IIIIII KANTON solothurn

KR.Nr.

Teilrevision des Informations- und Datenschutzgesetzes (InfoDG) und weiterer Gesetze

Botschaft und Entwurf des Regierungsrates
an den Kantonsrat von Solothurn
vom . . . . ., RRB Nr. . . . . .

Zuständiges Departement

Staatskanzlei

Vorberatende Kommissionen

Justizkommission
Finanzkommission

Inhaltsverzeichnis

Beilagen

Beschlussesentwurf
Synopse

Kurzfassung

Am 27. April 2016 verabschiedete die Europäische Union (EU) die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DSGVO) sowie die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts (Richtlinie). Die Richtlinie bildet für die Schweiz Bestandteil des Schengen-Besitzstands, weshalb sie von Bund und Kantonen umgesetzt werden muss. Auch die DSGVO ist für die Schweiz von Bedeutung, denn sie stellt den Massstab für die Beurteilung der Angemessenheit des Schweizerischen Datenschutzniveaus durch die EU dar. Der Bund und die Kantone müssen ihre Datenschutzgesetze mit der geänderten Rechtslage in der EU in Einklang bringen. Der Bund und die Mehrheit der Kantone haben dies in der Zwischenzeit getan. Mit dieser Vorlage soll das Informations- und Datenschutzgesetz (InfoDG; BGS 114.1) im Rahmen einer Teilrevision an die zwingenden Vorgaben des EU-Rechts angepasst werden. Dies hat insbesondere die folgenden Änderungen zur Folge:

- Anpassung des datenschutzrechtlichen Geltungsbereichs an den europäischen Rechtsrahmen (§ 2 Abs. 3 InfoDG).

- Übernahme bzw. Anpassung gewisser Begriffe (§ 6 InfoDG): Z.B. wird der Begriff des «Profilings» bei den besonders schützenswerten Personendaten neu eingeführt, während jener der «Datensammlung» aufgehoben werden kann.

- Regelung der Datenbearbeitung durch Auftragsdatenbearbeiterinnen bzw. Auftragsdatenbearbeiter (§ 6 Abs. 8 und § 17 InfoDG).

- Präzisierung der Informationspflicht (§ 18bis InfoDG).

- Gesetzliche Verankerung des Rechts auf Löschung oder Vernichtung unrichtiger oder widerrechtlich bearbeiteter Personendaten (§ 28 und § 30 InfoDG).

- Regelung der Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung bei Datenbearbeitungen, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen können (§ 30bis InfoDG).

- Regelung der Meldepflicht bei Verletzungen der Datensicherheit (§ 30ter InfoDG).

- Regelung der Verantwortung der Behörden für die Datenbearbeitung (§ 30^{quater} InfoDG).

- Stärkung der Unabhängigkeit der bzw. des Beauftragten für Information und Datenschutz (im Folgenden: IDSB), insbesondere durch den Verzicht auf das Antragsrecht des Regierungsrates bei ihrer bzw. seiner Wahl (§ 31 Abs. 1 InfoDG) und die abschliessende Aufzählung der Gründe für eine Amtsenthebung (§ 31 Abs. 2 InfoDG).

- Aktualisierung und Präzisierung des Aufgabenkatalogs der bzw. des IDSB (§ 32 InfoDG).

- Einführung einer Pflicht der Strafverfolgungs-, Strafgerichts- und Strafvollzugsbehörden, eine Datenschutzberaterin bzw. einen Datenschutzberater zu ernennen (§ 33ter InfoDG).

- Einführung einer Verfügungskompetenz der bzw. des IDSB gegenüber Behörden bei Datenschutzverletzungen (§ 38 InfoDG).

- Einführung der Möglichkeit, gegenüber dem Regierungsrat, dem Kantonsrat, den Gerichten sowie – in Strafverfahren – der Staats- und der Jugendanwaltschaft anstelle der Verfügung beratende Empfehlungen abzugeben (§ 38bis InfoDG).

Die Gelegenheit wird zudem wahrgenommen, einige weitere gesetzliche Anpassungen vorzunehmen, namentlich in Umsetzung erheblich erklärter Aufträge sowie durch die Normierung bisher bewährter Praxis, etwa:

- Umsetzung des Auftrags Rémy Wyssmann (SVP, Kriegstetten) «Verschleppung von Zugangsgesuchen verhindern» (A 0147/2021) durch Einführung einer Frist von 30 Tagen, innert welcher die Behörden Zugangsgesuche grundsätzlich behandeln müssen (§ 35 InfoDG).

- Umsetzung des Auftrags Rolf Sommer (SVP, Olten) «Offenlegung der Entschädigungen» (A 0034/2021) durch eine Regelung im Regierungs- und Verwaltungsorganisationsgesetz (RVOG; BGS 122.111), welche die Veröffentlichung der an die Mitglieder der Leitungs- und Aufsichtsorgane der mittelbaren Verwaltung ausgerichteten Entschädigungen vorsieht (§ 26 Abs. 6 RVOG).

