 Abs. 1 (geändert), Abs. 2 (geändert), Abs. 3 (geändert)

¹ Jede Person kann beim verantwortlichen Organ mündlich oder schriftlich Auskunft verlangen, ob Personendaten über sie vorhanden sind. Sie hat sich über ihre Identität auszuweisen.

- a. *aufgehoben*
- b. *aufgehoben*

² Das Organ muss der betroffenen Person mindestens Auskunft geben über

- a. *(neu)* die über sie vorhandenen Personendaten,
- b. *(neu)* die Rechtsgrundlage und den Zweck der Datenbearbeitung,
- c. *(neu)* soweit möglich die Herkunft der Personendaten und allfällige Empfänger bei Weitergabe,
- d. *(neu)* die Aufbewahrungsdauer der Personendaten oder die Kriterien für die Festlegung der Aufbewahrungsdauer,

e. *(neu)* ihre Rechte, insbesondere auf Berichtigung unrichtiger Personendaten.

³ Die Auskunft wird in allgemein verständlicher Form auf Verlangen mündlich oder schriftlich erteilt. Soweit die Mittel und Verfahren des Bearbeitens es zulassen, ist Einsicht in die Personendaten zu gewähren.

§ 17 Abs. 1 (geändert), Abs. 2 (geändert)

¹ Jede Person kann vom verantwortlichen Organ verlangen, dass unrichtige Personendaten über sie berichtigt werden.

² Bestreitet das Organ die Unrichtigkeit, hat es die Richtigkeit der Personendaten zu beweisen. Die betroffene Person hat im Rahmen des Zumutbaren bei der Abklärung mitzuwirken.

§ 18 Abs. 1 (geändert), Abs. 2

¹ Jede Person kann vom verantwortlichen Organ verlangen, dass

b. *(geändert)* unbefugt bearbeitete Personendaten gelöscht oder vernichtet oder die Folgen sonst wie beseitigt werden.

² Weist die betroffene Person ein schutzwürdiges Interesse nach,

c. *(geändert)* kann sie vom verantwortlichen Organ verlangen, dass es die Bearbeitung von bestimmten Personendaten einschränkt und insbesondere die Bekanntgabe von bestimmten Personendaten sperrt.

§ 19 Abs. 2 (aufgehoben)

Entscheid und Mitteilung (*Überschrift geändert*)

² *aufgehoben*

Titel nach § 20 (geändert)

4 Aufsicht

§ 21

aufgehoben

§ 22 Abs. 1 (geändert), Abs. 1^{bis} (neu), Abs. 1^{er} (neu), Abs. 2 (geändert), Abs. 3 (aufgehoben)

Aufsichtsstelle (*Überschrift geändert*)

¹ Der Kantonsrat wählt auf Antrag des Regierungsrates einen Beauftragten oder eine Beauftragte für den Datenschutz auf eine Amtsdauer von vier Jahren. Wiederwahl ist möglich.

^{1bis} Bei der erstmaligen Wahl des oder der Beauftragten legt der Regierungsrat jeweils den Besoldungsrahmen und die Besoldungsentwicklung fest.

^{1er} Der Regierungsrat kann das Arbeitsverhältnis aus wichtigen Gründen vor Ablauf der Amtsdauer auflösen. Die Auflösung aus wichtigen Gründen bedarf der Genehmigung durch die Geschäftsleitung des Kantonsrates.

² Der oder die Beauftragte ist fachlich selbständig und unabhängig; administrativ ist er oder sie der Staatskanzlei zugeordnet.

³ *aufgehoben*

§ 22a (neu)

Wählbarkeit, Unvereinbarkeiten

¹ Wählbar als Beauftragter oder Beauftragte für den Datenschutz ist eine in Datenschutzfragen ausgewiesene Fachperson.

² Er oder sie darf kein anderes öffentliches Amt ausüben.

³ Das zuständige Organ des Gemeinwesens kann eine Nebenbeschäftigung bewilligen, soweit diese die Ausübung des Amtes, insbesondere die Unabhängigkeit des Amtsinhabers oder der Amtsinhaberin, nicht beeinträchtigt.

