

Bericht und Antrag des Regierungsrats an den Landrat

28. März 2023

Nr. 2023-185 R-362-11 Bericht und Antrag des Regierungsrats an den Landrat zur Totalrevision des Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz; KDSG)

I. Zusammenfassung

Verschiedene Neuerungen im internationalen Recht im Bereich Datenschutz sowie die immer weiter fortschreitende technische Entwicklung machen Anpassungen des Datenschutzrechts in der Schweiz notwendig. Während der Bund zuständig ist, den Datenschutz bei der Bearbeitung durch Private und durch die Bundesverwaltung zu regeln, ist der Kanton zuständig, die Regeln für die Datenbearbeitung durch die Behörden des Kantons und der Gemeinden zu regeln. Der Bund hat eine Totalrevision des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) bereits beschlossen. Mit dieser Vorlage soll auch das kantonale Gesetz über den Schutz von Personendaten (Datenschutzgesetz [KDSG]; RB 2.2511) einer Totalrevision unterzogen werden.

Das KDSG stärkt den Datenschutz insgesamt. Es regelt Bereiche, die bisher nicht oder nur rudimentär normiert waren, namentlich die in der digitalen Welt nicht mehr wegzudenkende Datenbearbeitung durch beauftragte Dritte (Auftragsdatenbearbeitung), aber z. B. auch die Datensicherheit. Datenschutz-Folgenabschätzungen sollen das Verantwortungsbewusstsein der Behörden im Umgang mit Datenschutz erhöhen. Die Transparenz der Datenbearbeitung sowie die Kontrollmöglichkeiten der betroffenen Person werden punktuell verbessert und nicht zuletzt werden die Stellung und die Befugnisse der oder des Datenschutzbeauftragten gestärkt.

Inhaltsübersicht

- I. Zusammenfassung
- II. Ausführlicher Bericht
 - 1. Ausgangslage
 - 2. Grundzüge der Vorlage
 - 3. Finanzielle und personelle Auswirkungen
 - 4. Vernehmlassung
 - 5. Bemerkungen zu den einzelnen Bestimmungen
- III. Antrag

II. Ausführlicher Bericht

1. Ausgangslage

1.1 International

Auf internationaler Ebene wurde in den letzten Jahren im Bereich Datenschutz verschiedentlich neues Recht geschaffen oder bestehendes revidiert und weiterentwickelt. 2016 ist etwa die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) in Kraft getreten. Diese ist für die Schweiz grundsätzlich nicht verbindlich. Allerdings gilt die DSGVO in manchen Fällen auch für Datenbearbeitungen ausserhalb der EU, z. B. wenn diese im Zusammenhang damit stehen, betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten. Somit sind Schweizer Gewerbetreibende, die ihr Angebot auch im EU-Raum anbieten, gehalten, die DSGVO zu befolgen. Umgekehrt können aber auch Personen in der Schweiz, deren Daten im EU-Raum bearbeitet werden (z. B. von einem in der EU niedergelassenen Versandhändler), sich auf die DSGVO berufen und die daraus fließenden Rechte geltend machen. Ausserdem ist die Schweiz insgesamt gefordert, ihr Datenschutzniveau der DSGVO anzupassen. Denn eine Übermittlung von personenbezogenen Daten aus einem EU-Mitgliedsstaat in die Schweiz ist nur noch möglich, wenn die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau eingestuft wird.

Gleichzeitig mit der DSGVO hat die EU die Richtlinie 2016/680 zum Datenschutz in der Strafverfolgung verabschiedet. Anders als die DSGVO ist die Richtlinie nicht direkt anwendbar, sondern muss von den EU-Mitgliedstaaten erst im nationalen Recht umgesetzt werden. Über das Schengener Assoziierungsabkommen¹ ist auch die Schweiz verpflichtet, diese Richtlinie umzusetzen.

2018 wurde die revidierte Datenschutzkonvention des Europarats Nr. 108 verabschiedet. Diese geht weniger weit als die Rechtsakte der EU, sondern definiert lediglich Mindeststandards. Die Schweiz hat das Abkommen ebenfalls unterzeichnet. Die Konvention ist jedoch nicht direkt anwendbar, sondern muss erst im nationalen Recht umgesetzt werden.

1.2 Schweiz

Um die zuvor genannten internationalen Verpflichtungen anzugehen, aber auch um die aufgrund der rasanten technologischen Entwicklungen mittlerweile aufgetretenen Schwächen des Datenschutzes zu beheben, hat der Bund beschlossen, das eidgenössische Datenschutzrecht einer Totalrevision zu unterziehen. Das Parlament hat die Vorlage des Bundesrats zur Totalrevision des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) in zwei Etappen aufgeteilt. In einer ersten Etappe wurde ausschliesslich die Schengen-relevante EU-Richtlinie 2016/680 zum Datenschutz in der Strafverfolgung umgesetzt. Dazu wurden 2019 übergangsweise ein neues Schengen-Datenschutzgesetz (SDSG; SR 235.3) in Kraft gesetzt und weitere Bundesgesetze angepasst.

In einer zweiten Etappe wurde die eigentliche Totalrevision des DSG beschlossen (BBl 2020 7639), die

¹ Abkommen 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)

unter anderem die Datenschutzkonvention Nr. 108 des Europarats umsetzt und das schweizerische Datenschutzrecht der DSGVO der EU annähert. Das neue DSG und die dazugehörige Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11) treten am 1. September 2023 in Kraft.