- Normierung der Pflicht, bei Videoüberwachungsanlagen an öffentlichen und allgemein zugänglichen Orten eine Weisung für den Betrieb zu erlassen (§ 16bis Abs. 1 InfoDG).

- Einführung einer um 30 Jahre verlängerten Schutzfrist für Personendaten, die einem Berufsgeheimnis unterstehen, insbesondere Patientendaten (§ 21 Abs. 6 InfoDG).

- Einführung einer Veröffentlichungsflicht des Registers der Bearbeitungstätigkeiten durch die bzw. den IDSB (§ 25 InfoDG).

Sehr geehrter Herr Präsident,
sehr geehrte Damen und Herren

Wir unterbreiten Ihnen nachfolgend Botschaft und Entwurf über die Teilrevision des Informations- und Datenschutzgesetzes (InfoDG; BGS 114.1) und weiterer Gesetze.

1. Ausgangslage

1.1 Rechtsentwicklungen auf europäischer Ebene

In den vergangenen Jahren ist das Datenschutzrecht auf europäischer Ebene modernisiert und stark verändert worden. Am 27. April 2016 verabschiedeten das Parlament und der Rat der EU die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DSGVO)[1] sowie die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts (Richtlinie)[2]. Die Richtlinie bildet für die Schweiz Bestandteil des Schengen-Besitzstands, weshalb sie von Bund und Kantonen umgesetzt werden muss.

Die im Verhältnis zur Richtlinie etwas ausführlichere DSGVO ist zwar nicht Schengen-relevant, entfaltet aber gleichwohl – zumindest indirekt – wichtige Auswirkungen für die Schweiz. Die Schweiz gilt ausserhalb des Schengen-Raums im Datenschutzrecht als Drittstaat, was zur Folge hat, dass ein ungehinderter Datenaustausch zwischen den Mitgliedstaaten der EU und der Schweiz grundsätzlich davon abhängig ist, dass die Schweiz ein angemessenes Datenschutzniveau vorweist.[3] Mit Bericht vom 15. Januar 2024 bestätigte die Europäische Kommission die Angemessenheit des Schweizer Datenschutzniveaus. Die EU anerkennt dadurch, dass die Gesetzgebung der Schweiz weiterhin ein angemessenes Schutzniveau für die Bearbeitung von Personendaten bietet.[4]

Schliesslich hat auch der Europarat im Bereich des Datenschutzrechts Änderungen beschlossen, indem er eine modernisierte Fassung des Übereinkommens zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (SEV 108+)[5] verabschiedet hat. Die Schweiz hat das SEV 108+ am 21. November 2019 unterzeichnet und am 7. September 2023 ratifiziert, womit dieses innerstaatlich umzusetzen ist. Das SEV 108+ ist zur DSGVO und zur Richtlinie weitgehend deckungsgleich, wenn auch weniger detailliert.

Im Jahr 2018 fand die Dritte Schengen-Evaluierung der Schweiz statt. Im Anschluss an die Verabschiedung des (vertraulichen) Evaluierungsberichts hat der EU-Rat am 7. März 2019 eine Reihe von Empfehlungen zur Beseitigung festgestellter Mängel erlassen (Schengen-Empfehlungen).[6] Die Empfehlungen betreffen insbesondere die Ressourcen, Aufgaben und Kompetenzen der Datenschutzaufsichtsstellen.

1.2 Rechtsentwicklungen auf Bundesebene und in den Kantonen

Im Anschluss an die Rechtsentwicklungen auf europäischer Ebene hat der Bund das Bundesgesetz über den Datenschutz (DSG; SR 235.1) einer Totalrevision unterzogen. Leitlinien der Revision waren mitunter die Anpassung des Datenschutzes an die technologischen Entwicklungen

[1] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679.
[2] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016L0680.
[3] Vgl. Botschaft des Bundesrates vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 (nachfolgend zitiert als «Botschaft nDSG»), 6964 f.
[4] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52024DC0007.
[5] Abrufbar unter: https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726; Zweites Änderungsprotokoll zum Übereinkommen (Konvention 108+) in deutscher Sprache, vgl. BBl 2020, 599. Die Konvention 108+ tritt erst in Kraft, sobald 38 Vertragsstaaten das Änderungsprotokoll ratifiziert haben.
[6] Abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-7281-2019-INIT/de/pdf.

und die Angleichung der Rechtsordnung an den europäischen Rahmen, nicht zuletzt zur Beibehaltung des Angemessenheitsbeschlusses der EU-Kommission.[1] Im September 2020 haben National- und Ständerat das totalrevidierte DSG verabschiedet. Das DSG ist am 1. September 2023 in Kraft getreten.