§ 22b (neu)

Finanz- und Personalkompetenzen

¹ Der oder die Beauftragte für den Datenschutz verfügt über die im Voranschlag bewilligten Kredite in eigener Kompetenz.

² Er oder sie ist für alle personalrechtlichen Entscheide betreffend seine oder ihre Mitarbeiterinnen und Mitarbeiter zuständig, insbesondere für die Begründung, die Umgestaltung und die Beendigung von Arbeitsverhältnissen. Im Übrigen finden die Bestimmungen des Personalgesetzes vom 26. Juni 2001⁴ Anwendung.

§ 23 Abs. 1 (geändert), Abs. 2 (aufgehoben), Abs. 3 (neu)

¹ Der oder die Beauftragte für den Datenschutz

- b. (geändert) verfolgt die massgeblichen Entwicklungen und berät die verantwortlichen Organe in Fragen des Datenschutzes,
- c. (geändert) erteilt den betroffenen Personen Auskunft über ihre Rechte und behandelt aufsichtsrechtliche Anzeigen innert angemessener Frist,
- c^{bis}. (neu) gibt gegenüber den Organen Empfehlungen zu Datenbearbeitungen ab,
- d. aufgehoben
- e. (geändert) reicht in hängigen Verfahren auf Ersuchen von entscheidenden Organen oder Rechtsmittelbehörden und in Vernehmlassungsverfahren zu Entwürfen von rechtsetzenden Erlassen Stellungnahmen zu Datenschutzfragen ein,
- f. (geändert) orientiert die Organe und die Öffentlichkeit über wesentliche Anliegen des Datenschutzes,
- h. (geändert) nimmt zu Datenbearbeitungen Stellung, die ein hohes Risiko für Verletzungen von Persönlichkeits- und Grundrechten der betroffenen Personen bergen,
- k. aufgehoben

² aufgehoben

³ Der oder die Beauftragte erstattet dem Regierungsrat jährlich Bericht über die Schwerpunkte der Tätigkeit der Aufsichtsstelle. Er oder sie stellt den Tätigkeitsbericht der Aufsichts- und Kontrollkommission sowie der Planungs- und Finanzkommission des Kantonsrates zu und veröffentlicht ihn im Internet. Regierungsrat und Kantonsrat nehmen vom Bericht Kenntnis.

§ 24 Abs. 1 (geändert), Abs. 2 (geändert), Abs. 3 (geändert), Abs. 4 (geändert), Abs. 5 (geändert)

¹ Die verantwortlichen Organe sind verpflichtet, den Beauftragten oder die Beauftragte für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen.

² Der oder die Beauftragte kann ungeachtet allfälliger Geheimhaltungsvorschriften bei Organen schriftlich und mündlich Auskünfte über das Bearbeiten von Personendaten einholen, Einsicht in alle Daten und weitere Unterlagen nehmen und sich das Bearbeiten von Personendaten vorführen lassen.

³ Ergibt die Abklärung, dass Datenschutzvorschriften verletzt werden, kann der oder die Beauftragte eine Empfehlung abgeben. Das Organ hat zu erklären, ob es der Empfehlung Folge leisten wird.

⁴ Leistet das Organ der Empfehlung nicht Folge, kann der oder die Beauftragte entsprechende Massnahmen verfügen. Vorsorgliche Verfügungen bleiben vorbehalten.

⁵ Der oder die Beauftragte darf unter Vorbehalt besonderer Geheimhaltungsvorschriften Kenntnisse, die er oder sie bei seiner Tätigkeit erlangt, nur so weit bekanntgeben, als es zur Erfüllung seiner Aufgabe notwendig ist. Die Geheimhaltungspflicht besteht nach Beendigung des Dienstverhältnisses weiter.

Titel nach § 24 (neu)

4a Strafbestimmung und Rechtsschutz

⁴ SRL Nr. 51

§ 24b (neu)

Rechtsschutz

¹ Die Anfechtung von Entscheiden, die in Anwendung dieses Gesetzes erlassen werden, richtet sich, unter Einschluss der Kosten des Verfahrens, nach dem Gesetz über die Verwaltungsrechtspflege⁵.