1.3 Kanton

Das Datenschutzrecht in der Schweiz ist föderalistisch aufgebaut. Während der Bund zuständig ist, den Datenschutz für private Datenbearbeitende und für die Bundesverwaltung zu regeln, ist es Sache der Kantone, die Datenschutzregeln für die Behörden der Kantone und der Gemeinden zu bestimmen.

Das kantonale Gesetz über den Schutz von Personendaten (Datenschutzgesetz [KDSG]; RB 2.2511) stammt aus dem Jahr 1994 und wurde letztmals auf den 1. Januar 2008 angepasst. Schon damals ging es hauptsächlich darum, den gestiegenen europäischen Anforderungen Rechnung zu tragen. Unabhängig von den beschriebenen Entwicklungen auf europäischer und eidgenössischer Ebene zeigen sich beim Vollzug des KDSG mittlerweile auch sonst einige Schwächen. Das Gesetz hat mit den technischen Entwicklungen im Bereich der Datenbearbeitung nicht mitgehalten und ist spürbar in die Jahre gekommen, sodass der Änderungsbedarf offenkundig ist. Auch wenn der Kanton völkerrechtlich nicht direkt verpflichtet ist, das erwähnte internationale Recht umzusetzen, trägt auch das kantonale Recht letztlich seinen Teil zum schweizerischen Datenschutzniveau bei. Somit sind auch bei der vorliegenden Revision die internationalen Standards selbstverständlich nicht ausser Acht zu lassen.

2. Grundzüge der Vorlage

Schon bisher hat sich das Urner Datenschutzrecht stark am eidgenössischen orientiert. Deshalb wird die Totalrevision des DSG zum Anlass genommen, auch das kantonale Gesetz komplett zu überarbeiten. Die Revision verfolgt dabei verschiedene Ziele: So sind vor allem die festgestellten Schwächen zu beseitigen und die Anforderungen des internationalen Rechts umzusetzen. Und auch wenn sich die Regeln für Privatpersonen und die Bundesverwaltung nicht unbesehen auf die kantonale und die kommunalen Verwaltungen übertragen lassen, soll sich das neue Recht soweit wie möglich und sinnvoll ans eidgenössische Recht anlehnen. Das vereinfacht den Vollzug, z. B. in der Zusammenarbeit über die Kantongrenzen hinweg.

Anfang 2017 hat die Konferenz der Kantonsregierungen (KdK) einen umfangreichen tabellarischen Leitfaden veröffentlicht, der den Anpassungsbedarf bei kantonalen Datenschutzgesetzen im Hinblick auf die Datenschutzreform der EU und die Europaratskonvention Nr. 108 aufzeigt. Basierend auf einem ersten Vorentwurf für das neue eidgenössische DSG schlägt der Leitfaden auch mögliche Lösungen vor. Die Revision des eidgenössischen Rechts war von schwierigen Diskussionen geprägt, was letztlich zur Etappierung der Umsetzung und zu zeitlichen Verzögerungen geführt hat. Der beschlossene Gesetzestext weicht deshalb zum Teil wesentlich vom ursprünglichen Vorentwurf ab. Damit erweist sich der KdK-Leitfaden, der sich auf den erwähnten Vorentwurf zum DSG stützt, zumindest teilweise als veraltet. Aus diesem Grund übernimmt das KDSG die Empfehlungen der KdK nur teilweise. Im Wesentlichen folgt das KDSG dem eidgenössischen Recht, wie es letztlich beschlossen wurde.

In Übereinstimmung mit den internationalen Bestrebungen und dem neuen Bundesrecht stärkt auch

das KDSG den Datenschutz insgesamt. Es regelt Bereiche, die bisher nicht oder nur rudimentär normiert waren. So wird die heutzutage nicht mehr wegzudenkende, mit zunehmender Digitalisierung sogar noch zunehmende Datenbearbeitung durch beauftragte Dritte (Auftragsdatenbearbeitung) neu ausdrücklich geregelt. Datenschutz befasst sich vor allem mit dem Schutz der Persönlichkeit der betroffenen Personen. Dies ist aber nur möglich, wenn auch der Schutz der Daten selbst gewährleistet ist. Diese Datensicherheit war bisher jedoch kaum Thema im Gesetz und wird neu ebenfalls ausdrücklich geregelt. Die Datenschutz-Folgenabschätzung ist ein neues Instrument, mit dem das Verantwortungsbewusstsein der Behörden im Umgang mit Datenschutz erhöht werden soll. Des Weiteren verbessert das neue KDSG punktuell die Transparenz der Datenbearbeitung sowie die Kontrollmöglichkeiten der betroffenen Personen. Und nicht zuletzt werden die Stellung und die Befugnisse der oder des Datenschutzbeauftragten gestärkt. So soll beispielsweise neu die Wahl durch den Landrat und nicht mehr durch den Regierungsrat erfolgen.

Wie erwähnt werden nicht sämtliche Regelungen des Bundes übernommen. Beispielsweise verzichtet das KDSG auf die allgemeine Einführung von Datenschutzberatern, wie sie der Bund vorsieht. Auch der KdK-Leitfaden sieht keine allgemeine Notwendigkeit von Datenschutzberatern vor, sondern höchstens in bereichsspezifischen Gesetzen.

Wie schon bisher bleibt das KDSG ein eigentliches Rahmengesetz. Es regelt die Grundsätze und Prinzipien des Datenschutzes, z. B. die Notwendigkeit einer gesetzlichen Grundlage als Voraussetzung für eine rechtmässige Datenbearbeitung. Welche gesetzliche Grundlage aber im Einzelfall die Datenbearbeitung erlaubt, muss stets die jeweils anwendbare Spezialgesetzgebung beantworten.