Die meisten Kantone haben ihre Datenschutzgesetze angepasst. Die notwendigen Gesetzesrevisionen sind in den Kantonen AG, AI, AR, BL, BS, FR, GE, GL, GR, JU, LU, NE, OW, SG, SH, SZ, UR, VS, ZG und ZH beschlossen worden bzw. in Kraft getreten. In den übrigen sechs Kantonen sind Revisionsarbeiten derzeit im Gange.

1.3 Bedeutung für den Kanton Solothurn

Wie bereits ausgeführt, ist die Schweiz aufgrund der Schengen-Assoziierungsabkommen verpflichtet, die Richtlinie innerstaatlich umzusetzen, wobei die Schengen-Empfehlungen von Bedeutung sind. Ferner bewirkt die Unterzeichnung des SEV 108+ ebenfalls Anpassungsbedarf. Schliesslich bedingt die Aufrechterhaltung des Angemessenheitsbeschlusses der EU-Kommission auch die Berücksichtigung der DSGVO.

Die Umsetzung der erwähnten Erlasse erfordert neben den Revisionen auf Bundesebene auch solche auf kantonaler Ebene. Im Kanton Solothurn stehen das InfoDG sowie die Informations- und Datenschutzverordnung (InfoDV; BGS 114.2) im Fokus.

Die Revision bietet ausserdem einen Rahmen, um gewisse Anpassungen des nunmehr über 20 Jahre alten Gesetzes ins Visier zu nehmen. Dabei geht es primär nicht um eigentliche materielle Neuerungen, sondern um Nachführungen der entwickelten Verwaltungs- und Gerichtspraxis und um Angleichungen an die Rechtsordnungen des Bundes und anderer Kantone.

Zur Unterstützung der Kantone bei der Anpassung ihrer (Informations- und) Datenschutzgesetze aufgrund der gesetzgeberischen Entwicklungen auf europäischer Ebene hat die Konferenz der Kantonsregierungen (KdK) 2017 unter Mitwirkung von Vertretungen der kantonalen Datenschutzbeauftragten einen ausführlichen Leitfaden (KdK-Leitfaden) erarbeitet. Der KdK-Leitfaden hat als wesentliche Grundlage für die vorliegenden Revisionspunkte gedient.

1.4 Ziele der Revision

Die Ziele der vorliegenden Revision lassen sich folgendermassen zusammenfassen:

a. Vornahme der notwendigen Anpassungen aufgrund der neuen Anforderungen des europäischen Rechts;

b. Umsetzung der erheblich erklärten Aufträge Rémy Wyssmann (SVP, Kriegstetten) «Verschleppung von Zugangsgesuchen verhindern» (A 0147/2021) und Rolf Sommer (SVP, Olten) «Offenlegung der Entschädigungen» (A 0034/2021);

c. Vornahme von Anpassungen, welche sich aufgrund der Rechtsprechung und anderer Rechtsentwicklungen aufdrängen.

1.5 Daten juristischer Personen als Personendaten

Die DSGVO, die Richtlinie und das SEV 108+ sowie nun neu auch das DSG beschränken sich auf den Schutz von Daten über natürliche Personen, fassen somit Daten juristischer Personen nicht (mehr) unter den Begriff der «Personendaten». Die Kantone sind in dieser Frage unterschiedliche Wege gegangen. Während die Mehrheit der Kantone (z.B. die Kantone AG [§ 3 Abs. 1 Bst. d

[1] Vgl. Botschaft nDSG, 6970 ff.

IDAG-AG], BL [§ 3 Abs. 3 IDG-BL], BS [§ 3 Abs. 3 IDG-BS] und LU [§ 2 Abs. 1 KDSG-LU]) nur noch Daten über natürliche Personen schützen, haben z.B. die Kantone BE (Art. 3 Abs. 1 Bst. b E-KDSG-BE) und TG (§ 3 Abs. 1 E-TG DSG) keine derartige Einschränkung vorgenommen.

Aufgrund des Legalitätsprinzips (Art. 5 Abs. 1 der Bundesverfassung der Schweizerischen Eidgenossenschaft [BV; SR 101]) müssen die Behörden ihr Handeln immer auf eine Rechtsgrundlage abstützen können. Ferner bedürfen Eingriffe in Grundrechte zu ihrer Rechtfertigung nach Artikel 36 Absatz 1 BV einer genügend bestimmten gesetzlichen Grundlage. Die Ausnahme von Daten juristischer Personen vom Begriff «Personendaten» hätte zur Folge, dass für die Bearbeitung von Daten juristischer Personen keine Rechtsgrundlagen mehr vorhanden wären. Weil diese Bearbeitung allerdings weiterhin eine behördliche Handlung und einen Grundrechtseingriff verkörpert, müssten eine Reihe von Bestimmungen ergänzt bzw. neu geschaffen werden, welche die Bearbeitung mit Daten juristischer Personen regeln (der Bund hat in Art. 71 DSG für die dafür nötigen Gesetzesanpassungen eine Übergangsfrist von 5 Jahren vorgesehen). Auch im Zusammenhang mit Zugangsgesuchen nach dem Öffentlichkeitsprinzip wären Anpassungen erforderlich.