² Entscheide des oder der Beauftragten für den Datenschutz sind mit Verwaltungsgerichtsbeschwerde beim Kantonsgericht anfechtbar. Zur Beschwerde befugt sind die betroffenen Organe. Dem Kantonsgericht steht auch die Ermessenskontrolle zu.

§ 26

aufgehoben

§ 26a (neu)

Übergangsbestimmung zur Änderung vom ...

¹ Die erstmalige Wahl des oder der Beauftragten für den Datenschutz auf Amtsdauer gemäss § 22 Absatz 1 findet auf den 1. Januar 2022 für den Rest der Amtsdauer 2019–2023 statt. Der bisherige Mandatsträger übt das Amt bis 31. Dezember 2021 aus und kann wiedergewählt werden.

II.

1.

Gesetz über die Niederlassung und den Aufenthalt (NG) vom 1. Dezember 1948⁶ (Stand 1. Januar 2010) wird wie folgt geändert:

§ 12 Abs. 2 (geändert)

² Das Recht, Auskunft über die Personendaten der Einwohnerkontrolle zu verlangen und in sie Einsicht zu nehmen, richtet sich nach dem Kantonalen Datenschutzgesetz vom 2. Juli 1990⁷.

2.

Gesetz über die Organisation von Regierung und Verwaltung (Organisationsgesetz, OG) vom 13. März 1995⁸ (Stand 1. Februar 2018) wird wie folgt geändert:

§ 21b (neu)

Informations-, Geschäftsverwaltungs- und Dokumentationssysteme, Datenbearbeitung

¹ Die Verwaltung führt zur Erfüllung ihrer gesetzlichen Aufgaben elektronische Informations-, Geschäftsverwaltungs- und Dokumentationssysteme.

² Sie bearbeitet Personendaten und Angaben über juristische Personen und Personengesellschaften des Handelsrechts sowie Sachdaten im Rahmen ihrer Aufgabenerfüllung. Vorbehalten bleiben die Bestimmungen der Datenschutz-, der Informatik- und der Archivgesetzgebung.

³ Der Regierungsrat kann weitere Vorschriften erlassen.

3.

Gesetz über die Harmonisierung amtlicher Register (Registergesetz) vom 25. Mai 2009⁹ (Stand 1. Januar 2013) wird wie folgt geändert:

⁵ SRL Nr. [40](#)

⁶ SRL Nr. [5](#)

⁷ SRL Nr. [38](#)

⁸ SRL Nr. [20](#)

⁹ SRL Nr. [25](#)

§ 18 Abs. 1 (geändert)

¹ Das Recht, Auskunft über die Personendaten der Register gemäss den §§ 8–11 zu verlangen und in sie Einsicht zu nehmen, richtet sich nach dem Kantonalen Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 2. Juli 1990¹⁰.

§ 19 Abs. 1 (geändert)

¹ Sperrvermerke im Einwohnerregister der Gemeinde gemäss § 11 Absatz 4 des Kantonalen Datenschutzgesetzes werden auch in die kantonale Einwohnerplattform übernommen.

4.

Informatikgesetz vom 7. März 2005¹¹ (Stand 1. August 2013) wird wie folgt geändert:

§ 3 Abs. 1 (geändert), **Abs. 4** (geändert)

¹ Die Begriffe «Personendaten», «besonders schützenswerte Personendaten», «betroffene Person», «Bearbeiten von Personendaten», «Profiling», «verantwortliches Organ» sowie «Organ» richten sich nach dem Kantonalen Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 2. Juli 1990¹². Sie umfassen in diesem Gesetz in der Regel auch Angaben über bestimmte oder bestimmbar juristische Personen oder Personengesellschaften des Handelsrechts.

⁴ Zentrale Datenbanken bestehen aus zusammengeführten Datenbeständen verschiedener Organe. Sie können sich an einem beliebigen Ort befinden. Datenwarenhäuser und Datendreh scheiben sind zentrale Datenbanken.