3. Finanzielle und personelle Auswirkungen

Es liegt auf der Hand, dass steigende Anforderungen im Bereich Datenschutz und Datensicherheit kaum ohne finanziellen und personellen Mehraufwand bewältigt werden können. Allerdings ist dieser Mehraufwand nur bedingt auf das KDSG zurückzuführen. So ist etwa das neue Instrument der Datenschutz-Folgenabschätzung im Grundsatz sowohl im Recht des Europarats als auch der EU vorgesehen. Darauf zu verzichten, wird kaum möglich sein. Dass der Aufwand im Bereich Datensicherheit weiter steigt, ist weniger eine Folge der neuen Regelungen als vielmehr der zunehmenden Digitalisierung und der damit verbundenen steigenden Internet-Kriminalität geschuldet. Mit Mehraufwand ist auch bei konsequenter Führung der öffentlichen Register der Datensammlungen zu rechnen. Diese Pflicht ist aber nicht neu, sondern wurde bisher lediglich vernachlässigt.

Als Rahmengesetz regelt das KDSG nur die Grundsätze. Bei der Umsetzung besteht durchaus Spielraum, sodass die finanziellen und personellen Auswirkungen nicht im Voraus bezifferbar sind. Jedoch können einige Punkte näher beleuchtet werden:

- Die neu geregelte Datenschutz-Folgenabschätzung führt offenkundig zu Mehraufwand. Allerdings ist sie nur bei neuen Datenbearbeitungen vorgesehen und sofern diese ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen können. Der allgemeine Verhältnismässigkeitsgrundsatz ist auch hier zu beachten, sodass die Folgenabschätzung nicht immer gleich umfangreich ausfallen wird. So ist bei einem grossen Digitalisierungsprojekt vielleicht mit einer Datenschutz-Folgenabschätzung in erheblichem Umfang zu

rechnen, die kaum ohne externe fachliche Begleitung zu bewerkstelligen ist. Wenn hingegen die Verwaltung künftig systematisch E-Mail-Adressen der Bevölkerung erfassen und verwenden soll, kann die Datenschutz-Folgenabschätzung, falls überhaupt notwendig, deutlich geringer ausfallen.

- Da die Anforderungen des Datenschutzes und der Datensicherheit auch ohne das neue KDSG insgesamt steigen und der Einbezug der oder des Datenschutzbeauftragten zum Teil ausdrücklich vorgeschrieben wird, ist auch hier zusätzlicher Aufwand zu erwarten. Damit ist fraglich, wie lange das Pensum der oder des Datenschutzbeauftragten von derzeit 20 Prozent noch genügen kann.
- Nicht zuletzt ist insbesondere bei der Einführung des KDSG mit gewissem Mehraufwand bezüglich Schulung, Weiterbildung usw. zu rechnen.

4. Vernehmlassung

Im Vernehmlassungsverfahren sind 32 Eingaben eingegangen. 16 Stellungnahmen befürworten die Vorlage insgesamt, stellen aber einzelne Anträge, die sich jedoch nur auf Details des Gesetzestextes oder den Vollzug beziehen. Zehn Antworten unterstützten die Vorlage vorbehaltlos ohne weitere Anträge. Sechs Vernehmlassungsadressatinnen und -adressaten haben ausdrücklich auf eine Stellungnahme verzichtet.

Verschiedene Rückmeldungen beziehen sich auf die Umsetzung des Gesetzes. So wird verschiedentlich gemahnt, genügend Ressourcen für die beauftragte Person für Datenschutz bereitzustellen. Mehrfach gefordert wird auch, das Archivreglement (RB 10.6212) zu überarbeiten bzw. die Archivierung auch für Gemeinden usw. zu regeln. Verschiedene Gemeinden ersuchen schliesslich um Unterstützung bei der Umsetzung des Gesetzes, z. B. in Form von Arbeitsempfehlungen, Weisungen usw., insbesondere auch zum neuen Instrument der Datenschutz-Folgenabschätzung. Hierzu ist zu sagen, dass die zuständigen Behörden selbstverständlich für einen reibungslosen Vollzug des Gesetzes zu sorgen haben. Dabei sind allerdings nicht nur die für die Datenbearbeitung verantwortlichen Behörden gefordert, sondern auch der Kanton, namentlich der Regierungsrat im Rahmen seiner Aufsicht über die Gemeinden und die beauftragte Person für Datenschutz, die nicht nur Kontroll-, sondern auch Beratungsaufgaben hat. Die Frage nach den benötigten Ressourcen oder nach einer umfassenden Regelung der Archivierung ist jedoch nicht zuletzt auch politischer Natur. Beispielsweise kann das Archivreglement die Archivierungspflicht nur für die Kantonale Verwaltung regeln (mit wenigen Ausnahmen). Für eine weitergehende Regelung ist eine Grundlage in einem Gesetz notwendig.

Auf die Anträge zum Gesetzestext wird, soweit nötig, unter den Bemerkungen zu den einzelnen Bestimmungen eingegangen.

5. Bemerkungen zu den einzelnen Bestimmungen

Artikel 1

Der Zweck des Gesetzes ist derselbe wie bisher. Allerdings weist bereits der Zweckartikel darauf hin,

dass der Geltungsbereich des neuen Gesetzes nur für natürliche Personen gilt.