Da mit der Entlassung der juristischen Personen aus dem Begriff der «Personendaten» zahlreiche Rechtsgrundlagen in vielen Bereichen angepasst oder neu geschaffen werden müssten, um dem Legalitätsprinzip zu genügen, verzichtet der vorliegende Revisionsentwurf auf diese Änderung.

1.6 Vernehmlassungsverfahren

Über die Vorlage wurde vom 17. November 2025 bis 17. Februar 2026 ein öffentliches Vernehmlassungsverfahren durchgeführt. Eine Vernehmlassung eingereicht haben: …

Mit RRB Nr. 2025/… vom … 2025 hat der Regierungsrat vom Vernehmlassungsergebnis Kenntnis genommen und die Staatskanzlei beauftragt, Botschaft und Entwurf an den Kantonsrat auszuarbeiten.

Das Vernehmlassungsergebnis lässt sich im Wesentlichen wie folgt zusammenfassen:

…

1.7 Erwägungen, Alternativen

Das kantonale Recht muss an das europäische Datenschutzrecht (Schengen-Besitzstand) angepasst werden. Alternativen bestehen nicht.

2. Verhältnis zur Planung

Das Vorhaben ist im Legislaturplan 2025-2029 nicht enthalten, ebenso nicht im IAFP 2026-2029.

3. Auswirkungen

3.1 Personelle und finanzielle Konsequenzen

Bei der kantonalen Verwaltung und den Gerichten haben die Bereiche Datenschutz und Datensicherheit bzw. Informationssicherheit im Allgemeinen bereits in den letzten Jahren stark an Bedeutung gewonnen und es besteht generell Nachholbedarf, was auch durch die digitale Transformation bedingt ist. Dadurch fällt ein nur schwer bezifferbarer Mehraufwand an, welcher mit erhöhten (personellen und finanziellen) Ressourcen einhergeht. Als grobe Schätzung wird grundsätzlich von einem Mehraufwand von 20 Stellenprozenten bei jedem Departement sowie

der Staatskanzlei und den Gerichten ausgegangen, ohne Einrechnung der zu ernennenden Datenschutzberaterinnen bzw. -berater und der aktualisierten Aufgaben der bzw. des IDSB (s. nachfolgend). Dies ergibt ein zusätzliches Stellenpensum von 140 Prozent.

Nach § 33ter InfoDG müssen Strafverfolgungs-, Strafgerichts- und Strafvollzugsbehörden eine Datenschutzberaterin bzw. einen Datenschutzberater ernennen. Soweit noch nicht erfolgt, wird dies bei der Gerichtsverwaltung, der Staats- sowie der Jugendanwaltschaft, der Polizei des Kantons Solothurn und dem Amt für Justizvollzug einen entsprechenden Ressourcenausbau zur Folge haben. Bei der Polizei Kanton Solothurn besteht dafür ein zusätzlicher Pensenbedarf von ca. 50 bis 60 %. Für die Staats- und Jugendanwaltschaft wird dieser auf 20 bis 50 % geschätzt. Das Amt für Justizvollzug schätzt den Bedarf auf ein Pensum von 50 bis 60 %. Die Gerichtsverwaltung verfügt bereits über eine Datenschutz- und Informationssicherheitsberaterin (100 %-Pensum). Dies ergibt zusammen ein zusätzliches Stellenpensum von 120 bis 170 Prozent.