§ 4 Abs. 3 (geändert)

³ Techniken, die geeignet sind, aus Daten oder Personendaten besonders schützenswerte Personendaten herzustellen oder damit ein Profiling vorzunehmen, dürfen nur dann eingesetzt werden, wenn die Voraussetzungen gemäss § 5 Absatz 2 des Kantonalen Datenschutzgesetzes erfüllt sind.

§ 5 Abs. 3 (geändert)

³ Der Regierungsrat kann, nachdem er die Stellungnahme des oder der Beauftragten für den Datenschutz eingeholt hat, vor Inkrafttreten eines formellen Gesetzes eine zentrale Datenbank mit besonders schützenswerten Personendaten oder Resultaten von Profilings während einer einmaligen befristeten Zeitspanne von höchstens fünf Jahren bewilligen, wenn

Aufzählung unverändert.

§ 6 Abs. 5 (geändert)

⁵ § 6 Absatz 3 des Kantonalen Datenschutzgesetzes ist auf zentrale Datenbanken nicht anwendbar.

§ 7 Abs. 1 (geändert), **Abs. 2** (geändert)

¹ Der Umfang der Zugriffs- und Bearbeitungsberechtigung von Organen auf Personendaten einer zentralen Datenbank bestimmt sich nach Massgabe des Kantonalen Datenschutzgesetzes und ist technisch und organisatorisch auf geeignete Weise sicherzustellen. § 6 Absatz 3 bleibt vorbehalten.

² Werden die in einem Datenwarenhäuser gespeicherten Personendaten von keinem beteiligten Organ mehr benötigt, sind sie dem zuständigen Archiv zur Übernahme anzubieten. Werden sie vom Archiv als nicht archivwürdig eingestuft, sind sie umgehend zu löschen oder zu vernichten.

¹⁰ SRL Nr. 38. Auf dieses Gesetz wird im Folgenden nicht mehr hingewiesen.

¹¹ SRL Nr. 26

¹² SRL Nr. 38. Auf dieses Gesetz wird im Folgenden nicht mehr hingewiesen.

§ 10 Abs. 1 (geändert), Abs. 2 (geändert), Abs. 3 (geändert)

Publikation (*Überschrift geändert*)

¹ Die Errichtung von Datenwarenhäusern ist vom Betreiber vor der Betriebsaufnahme im Kantonsblatt zu publizieren. In der Publikation sind für jedes Datenwarenhaus die daran beteiligten Organe und die entsprechenden Datenbestände sowie der Betreiber aufzuführen. Ferner hat die Publikation für jeden Datenbestand Auskunft zu geben über die Rechtsgrundlage, den Zweck, die Mittel und Verfahren des Bearbeitens, die Art und Herkunft der Personendaten und deren regelmässige Empfänger sowie über das Vorhandensein und den Aufbewahrungsort von Kopien.

² In der Publikation sind ferner die Kontrollrechte jeder Person sowie die zuständigen Aufsichtsstellen für den Datenschutz gemäss diesem Gesetz und dem Kantonalen Datenschutzgesetz anzugeben.

³ Die Angaben gemäss Absatz 1 sind in das Verzeichnis der Datenbearbeitungstätigkeiten aufzunehmen.

§ 11 Abs. 1, Abs. 4 (geändert)

¹ Jede Person kann bei der zuständigen Aufsichtsstelle für den Datenschutz Auskunft verlangen

a. (*geändert*) über den Inhalt des Verzeichnisses der Datenbearbeitungstätigkeiten,

⁴ Das Verfahren betreffend Auskunft über die über eine betroffene Person vorhandenen Personendaten sowie betreffend Einsicht, Berichtigung und andere Ansprüche richtet sich nach dem Kantonalen Datenschutzgesetz. Auf Begehren der betroffenen Person leitet die zuständige Aufsichtsstelle für den Datenschutz bei den Organen, welche berechtigt sind, auf ihre Personendaten zuzugreifen oder sie zu bearbeiten, das Verfahren ein.

§ 15 Abs. 2 (geändert)

² Er hat dem auslagernden Organ, der zuständigen Aufsichtsstelle für den Datenschutz sowie der Finanzkontrolle Zutritt zu den Räumen und Anlagen sowie die erforderlichen Zugriffsrechte auf die entsprechenden Daten zu gewähren und sie angemessen zu unterstützen.