Artikel 2

Der Geltungsbereich entspricht grundsätzlich dem bisherigen Recht. Die Bestimmung ist jedoch neu strukturiert und mit punktuellen Änderungen versehen. Das Gesetz beschränkt den Geltungsbereich neu ausdrücklich auf natürliche Personen, wie es auch das neue DSG tut. Dies entspricht ebenfalls den datenschutzrechtlichen Bestimmungen der EU und des Europarats. Auch wenn die Bearbeitung von Daten über juristische Personen nicht dem KDSG unterliegt, ist deren Persönlichkeit aufgrund anderer Rechtsgrundlagen geschützt. Zu nennen sind etwa Artikel 13 der Bundesverfassung (BV; SR 101), Artikel 28 ff. des Zivilgesetzbuchs (ZGB; SR 210) oder das Bundesgesetz gegen den unlauteren Wettbewerb (UWG; SR 241).

Wie bereits nach bisherigem Recht gilt das KDSG nicht, wenn eine Behörde am wirtschaftlichen Wettbewerb teilnimmt und dabei nicht hoheitlich handelt. Neu wird jedoch präzisiert, dass in diesem Fall die Vorschriften des Bundesrechts für Private gelten, die Aufsicht aber trotzdem durch die beauftragte Person für Datenschutz des Kantons erfolgt.

Artikel 3

Die Begriffsdefinitionen entsprechen dem bisherigen Recht, wurden jedoch an die aktuellen Bedürfnisse angepasst. So wurden die besonders schützenswerten Daten mit Blick auf das Bundesrecht und das europäische Recht erweitert. Neue Begriffe wie Profiling, Verletzung der Datensicherheit oder Auftragsbearbeiterin und Auftragsbearbeiter kommen dazu. Wie im DSG wird auch hier der bisherige Begriff der Inhaberin oder des Inhabers der Datensammlung ersetzt durch den der verantwortlichen Behörde. Im Übrigen folgen die Begriffsdefinitionen weitgehend dem Bundesrecht.

Nach wie vor ist auch die Rassenzugehörigkeit in der Aufzählung enthalten, was in der Vernehmlassung vereinzelt kritisiert wurde. Die Verwendung des Begriffs ist durchaus umstritten und der Versuch, Menschen aufgrund äusserer Merkmale in verschiedene «Rassen» einzuteilen, ist wissenschaftlich nicht haltbar. Dennoch wird der Begriff im EU-Recht und auch im DSG nach wie vor verwendet. Sowohl die EU als auch der Bundesrat haben dazu erklärt, dass die Verwendung dieses Begriffs nicht bedeutet, dass damit Theorien gutgeheissen werden, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen (vgl. BBl 2017 6941, 7020). In Übereinstimmung mit dem nationalen und internationalen Recht behält auch das KDSG den Begriff Rasse weiterhin bei, selbstverständlich verbunden mit derselben Erklärung.

Artikel 4

Die allgemeinen Voraussetzungen zur Bearbeitung von Personendaten (Abs. 1, 3 und 4) sind die gleichen wie nach bisherigem Recht. Für besonders schützenswerte Daten gab es bisher keine besonderen Vorschriften. Neu ist für die Bearbeitung dieser Daten sowie für das neu geregelte Profiling ein Gesetz im formellen Sinn als Grundlage nötig (Abs. 2), wie es auch das DSG fordert.

Artikel 5

Bisher nicht geregelt war die Auftragsbearbeitung, also die mit fortschreitender Digitalisierung immer häufiger vorkommende Bearbeitung von Personendaten im Auftrag der verantwortlichen Behörde. Diese Lücke wird mit einer neuen Bestimmung geschlossen. Diese entspricht unverändert dem Wortlaut von Artikel 9 DSG.

Artikel 6

Die Bestimmung wiederholt den bisherigen Artikel 6.

Artikel 7

Die Pflicht zum Erstellen einer Datenschutz-Folgenabschätzung ist eine Anforderung des europäischen Rechts. Die Datenschutz-Folgenabschätzung ist ein Instrument, um Risiken zu erkennen und zu bewerten, die für die betroffene Person durch die Datenbearbeitung entstehen können. Auf der Basis dieser Abschätzung sollen gegebenenfalls Massnahmen definiert werden, um diese Risiken für die betroffene Person zu bewältigen. Die neue Bestimmung übernimmt den Teil von Artikel 22 DSG, der für die Bundesbehörden gilt.

Als neues Instrument werden Datenschutz-Folgenabschätzungen zweifellos zu einem Mehraufwand führen. Allerdings ist eine Datenschutz-Folgenabschätzung nicht für jede Datenbearbeitung nötig, sondern nur, wenn eine vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

In der Vernehmlassung wurde mehrfach gefordert, das Gesetz solle die «Angemessenheit» der Datenschutz-Folgenabschätzung oder die «Angemessenheit» der Massnahme ausdrücklich festhalten. Sowohl die in der Folgenabschätzung zu beurteilenden Risiken als auch die möglichen Massnahmen sind jedoch derart offen formuliert, dass die zuständige Behörde in ihrer Arbeit hier zweifellos über grossen Beurteilungsspielraum verfügt. Die Botschaft des Bundesrats zum DSG hält ausdrücklich fest, dass bei den zu treffenden Massnahmen durchaus eine Abwägung zwischen den Interessen der betroffenen Person und der verantwortlichen Behörde erfolgen darf (vgl. BBl 2017 6941, 7061). Damit steht fest, dass bei einer Datenschutz-Folgenabschätzung ein erheblicher Ermessensspielraum besteht. Damit muss der Entscheid ohnehin «angemessen» sein und eine entsprechende Präzisierung des Gesetzestexts ist unnötig. Nachdem die Bestimmung weitgehend dem Bundesrecht entspricht, würde ein Abweichen vom Wortlaut des DSG überdies zur Frage führen, ob damit eine inhaltliche Änderung beabsichtigt wird, was vorliegend nicht der Fall ist.