Der Aufgabenkatalog der bzw. des IDSB wird aktualisiert. Bei einigen Anpassungen handelt es sich nicht um materielle Änderungen. Sie haben keine unmittelbaren finanziellen Auswirkungen. Dies betrifft insbesondere § 32 Absatz 1 Buchstabe b InfoDG (Beratung, Unterstützung, Schulung und Sensibilisierung), Buchstabe i (Zusammenarbeit mit anderen Behörden) und Buchstabe k (Behandlung von aufsichtsrechtlichen Anzeigen). Ein Mehraufwand wird bei der bzw. dem IDSB hingegen aufgrund von neuen Aufgaben entstehen: Neu können auch die von Zugangsgesuchen betroffenen Dritten ein Schlichtungsverfahren beantragen (§ 36 Abs. 1bis InfoDG). Die Anzahl der Schlichtungsverfahren wird sich daher erhöhen. Neu prüft die bzw. der IDSB ausserdem im Rahmen der Vorabkontrollen die von den Behörden erarbeiteten Datenschutz-Folgenabschätzungen (§ 32 Bst. h InfoDG), woraus sich ebenfalls ein Mehraufwand ergibt. Weiter nimmt die bzw. der IDSB neu die Meldungen von Datensicherheitsvorfällen entgegen und behandelt sie (§ 32 Abs. 1 Bst. j InfoDG). Ein Mehraufwand wird sich durch die weitergehende materielle Behandlung der Meldungen ergeben. Die bzw. der IDSB wird insbesondere prüfen müssen, ob die Behörden die betroffenen Personen informiert haben, soweit dies notwendig ist. Es ist zudem damit zu rechnen, dass sich aufgrund der neuen Meldepflicht von Datensicherheitsvorfällen der aufsichtsrechtliche Handlungsbedarf deutlicher und dringender zeigen wird. Ein Mehraufwand wird sich bei der bzw. dem IDSB schliesslich auch durch die indirekten Auswirkungen der Gesetzesrevision ergeben. Weil den Behörden neue Aufgaben übertragen werden, wird der Beratungs-, Unterstützungs- und Schulungsaufwand grösser werden. Die IDSB rechnet daher damit, dass aufgrund der direkten und indirekten Auswirkungen der Gesetzesrevision zusätzlich 60 bis 100 Stellenprozente (Juristin oder Jurist) erforderlich werden, um die beabsichtigte Wirkung der Gesetzesrevision sicherstellen zu können.

Insgesamt wird der personelle Mehraufwand somit grob auf 320 bis 410 Stellenprozente geschätzt. Bei Zugrundelegung einer Juristenstelle mit Lohnklasse 21 und mittlerer Erfahrungsstufe 10 wird dieser zusätzliche Besoldungsaufwand (inkl. Sozialversicherungsbeiträgen des Arbeitgebers) auf rund CHF 480'000 bis CHF 615'000 grob geschätzt. Die Kosten für eine allfällige Applikation zur Veröffentlichung der Register der Bearbeitungstätigkeiten können noch nicht abgeschätzt werden.

3.2 Vollzugsmassnahmen

Die Änderungen auf Gesetzesstufe haben Anpassungen im Verordnungsrecht, insbesondere in der InfoDV zur Folge und werden sich auf verwaltungsinterne Vorgaben auswirken (z.B. Konzept Informationssicherheit der kantonalen Verwaltung gem. RRB Nr. 2020/1659).

3.3 Folgen für die Gemeinden

Für die Gemeinden hat die Vorlage nur geringe Auswirkungen.

Die in § 30bis InfoDG neu vorgesehene Datenschutz-Folgenabschätzung wird bei entsprechenden Projekten von den Gemeinden vorgenommen werden müssen.

Nach § 33ter InfoDG müssen Strafverfolgungs-, Strafgerichts- und Strafvollzugsbehörden eine Datenschutzberaterin bzw. einen Datenschutzberater ernennen. Auch für die Stadtpolizei der Einwohnergemeinde der Stadt Solothurn wird eine solche Ernennung nötig sein.

4. Erläuterungen zu einzelnen Bestimmungen der Vorlage

4.1 Informations- und Datenschutzgesetz (InfoDG; BGS 114.1)

§ 2 (Geltungsbereich)
Das InfoDG definiert in § 2 jeweils für das Öffentlichkeitsprinzip (Abs. 2) und den Datenschutz (Abs. 3) den Geltungsbereich. Eine Anpassung erfolgt beim Geltungsbereich für den Datenschutz (§ 2 Abs. 3 Bst. c InfoDG). Das europäische Recht sieht keine allgemeine Ausnahme vom Geltungsbereich für hängige Straf-, Zivil- und verwaltungsrechtliche Klage-, Beschwerde- und Einspracheverfahren vor. In diesen Bereichen kommen jedoch die anwendbaren Verfahrensgesetze als bereichsspezifisches Datenschutzrecht zur Anwendung, soweit es um die (Datenschutz-)Rechte der betroffenen Personen, namentlich der Verfahrensparteien, geht. Hier ist vor allem das Einsichtsrecht relevant, aber etwa auch das Berichtigungs- und Löschungsrecht (s. Titel 5.4 InfoDG). Beispielsweise richtet sich das Einsichtsrecht der Parteien im Strafverfahren nach Artikel 101 der Schweizerischen Strafprozessordnung (StPO; SR 312.0) und zwar abschliessend (bzw. ausschliesslich). Subsidiär, also wenn das Verfahrensgesetz keine Regelung enthält (weder ausdrücklich noch durch qualifiziertes Schweigen), kommt auf die Rechte der Betroffenen das InfoDG zur Anwendung. Soweit es nicht um die Rechte der Betroffenen geht, ist das InfoDG neu auch in hängigen Verfahren anwendbar, etwa in Bezug auf die Datenschutzgrundsätze und die Datensicherheit (§ 16 InfoDG). Soweit Spezialerlasse inhaltlich weitergehende Bestimmungen zu Datenschutz und Datensicherheit enthalten, gehen diese den allgemeinen Bestimmungen des InfoDG als lex specialis vor. Nach dem Abschluss eines Verfahrens richten sich die Rechte nach dem InfoDG. Die gewählte Lösung entspricht dem europäischen Rechtsrahmen. Der Bund und die anderen Kantone haben ähnliche Regelungen zum Geltungsbereich erlassen (z.B. Art. 2 Abs. 3 DSG, § 2 Abs. 2bis IDAG-AG und § 2 Abs. 2bis IDG-BL).