§ 16 Abs. 1 (geändert)

¹ Als Inhaber der Datensammlung gilt das verantwortliche Organ.

§ 18 Abs. 1 (geändert), Abs. 2 (geändert)

¹ Die Informatikmittel sind durch das verantwortliche Organ beziehungsweise den Betreiber einer zentralen Datenbank gegen Verlust und unerwünschte Einwirkungen zu sichern. Personendaten sind vor unbefugtem Zugriff und unbefugter Bearbeitung zu schützen.

² Die Organe der Informatik unterstützen die verantwortlichen Organe und die Betreiber von zentralen Datenbanken bei der Festlegung und der Umsetzung von Sicherheitsmassnahmen.

5.

Statistikgesetz vom 13. Februar 2006¹³ (Stand 1. August 2009) wird wie folgt geändert:

§ 3 Abs. 8 (geändert), Abs. 9 (geändert)

⁸ Die Definitionen von Personendaten und besonders schützenswerten Personendaten gemäss dem Kantonalen Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 2. Juli 1990¹⁴ gelten auch für dieses Gesetz. Sie umfassen in diesem Gesetz auch Angaben über bestimmte oder bestimmbare juristische Personen oder Personengesellschaften des Handelsrechts.

¹³ SRL Nr. 28a

¹⁴ SRL Nr. 38. Auf dieses Gesetz wird im Folgenden nicht mehr hingewiesen.

⁹ Personenbezogene Daten sind anonymisierte Individualdaten, bei welchen Rückschlüsse auf die natürliche oder juristische Person oder auf eine Personengesellschaft des Handelsrechts ohne grossen Aufwand möglich sind.

§ 16 Abs. 2 (*geändert*)

² Er kann dabei die Übernahme von Daten aus Datenbeständen anordnen, sofern deren Rechtsgrundlage die Verwendung für statistische Zwecke nicht ausdrücklich ausschliesst. Unterliegen diese Daten einer gesetzlich verankerten Geheimhaltungspflicht, dürfen sie nicht weitergegeben werden.

§ 22 Abs. 3 (*geändert*)

³ Personendaten dürfen unter Vorbehalt von § 10 Absatz 2 und § 23 Absatz 4 niemandem zugänglich gemacht werden.

6.

Gesetz über die Geoinformation und die amtliche Vermessung (Geoinformationsgesetz, GIG) vom 8. September 2003¹⁵ (Stand 1. Juni 2015) wird wie folgt geändert:

§ 3 Abs. 1

¹ Im Anwendungsbereich dieses Gesetzes gelten folgende Begriffsbestimmungen:

- h. (*geändert*) Verantwortliches Organ ist das Organ, das, allein oder zusammen mit anderen Organen, über den Zweck und die Mittel der Bearbeitung von Daten entscheidet.

§ 9 Abs. 1 (*geändert*)

¹ Werden Personendaten bearbeitet, gelten die Vorschriften des Bundes und des Kantons über den Datenschutz. Das verantwortliche Organ hat dafür Gewähr zu leisten, dass die datenschutzrechtlichen Bestimmungen eingehalten werden.

§ 20 Abs. 1 (*geändert*)

¹ Schutzrechte, die bei der Bearbeitung und Nachführung von GIS-Datenbanken entstehen, gehen an das Gemeinwesen über, zu dem das verantwortliche Organ gehört.

7.

Gesetz über die Videoüberwachung vom 20. Juni 2011¹⁶ (Stand 1. Februar 2018) wird wie folgt geändert:

§ 6 Abs. 1 (*geändert*)

¹ Soweit das Gesetz nichts anderes vorschreibt, kommen die Bestimmungen des Kantonalen Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 2. Juli 1990¹⁷ zur Anwendung.

8.