Artikel 8

Die Bestimmung beschreibt die Konsequenzen aus der Datenschutz-Folgenabschätzung und ist dementsprechend ebenfalls neu. Auch hier wird das Bundesrecht (Art. 23 DSG) übernommen. So ist die Konsultation der oder des Datenschutzbeauftragten erst notwendig, wenn trotz der aufgrund einer Datenschutz-Folgenabschätzung vorgesehenen Massnahmen immer noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person besteht.

Artikel 9

Nach bisherigem Recht wurde zwischen der Datenbekanntgabe an andere Behörden und an Private unterschieden. Diese Unterscheidung hat im Ergebnis kaum Auswirkungen und ist deshalb nicht mehr zweckmässig. Auch der Bund trifft diese Unterscheidung nicht, sodass darauf verzichtet werden soll. Stattdessen regelt Artikel 9 neu die Grundsätze der Bekanntgabe von Personendaten. Die Buchstaben a bis c entsprechen dabei der Regelung des bisherigen Rechts. Die Buchstaben d bis f übernehmen die Regelung des Bundesrechts (Art. 36 Abs. 2 Bst. c bis e DSG). Absatz 2 entspricht dem bisherigen Artikel 8 Absatz 3, während Absatz 3 den Artikel 36 Absatz 6 DSG übernimmt. Letzterer schränkt eine grundsätzlich zulässige Datenbekanntgabe ein, wenn bestimmte Voraussetzungen vorliegen.

Im Vernehmlassungsverfahren wurde vereinzelt die Forderung gestellt, es sei ein neuer Absatz zu schaffen, der betroffenen Personen unter bestimmten Voraussetzungen die Möglichkeit einräumt, die Bekanntgabe ihrer eigenen Daten an Private zu sperren. Das KDSG sieht jedoch bereits gewisse Fälle vor, in denen die betroffene Person der Datenbekanntgabe zustimmen muss oder auf andere Art Einfluss auf eine Datenbekanntgabe nehmen kann (Art. 9 Abs. 1 Bst. c, e und f). Im Grundsatz wird damit dem geforderten Anliegen bereits Rechnung getragen. Die Schaffung einer zusätzlichen Möglichkeit, in den zulässigen Fällen eine Datenbekanntgabe pauschal zu sperren, ist unnötig und widerspricht dem Konzept der Bestimmung.

Artikel 10

Das europäische Recht verlangt, dass Daten grundsätzlich nur ins Ausland übermittelt werden dürfen, wenn ein angemessenes Datenschutzniveau besteht. Für die Länder der EU und die Vertragsstaaten der Europakonvention Nr. 108, die dieser Regelung unterstehen, gilt dies ohne Weiteres (Abs. 1). Für Drittstaaten ist das Datenschutzniveau jeweils gesondert zu betrachten. Dass es kaum zweckmässig ist, wenn die Urner Behörden diese Prüfung jeweils im Einzelfall selber vornehmen müssen, leuchtet ein. Deshalb wird auf das Bundesrecht verwiesen (Abs. 2). Demzufolge soll der Bundesrat in der Verordnung feststellen, welche Staaten über ein angemessenes Datenschutzniveau verfügen.

Artikel 11

Die Bestimmung entspricht inhaltlich weitgehend dem bisherigen Recht. Der Wortlaut folgt dem neuen Bundesrecht und übernimmt damit auch den neuen Buchstaben b, der den Schutz besonders schützenswerter Daten verstärkt. Der frühere Artikel 10 Absatz 2, der zusätzlich noch die Bekanntgabe von Daten zur Bearbeitung für nicht personenbezogene Zwecke an andere Behörden regelte, wird nicht mehr übernommen. Die Bestimmung hatte keinen eigenen Anwendungsbereich, denn die Datenbearbeitung, die ja nach wie vor geregelt ist, umfasst auch die Datenbekanntgabe.

In der Vernehmlassung wurde angeregt, im ganzen Artikel einheitlich vorzusehen, dass die Personendaten «anonymisiert» sein müssen, und nicht vereinzelt zu verlangen, dass die betroffenen Personen «nicht bestimmbar» sind. Damit eine Person nicht mehr bestimmbar sei, müssten die Daten ohnehin anonymisiert sein. Namentlich genüge eine Pseudonymisierung nicht. Dieser Auffassung ist jedoch

nicht zu folgen. Der Bundesrat hält in seiner Botschaft fest, dass die betroffene Person nicht bestimmbar ist, wenn die Daten in pseudonymisierter Form weitergegeben werden und der Schlüssel bei der weitergebenden Person verbleibt (faktische Anonymisierung; BBl 2017 6941, 7083).

Artikel 12

Der Grundsatz der Datensicherheit fand im bisherigen Recht nur wenig Beachtung (vgl. Art. 11 im bestehenden KDSG). Datenschutz - also der Persönlichkeitsschutz der einzelnen Personen - ist jedoch nur möglich, wenn auch die Datensicherheit gegeben ist, d. h. wenn allgemeine technische und organisatorische Massnahmen für die Sicherheit der Daten sorgen. Auch das internationale Recht stellt explizite Anforderungen an die Datensicherheit. Die Vorlage trägt diesen Anforderungen Rechnung und übernimmt hierzu weitgehend das ebenfalls überarbeitete Bundesrecht. Demnach muss die Datensicherheit dem jeweiligen Risiko angemessen sein. Im Vernehmlassungsverfahren wurde gefordert, die Regelung der Datensicherheit solle sich an den Artikeln 1 bis 5 der neuen Datenschutzverordnung des Bundes orientieren. Auf eine entsprechende Regelung im Gesetz wird jedoch verzichtet. Zum einen sind eigentliche Ausführungsbestimmungen, wie sie in der Datenschutzverordnung enthalten sind, auf Gesetzesebene nicht stufengerecht. Zum anderen wird bei der Auslegung dieser Bestimmung, die weitgehend dem Bundesrecht entspricht, zweifellos auch das Ausführungsrecht des Bundes herangezogen werden. Zudem bietet die vorliegende Regelung mehr Flexibilität, indem dem Regierungsrat ermöglicht wird, auch eigene Ausführungsbestimmungen zu erlassen.