§ 6 (weitere Begriffe)
<u>Besonders schützenswerte Personendaten (Abs. 3):</u>
Das europäische Recht sowie das DSG nehmen neu genetische und biometrische Daten in den Katalog der besonders schützenswerten Personendaten auf. Auch im InfoDG soll der Katalog der besonders schützenswerten Personendaten entsprechend erweitert werden. Genetische Daten sind Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden; darin eingeschlossen ist auch das DNA-Profil. Bei biometrischen Daten handelt es sich um durch spezielle technische Verfahren gewonnene Personendaten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen.[1]

Diese Änderung ist aufgrund von Artikel 10 Richtlinie sowie Artikel 6 Absatz 1 SEV 108+ erforderlich. Der Bund (Art. 5 Bst. c Ziff. 3 und 4 DSG) und die Mehrheit der Kantone, die ihre Revisionsarbeiten abgeschlossen haben, haben diese Anpassung vorgenommen (z.B. die Kantone AI [Art. 3 Abs. 6 Bst. d DIAG-AI], BL [§ 3 Abs. 4 Ziff. 2 und 5 IDG-BL], BS [§ 3 Abs. 4 Ziff. 2 und 5 IDG-BS], SG [Art. 1 Abs. 1 Bst. b Ziff. 2bis und 2ter DSG-SG], SH [Art. 2 Abs. 1 Bst. d Ziff. 5 und 6 DSG-SH] und ZH [§ 3 Abs. 4 Ziff. 2 IDG-ZH]). Hingegen wurde der Katalog der besonders schützenswerten Personendaten von anderen Kantonen (wie z.B. den Kantonen AG, GL, GR, NW, TI und VD) bis anhin noch nicht mit den genetischen und biometrischen Daten ergänzt.

[1] Vgl. Botschaft nDSG, 7020.

Im Rahmen dieser Revision soll der Ausdruck «rassische Herkunft» aus § 6 InfoDG gestrichen werden. Diejenigen Daten, die als besonders schützenswert gelten sollen, sind bereits unter dem geltenden Recht vollumfänglich vom Begriff der «ethnischen Herkunft» erfasst, weshalb die Streichung keine materiellen Änderungen bewirkt. Die europäischen Rechtsgrundlagen sowie das DSG haben den Begriff der Rasse bzw. Rassenzugehörigkeit beibehalten. Demgegenüber empfiehlt der KdK-Leitfaden, auf diesen Begriff künftig zu verzichten (vgl. Ziff. 3.3 des KdK-Leitfadens). Dieser Empfehlung ist bislang die überwiegende Mehrheit der Kantone gefolgt, die ihre Datenschutzgesetze bereits revidiert haben (z.B. die Kantone AG, BL, OW, SG und SH). Soweit ersichtlich verwenden einzig die Kantone FR (Art. 4 Abs. 1 Bst. c Ziff. 2 LPrD-FR), UR (Art. 3 Bst. b Ziff. 2 KDSG-UR) und VS (Art. 3 Abs. 7 Bst. b LIPDA-VS) noch die Begrifflichkeit «Zugehörigkeit zu einer Rasse» in ihren datenschutzrechtlichen Bestimmungen.

Bezüglich der Qualifizierung von Ergebnissen eines Profilings als besonders schützenswerte Personendaten wird auf die nachfolgenden Ausführungen zum Begriff «Profiling» (Abs. 7) verwiesen.

Bearbeiten (Abs. 5):
Die Änderung ist redaktioneller Natur und dient dem besseren Verständnis der Norm. Es wird klargestellt, dass die praktisch wichtigen Anwendungsfälle des Speicherns und des Löschens ebenfalls Bearbeitungen im Sinne des InfoDG darstellen. Gleichzeitig werden gewisse praktisch nicht bedeutsame bzw. nicht mehr zeitgemässe Formulierungen gestrichen. Im Ergebnis entspricht die vorgeschlagene Aufzählung derjenigen im DSG (vgl. Art. 5 Bst. d DSG), bis auf den Anwendungsfall des «zugänglich Machens», der jedoch wichtig ist, weil er klarstellt, dass auch eine bloss «passive» Bekanntgabe von Personendaten eine Form der Bearbeitung darstellt.