Gesetz über die Verwaltungsrechtspflege (VRG) vom 3. Juli 1972¹⁸ (Stand 1. Januar 2019) wird wie folgt geändert:

¹⁵ SRL Nr. [29](#)

¹⁶ SRL Nr. [39](#)

¹⁷ SRL Nr. [38](#)

¹⁸ SRL Nr. [40](#)

§ 141a (neu)

15. Veröffentlichung und Zugang zu Rechtsmittelentscheiden

¹ Bei der Veröffentlichung von Rechtsmittelentscheiden und der Gewährung des Zugangs zu Rechtsmittelentscheiden ist dem Persönlichkeits- und Datenschutz insbesondere durch Unkenntlichmachen der Namen der Parteien Rechnung zu tragen.

9.

Gesetz über das öffentlich-rechtliche Arbeitsverhältnis (Personalgesetz, PG) vom 26. Juni 2001¹⁹ (Stand 1. August 2020) wird wie folgt geändert:

§ 67 Abs. 3 (geändert)

³ Wurde die oder der Angestellte von einem gesetzgebenden Organ gewählt, ist die oberste Dienstaufsichtsbehörde für die übrigen personalrechtlichen Entscheide zuständig. Ist der Regierungsrat oberste Dienstaufsichtsbehörde, gilt Absatz 2. Für die der Staatskanzlei administrativ zugeordneten Funktionen ist der Staatsschreiber oder die Staatsschreiberin zuständig. Für die dem Kantonsgericht unterstellten Gerichte und Organisationseinheiten gilt die Verordnung des Kantonsgerichtes.

10.

Gesetz über den Justizvollzug (JVG) vom 14. September 2015²⁰ (Stand 1. Juli 2016) wird wie folgt geändert:

§ 22 Abs. 1 (geändert)

¹ Psychiaterinnen und Psychiater, Ärztinnen und Ärzte, Psychologinnen und Psychologen und andere Fachpersonen, die mit einer Begutachtung oder Behandlung betraut sind, dürfen in die Vollzugsakten, einschliesslich besonders schützenswerter Personendaten, Persönlichkeitsprofile und Ergebnisse von Profilings, Einsicht nehmen, soweit die Aktenkenntnis für ihre Aufgabenerfüllung erforderlich ist.

11.

Gesetz über die Luzerner Polizei (PolG) vom 27. Januar 1998²¹ (Stand 1. Januar 2020) wird wie folgt geändert:

§ 4 Abs. 1, Abs. 3 (geändert)

¹ Die Luzerner Polizei kann zur recht- und zweckmässigen Erfüllung ihrer Aufgaben

- b. (geändert) geeignete Datenbearbeitungssysteme führen,
- c. (geändert) besonders schützenswerte Personendaten bearbeiten, soweit dies zur Erfüllung ihrer Aufgaben unentbehrlich ist,
- d. (neu) Profilings vornehmen, insbesondere für kriminalpolizeiliche Zwecke.

³ Soweit dieses Gesetz nichts anderes regelt, gelten die Bestimmungen des Kantonalen Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 2. Juli 1990²².

§ 4^{bis} Abs. 1 (geändert)

¹ Die Luzerner Polizei kann anderen Behörden und Dritten Personendaten unter den Voraussetzungen des Kantonalen Datenschutzgesetzes bekannt geben.

¹⁹ SRL Nr. [51](#)

²⁰ SRL Nr. [305](#)

²¹ SRL Nr. [350](#)

²² SRL Nr. [38](#). Auf dieses Gesetz wird im Folgenden nicht mehr hingewiesen.

12.

Gesetz über das Archivwesen (Archivgesetz) vom 16. Juni 2003²³ (Stand 1. Juli 2019) wird wie folgt geändert:

§ 3 Abs. 5 (geändert)

⁵ Für die Begriffe «Personendaten», «besonders schützenswerte Personendaten» und «betroffene Person» gelten die Definitionen des Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 2. Juli 1990²⁴. Sie umfassen in diesem Gesetz auch Angaben über bestimmte oder bestimmbare juristische Personen oder Personengesellschaften des Handelsrechts.

§ 6 Abs. 2 (neu)

² Sie können dem Staatsarchiv die für die Vorbereitung der Übernahme erforderlichen Zugriffsrechte zu den elektronischen Informations-, Geschäftsverwaltungs- und Dokumentationssystemen einräumen. Die öffentlichen Organe sind für die Zugriffsverwaltung verantwortlich.