Artikel 13

Auch die Pflicht zur Meldung von Verletzungen der Datensicherheit entspricht den Anforderungen des internationalen Rechts. Anders als im Bundesrecht verzichtete der Vernehmlassungsentwurf noch darauf, den Mindestinhalt der Meldung gesetzlich festzulegen, was in mehreren Stellungnahmen kritisiert wurde. Die Regelung wurde entsprechend überarbeitet und entspricht nun weitgehend dem Bundesrecht.

Artikel 14

Die Bestimmung entspricht unverändert dem bisherigen Recht. Weiterhin sollen der Kanton, die Gemeinden sowie die öffentlich-rechtlichen Körperschaften und Anstalten das vorgeschriebene öffentliche Register selber führen - nicht wie beim Bund, wo die oder der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte dieses Register führt. Der Bund verwendet überdies neu den Begriff der Datensammlung nicht mehr. Stattdessen wird nur noch der Begriff «Bearbeiten von Daten» benutzt. Dementsprechend führt die oder der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte künftig kein «Register der Datensammlungen» mehr, sondern ein «Register der Bearbeitungstätigkeiten der Bundesorgane». Die Auswirkungen dieser Änderungen erscheinen gering, sodass im kantonalen Recht an der bisherigen Terminologie festgehalten wird.

Der Kanton führt sein Register bisher zentral bei der Standeskanzlei. Die zentrale Bewirtschaftung ist kaum mehr zeitgemäss. Abgesehen von den inhaltlichen Vorgaben schreibt das Gesetz den Gemeinden nicht vor, wie sie ihre Register führen sollen. So ist es dem Regierungsrat ohne Weiteres erlaubt, für die Kantonale Verwaltung eine neue Regelung zu treffen.

Artikel 15

Die Bestimmung übernimmt weitgehend den Wortlaut der entsprechenden Regelung von Artikel 38 DSGVO, der wiederum praktisch unverändert dem bisherigen (Bundes-)Recht entspricht. Die neue Formulierung bringt materiell kaum Änderungen. Wie bisher regelt der Regierungsrat im Rahmen seiner Zuständigkeit die Archivierung im Archivreglement. Andere Akteurinnen und Akteure, namentlich Gemeinden, Korporationen und weitere öffentlich-rechtliche Körperschaften und Anstalten sind für die Regelung ihrer Archivierung selber zuständig, vorbehältlich allfälliger Vorschriften in einzelnen Spezialgesetzen.

Im Vernehmlassungsverfahren wurde vereinzelt angeregt, die Datenvernichtung sei dahingehend zu präzisieren, dass Daten «weder visuell noch elektronisch oder auf sonst welche Art ausgelesen werden können». Das ist unnötig. Denn wenn die Daten noch auslesbar sind, sind sie nicht vernichtet.

Artikel 16

Die Einsicht in die Register entspricht unverändert dem bisherigen Recht.

Artikel 17

Neu geregelt wird hingegen das Auskunftsrecht. Anstatt wie bisher nur das Recht auf Einsichtnahme in Daten im Grundsatz festzuhalten, regelt die neue Bestimmung auch die Zuständigkeiten im Falle einer Auftragsdatenbearbeitung (Abs. 2) und stellt klar, dass auf das Auskunftsrecht nicht im Voraus verzichtet werden kann (Abs. 4). Die neue Bestimmung entspricht weitgehend Artikel 25 DSGVO. Im Gegensatz zum Bund verzichtet die kantonale Regelung jedoch auf eine (ohnehin nicht abschliessende) Aufzählung, welche Informationen in jedem Fall mitzuteilen sind (Art. 25 Abs. 2 DSGVO). Andere Inhalte der bundesrechtlichen Regelung werden an anderer Stelle dieser Vorlage berücksichtigt. So befindet sich die Möglichkeit, Gesundheitsdaten durch eine Gesundheitsfachperson mitzuteilen (Art. 25 Abs. 3 DSGVO) in ähnlicher Weise in Artikel 18. Der Grundsatz der Kostenlosigkeit der Auskunft (Art. 25 Abs. 6 DSGVO) ist in Artikel 22 enthalten. Nicht übernommen wird die Vorschrift, wonach eine Auskunft in der Regel innerhalb von 30 Tagen erteilt wird (Art. 25 Abs. 7 DSGVO), obwohl dies in der Vernehmlassung vereinzelt gefordert wurde. Der Anspruch auf eine Beurteilung innert angemessener Frist ergibt sich aus den allgemeinen Verfahrensgarantien von Artikel 29 BV. Eine dem Einzelfall angemessene Frist erscheint sinnvoller als eine kaum verbindliche Regelfrist.

Artikel 18

Die Einschränkungen des Auskunftsrechts entsprechen inhaltlich dem bisherigen Recht und wurden nur sprachlich angepasst.