Datensammlung (bisheriger Abs. 6):
Der Begriff der Datensammlung wurde im Laufe der Revision aus dem DSG gestrichen. Das DSG verwendet im Zusammenhang mit den Verzeichnissen neu den Begriff «Bearbeitungstätigkeiten». In Anlehnung an das DSG wird der Begriff «Datensammlung» auch im InfoDG nicht mehr verwendet und Absatz 6 wird aufgehoben. Im Zusammenhang mit den Verzeichnissen wird der Begriff «Bearbeitungstätigkeiten» verwendet.

Profiling (Abs. 7):
Die Richtlinie (Art. 3 Ziff. 4) und die DSGVO (Art. 4 Ziff. 4) haben den Begriff des Profilings eingeführt. Der Bund und bis anhin – soweit ersichtlich – alle Kantone haben diesen Begriff in ihre Datenschutzgesetze aufgenommen. Das Profiling wird von der geforderten Rechtsetzungsstufe her den besonders schützenswerten Personendaten gleichgestellt (vgl. unten, zu § 15 Abs. 2 InfoDG sowie Art. 34 Abs. 2 Bst. b DSG).

Beim Profiling handelt sich dabei jedoch nicht um eine Art von Daten, sondern um eine Art der Daten*bearbeitung.* Insofern ist das Profiling nicht deckungsgleich zum Persönlichkeitsprofil. Das Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine *Beurteilung* wesentlicher Aspekte der Persönlichkeit erlaubt (§ 6 Abs. 4 InfoDG). Beim Profiling werden aufgrund verschiedener Merkmale einer Person oder einer Gruppe Annahmen über deren Verhalten, Vorlieben, Fähigkeiten oder Bedürfnisse erstellt.[1] Es handelt sich beim Profiling mithin um einen dynamischen, automatisierten Auswertungsprozess.[2]

Der Wortlaut der vorgeschlagenen Legaldefinition ist an jenen im DSG (vgl. Art. 5 Bst. f DSG) angelehnt, wobei der schlankeren Systematik des InfoDG Rechnung getragen wird, ohne dass ein materieller Unterschied zum Begriff auf Bundesebene beabsichtigt wird. Eine ähnliche Regelung ist im KdK-Leitfaden (unter Ziff. 3.8) und in den Gesetzen diverser anderer Kantone enthalten. Die Einführung des Begriffs des Profilings und die Regelung der Anforderungen daran werden

[1] Eingehend dazu OLIVIER HEUBERGER, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, Zürich 2020, N 54 ff.
[2] Vgl. Botschaft nDSG, 7021 f.

von der Richtlinie und der DSGVO gefordert. Das europäische Recht kennt das Persönlichkeitsprofil nicht. Im DSG ist der Begriff des Persönlichkeitsprofils gestrichen worden. Bis anhin haben ungefähr die Hälfte aller Kantone (z.B. die Kantone AI, GL, OW, SZ, UR, ZG und ZH) den Begriff des Persönlichkeitsprofils aufgehoben. Einige Kantone, z.B. AR (Art. 2 Abs. 4 DIAG-AR) und BL (§ 3 Abs. 4 Bst. b IDG-BL), verwenden bzw. definieren den Begriff Persönlichkeitsprofil weiterhin in ihren datenschutzrechtlichen Erlassen. Weil sich die Begriffe «Persönlichkeitsprofil» und «Profiling» unterscheiden und unterschiedliche Anwendungsfälle haben, erscheint die Aufhebung des Begriffs «Persönlichkeitsprofil» nicht zweckmässig. In dieser Vorlage wird der Begriff des Persönlichkeitsprofils beibehalten (§ 6 Abs. 4 InfoDG).