13.

Steuergesetz (StG) vom 22. November 1999²⁵ (Stand 1. Januar 2020) wird wie folgt geändert:

§ 137 Abs. 5 (geändert)

⁵ Die Daten dürfen den mit dem Vollzug dieses Gesetzes betrauten Behörden auch auf Listen oder elektronischen Datenträgern weitergegeben oder mittels eines Abrufverfahrens zugänglich gemacht werden. Die Daten und die zu deren Bearbeitung verwendeten Datenträger, EDV-Programme und Programmdokumentationen sind vor unbefugtem Bearbeiten, Verändern, Zerstören sowie vor Entwendung zu schützen.

14.

Gesundheitsgesetz (GesG) vom 13. September 2005²⁶ (Stand 1. Juni 2020) wird wie folgt geändert:

§ 53h Abs. 4 (geändert)

⁴ Die Bestimmungen des Kantonalen Datenschutzgesetzes vom 2. Juli 1990²⁷ sind einzuhalten.

15.

Spitalgesetz vom 11. September 2006²⁸ (Stand 1. Juni 2020) wird wie folgt geändert:

§ 6g Abs. 1 (geändert)

¹ Soweit dieses Gesetz keine besonderen Bestimmungen über den Datenschutz enthält, kommen bei der Bearbeitung von Personendaten die Bestimmungen des Kantonalen Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 2. Juli 1990²⁹ zur Anwendung.

²³ SRL Nr. [585](#)

²⁴ SRL Nr. [38](#). Auf dieses Gesetz wird im Folgenden nicht mehr hingewiesen.

²⁵ SRL Nr. [620](#)

²⁶ SRL Nr. [800](#)

²⁷ SRL Nr. [38](#)

²⁸ SRL Nr. [800a](#)

²⁹ SRL Nr. [38](#)

16.

Einführungsgesetz zum Bundesgesetz über die Krankenversicherung vom 23. März 1998³⁰ (Stand 1. Januar 2019) wird wie folgt geändert:

§ 5a Abs. 8 (geändert)

⁸ Im Übrigen gelten die §§ 15 und 17–20 des Kantonalen Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 2. Juli 1990³¹.

17.

Sozialhilfegesetz (SHG) vom 16. März 2015³² (Stand 1. März 2020) wird wie folgt geändert:

§ 52a Abs. 2 (geändert)

² Zugriff auf die Einwohnerplattform und die Steuerdatenbank erhalten nur diejenigen Einwohnergemeinden, welche die Beschränkung der Zugriffsrechte in technischer, organisatorischer, personeller und administrativer Hinsicht gemäss § 6 Absatz 1^{bis} des Kantonalen Datenschutzgesetzes vom 2. Juli 1990³³ gewährleisten.

18.

Kantonales Landwirtschaftsgesetz (KLwG) vom 12. September 1995³⁴ (Stand 1. Januar 2020) wird wie folgt geändert:

§ 6 Abs. 3 (geändert)

³ Die Betriebsdaten sind den vom Regierungsrat in der Verordnung angeführten Stellen und Organisationen vollständig oder in Teilen zugänglich. Vorbehalten bleiben die Bestimmungen des Kantonalen Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 2. Juli 1990³⁵.

III.

Keine Fremdaufhebungen.

IV.

Die Änderung tritt am ... in Kraft. Sie ist zu veröffentlichen.

Luzern,

Im Namen des Kantonsrates:

Die Präsidentin:

Der Staatsschreiber:

³⁰ SRL Nr. [865](#)

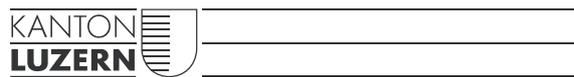
³¹ SRL Nr. [38](#)

³² SRL Nr. [892](#)

³³ SRL Nr. [38](#)

³⁴ SRL Nr. [902](#)

³⁵ SRL Nr. [38](#)



Staatskanzlei

Bahnhofstrasse 15
6002 Luzern

Telefon 041 228 50 33
staatskanzlei@lu.ch
www.lu.ch