Artikel 19

Die Bestimmung über den Anspruch auf Berichtigung unrichtiger Daten entspricht unverändert dem bisherigen Recht. Das Bundesgesetz sieht für diesen Anspruch keinen eigenen Artikel mehr vor, sondern regelt den Grundsatz der Richtigkeit der Daten einerseits unter den allgemeinen Grundsätzen

der Datenbearbeitung (Art. 6 Abs. 5 DSG) und den Anspruch auf Berichtigung im Artikel über Ansprüche und Verfahren (Art. 41 DSG).

Im Vernehmlassungsverfahren ging ein Antrag ein, wonach Daten gelöscht werden müssen, wenn deren Richtigkeit nicht bewiesen werden könne. Für Daten, die grundsätzlich zur Erfüllung einer gesetzlichen Aufgabe benötigt werden (siehe Art. 4), pauschal die Löschung zu verlangen, wenn deren Richtigkeit nicht bewiesen werden kann, ist jedoch nicht sachgerecht und in der Regel wohl weder im Interesse der betroffenen Person noch der bearbeitenden Behörde. Auch das DSG sieht für den Fall, dass die Richtigkeit von Daten nicht bewiesen werden kann, lediglich einen Bestreitungsvermerk vor.

Artikel 20

Die Bestimmung übernimmt die bestehende Regelung. Diese entspricht dem bisherigen und im Grundsatz auch dem neuen Bundesrecht. Zwar wird Artikel 41 DSG weiter ausgebaut und zählt neu ausdrücklich auf, was der Anspruch gegen widerrechtliche Datenbearbeitung alles umfasst (Berichtigen, Löschen oder Vernichten der Daten, unter bestimmten Voraussetzungen: Einschränken der Datenbearbeitung sowie Ausnahmen bei Daten in öffentlich zugänglichen Archiven). Das kantonale Recht verzichtet darauf, den Unterlassungs-, Beseitigungs- und Feststellungsanspruch umfassend zu präzisieren. Damit ist nach Prüfung der Umstände im Einzelfall zu entscheiden, wie ein geltend gemachter Anspruch letztlich umzusetzen ist.

Artikel 21

Die Bestimmung über den Rechtsschutz entspricht dem kantonalen Standard und wurde aus dem bisherigen Recht unverändert übernommen.

Artikel 22

Der Grundsatz der Gebührenfreiheit entspricht dem bisherigen Recht und gilt auch im Bundesrecht. Wie bisher gibt es jedoch Ausnahmen, um Missbräuchen vorzubeugen.

Artikel 23

Die Unabhängigkeit ist eine wichtige Voraussetzung für die wirksame Tätigkeit der oder des Beauftragten für Datenschutz. Sie findet sich in den internationalen Anforderungen und ist auch im geltenden Recht geregelt. Bisher wird die beauftragte Person für Datenschutz vom Regierungsrat gewählt. Als oberste Verwaltungsbehörde gehört der Regierungsrat jedoch zum Kreis der kontrollierten Behörden. Ausserdem sieht das bisherige Recht vor, dass der beauftragten Person für Datenschutz nur gekündigt werden kann, wenn ein sachlich zureichender Grund vorliegt. Dieselbe Voraussetzung gilt jedoch für alle kantonalen Angestellten (Art. 16 Personalverordnung; RB 2.4211). Für die Kündigung der oder des Datenschutzbeauftragten gibt es demnach keine höhere Hürde.

Die «Wahl des Kontrollorgans durch die Kontrollierten» sowie die relativ einfache Kündigungsmöglichkeit lassen sich mit der geforderten Unabhängigkeit nur schwer vereinbaren. Die KdK empfiehlt in

ihrem Leitfaden auch eine Wahl durch das Parlament oder wenigstens unter Beteiligung des Parlaments, die Wahl auf eine feste Amtszeit von mindestens vier Jahren sowie eine Beschränkung der Amtsenthebung. Diesen Empfehlungen soll gefolgt werden. Dementsprechend bestimmt die Vorlage neu den Landrat als Wahlbehörde. Ohne anderslautende Regelung gilt ohne Weiteres die Amtsdauer von vier Jahren gemäss Artikel 83 der Verfassung des Kantons Uri (RB 1.1101), was das Gesetz im Sinne der Klarstellung vermerkt. Soweit ersichtlich verfügen sämtliche Kantone der Zentralschweiz über eine ähnliche Regelung. Nur Nidwalden sieht eine Wahl durch den Regierungsrat vor, jedoch auf eine feste Amtszeit.

Neu werden auch einige Unvereinbarkeiten geregelt, um die Unabhängigkeit der oder des Beauftragten zu gewährleisten. So darf die beauftragte Person für Datenschutz gleichzeitig kein anderes öffentliches Amt und keine leitende Funktion in einer politischen Partei ausüben (Abs. 2) und eine zusätzliche Erwerbstätigkeit muss vom Regierungsrat bewilligt werden (Abs. 3). Die übrigen Bestimmungen (Abs. 4: finanzielle und personelle Unabhängigkeit, Abs. 5: Möglichkeit der Zusammenarbeit mit anderen Kantonen) entsprechen dem bisherigen Recht. Als Konsequenz der Wahl durch den Landrat wird für die Übertragung der Aufgaben der oder des Datenschutzbeauftragten auf eine Person oder Stelle eines anderen Kantons oder für die Einrichtung eines gemeinsamen Organs neu die Genehmigung des Landrats verlangt.

Artikel 24

Die Aufgaben der oder des Beauftragten für Datenschutz sind nach wie vor dieselben. Die Bestimmung wird gegenüber dem bisherigen Recht nur geringfügig angepasst. Neu ist hingegen Absatz 4, der gerichtliche Verfahren von der Aufsicht der beauftragten Person für Datenschutz ausnimmt. Dabei handelt es sich um das Gegenstück zu Artikel 2 Absatz 4, der dieselben Verfahren vom Geltungsbereich des Datenschutzgesetzes ausnimmt. Bereiche, die nicht dem Datenschutzgesetz unterliegen, sollen konsequenterweise auch nicht der Aufsicht der oder des Datenschutzbeauftragten unterliegen.

In der Vernehmlassung wurde gefordert, für die Berichterstattung an den Landrat (Art. 24 Abs. 3 Bst. e) sei die Periodizität zu präzisieren (Ein- oder Zweijahresrhythmus, allenfalls analog zum Rechenschaftsbericht des Regierungsrats über die Kantonale Verwaltung). Eine Regelung analog zum Rechenschaftsbericht über die Kantonale Verwaltung ist durchaus sinnvoll. Allerdings sieht auch die Verfassung des Kantons Uri diesbezüglich lediglich vor, dass der Regierungsrat dem Landrat den Rechenschaftsbericht regelmässig vorzulegen hat. Für den praktizierten zweijährigen Rhythmus gibt es keine gesetzliche Grundlage. Im Sinne einer Gleichbehandlung wird auch an dieser Stelle auf Gesetzesstufe lediglich präzisiert, dass der Rechenschaftsbericht regelmässig zu erfolgen hat.

Artikel 25

Der Beginn eines Verfahrens (Abs. 1) sowie die Befugnisse der beauftragten Person im Rahmen der Abklärungen (Abs. 2) sind gleich wie bisher. Neu geregelt werden jedoch die Möglichkeiten am Ende eines Verfahrens. Bislang konnte die oder der Datenschutzbeauftragte bei festgestellten Datenschutzverletzungen lediglich Empfehlungen abgeben. Weigerte sich die verantwortliche Behörde,

diesen zu folgen, musste sie dies der beauftragten Person für Datenschutz in einer Verfügung mitteilen, wogegen diese Beschwerde einlegen konnte. In der Praxis wurde das Verfahren kaum je in dieser Form angewandt. In aller Regel können datenschutzrechtliche Probleme zwischen den Behörden und der oder dem Datenschutzbeauftragten einvernehmlich besprochen und gelöst werden. Das neue Recht hält deshalb den Grundsatz der einvernehmlichen Lösung ausdrücklich fest. Dieser ähnelt zwar der Empfehlung der beauftragten Person für Datenschutz nach bisherigem Recht, verdeutlicht jedoch den kooperativen und informellen Ansatz, während Empfehlungen letztlich einseitig erlassen werden und auch sehr förmlich daherkommen können.

Erst bei Uneinigkeit der Beteiligten wird ein formelles Verfahren vorgesehen. Neu ist es jedoch die beauftragte Person für Datenschutz, die in diesem Fall eine Verfügung erlassen kann. Die betroffene Behörde hat die Möglichkeit, die Verfügung beim Obergericht anzufechten. Dies bedeutet eine Stärkung der Position der oder des Datenschutzbeauftragten, auch wenn davon auszugehen ist, dass dieses formelle Verfahren auch weiterhin kaum zur Anwendung kommen wird.

Artikel 26

Die Regelung der Schweigepflicht entspricht dem bisherigen Recht und benötigt keine weiteren Erläuterungen.

Artikel 27

Die Befugnis des Regierungsrats, Ausführungsbestimmungen zu erlassen, ergibt sich grundsätzlich aus Artikel 94 Verfassung des Kantons Uri. Eine ausdrückliche Regelung im Spezialerlass ist aber nicht unüblich und wurde auch hier aus dem bisherigen Recht übernommen.

Artikel 28

Bei den Strafbestimmungen besteht kein Änderungsbedarf. Sie entsprechen unverändert dem bisherigen Recht.

Artikel 29

Hier handelt es sich um die übliche Aufhebungsbestimmung.

Artikel 30

Nachdem das KDSG einen anderen Kurztitel trägt als das bisherige Gesetz, sind die Verweise in anderen Rechtserlassen, die den bisherigen Kurztitel verwenden, entsprechend anzupassen. Dabei können nur Rechtserlasse der gleichen Stufe (d. h. Gesetz) geändert werden. Nicht anzupassen sind Verweise, die den vollen Titel des Gesetzes verwenden. Dieser ändert sich nicht.

Artikel 31

Damit laufende Datenbearbeitungen mit dem Inkrafttreten des neuen Gesetzes nicht plötzlich unrechtmässig werden, wird eine Übergangsbestimmung geschaffen. Zu denken ist etwa an die Bearbeitung von besonders schützenswerten Daten (Art. 4 Abs. 2), für die neu eine Grundlage in einem Gesetz im formellen Sinn verlangt wird. Andere Verschärfungen, wie z. B. die Datenschutz-Folgenabschätzung (Art. 7), gelten ohnehin nur für neue Datenbearbeitungen. Dafür ist keine Übergangsbestimmung nötig.

Artikel 32

Die Bestimmung enthält die übliche Inkrafttretensformel. Das Gesetz soll nach der Volksabstimmung in Kraft treten, sobald das Abstimmungsergebnis erwahrt wurde.

III. Antrag

Gestützt auf den vorstehenden Bericht beantragt der Regierungsrat dem Landrat, den folgenden Beschluss zu fassen:

Das Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz; KDSG), wie es in der Beilage enthalten ist, wird zuhanden der Volksabstimmung verabschiedet.

Beilage

- Kantonales Datenschutzgesetz (KDSG; RB 2.2511)