Auftragsdatenbearbeiterin bzw. Auftragsdatenbearbeiter (Abs. 8):
Dieser Begriff ist ebenfalls vom europäischen Recht eingeführt (Art. 3 Ziff. 9 Richtlinie; Art. 4 Ziff. 8 DSGVO; Art. 2 Bst. f SEV 108+; Englisch: *processor*) und im DSG übernommen worden. In den meisten Konstellationen handelt es sich bei der Auftragsdatenbearbeiterin bzw. beim Auftragsdatenbearbeiter um die «Dritte» bzw. den «Dritten» im Sinne des geltenden § 17 InfoDG. Da es nicht bloss um die Bearbeitung eines Auftrages geht, sondern um die Bearbeitung *von Daten* im Auftrag einer Behörde, wird in Absatz 8 der Begriff der Auftrags*daten*bearbeiterin bzw. des Auftrags*daten*bearbeiters verwendet – und nicht wie in der Richtlinie[1] und im DSG der Begriff «Auftragsbearbeiter». Auch wird, wie im Kanton Solothurn in neueren Erlassen üblich, sowohl die weibliche als auch die männliche Form verwendet (anders als im DSG, das nur die männliche Form verwendet, etwa in Art. 5 Bst. k DSG). Namentlich die Kantone BL (§ 3 Abs. 8 IDG-BL) und ZG (§ 6 DSG-ZG) haben sich, in Anlehnung an den KdK-Leitfaden (vgl. dort Ziff. 3.10), ebenfalls für den Begriff «Auftragsdatenbearbeiterin» bzw. «Auftragsdatenbearbeiter» entschieden.

§ 15 (Rechtsgrundlage)
Absatz 2: Aufgrund der Anforderungen der Richtlinie (Art. 11) und der DSGVO (Art. 22) muss die Vornahme eines Profilings den gleichen strengeren Voraussetzungen wie die Bearbeitung von besonders schützenswerten Personendaten unterworfen werden.

Absatz 3: Dieser neue Absatz entspricht inhaltlich Artikel 34 Absatz 4 Buchstabe c DSG. Er ist, ähnlich einer polizeilichen Generalklausel, auf Ausnahmesituationen zugeschnitten, in denen Leib und Leben unmittelbar bedroht sind und aufgrund der zeitlichen Dringlichkeit die rechtzeitige Einholung einer Einwilligung sich als nicht möglich erweist. Zu denken ist etwa an die Übermittlung von Blutwerten eines bewusstlosen Unfallopfers oder an die Weitergabe von Gesundheitsdaten eines Kindes in Abwesenheit seiner Eltern.[2] In der Richtlinie (Art. 10 Bst. b) und der DSGVO (Art. 6 Abs. 1 Bst. d und Art. 9 Abs. 2 Bst. c) sind ebenfalls analoge Ausnahmetatbestände vorgesehen. Auf kantonaler Ebene kennt z.B. der Kanton SZ eine ähnliche Bestimmung (§ 9 Abs. 3 Bst. b ÖDSG-SZ).

Eine inhaltlich entsprechende Ausnahmebestimmung kennt das geltende Recht bereits in § 21bis Absatz 2 Buchstabe d InfoDG (grenzüberschreitende Bekanntgabe). Diese Vorschrift soll redaktionell an die neue Bestimmung angepasst werden, um einen inhaltlich identischen Schutzzweck zu gewährleisten (s. unten, zu § 21bis Abs. 2 Bst. d).

[1] Wobei anzumerken ist, dass Richtlinie und DSGVO stets von Daten*verarbeitung* und deshalb auch von Auftrags*verarbeiter* sprechen.
[2] Vgl. HORST HEBERLEIN, Beck Kurzkommentar DSGVO, Art. 6 N 18.

§ 16 (Grundsätze)

Datenschutz durch technische und organisatorische Massnahmen, datenschutzfreundliche Voreinstellungen und Datensicherheit

Die neuen europäischen Rechtsordnungen (Art. 4 Abs. 4 Richtlinie; Art. 5 Abs. 2 DSGVO; Art. 10 Abs. 1 SEV 108+) verlangen einen Nachweis, dass die für die Datenbearbeitung verantwortliche Behörde die Datenschutzvorschriften einhält. Viele Kantone sehen in Anlehnung an den KdK-Leitfaden in ihren Datenschutzgesetzen neu eine sog. Rechenschaftspflicht vor, so beispielsweise AG (§ 12 Abs. 2 IDAG-AG), BL (§ 6 Abs. 3 IDG-BL) und ZG (§ 5d Abs. 3 DSG-ZG). Einzelne Kantone sehen in ihren Gesetzen keine Rechenschaftspflicht vor, wohl aber eine Verpflichtung der Behörde, mit technischen und organisatorischen Massnahmen die Einhaltung des Datenschutzes sicherzustellen, so beispielsweise die Kantone ZH (§ 13 Abs. 1 IDG-ZH) und LU (§ 6 Abs. 1bis KDSG-LU). Der Bund hat die Rechenschaftspflicht nicht ins revidierte DSG übernommen. Er konstituiert jedoch die Pflicht zur Einhaltung des Datenschutzes durch technische und organisatorische Massnahmen und hat in Artikel 7 DSG die internationalen Anforderungen an den Datenschutz durch technische und organisatorische Massnahmen umgesetzt, wie sie sich aus Artikel 8bis Ziff. 3 SEV 108+, Artikel 20 Absatz 1 Richtlinie und Artikel 25 DSGVO ergeben.

Mit der Revision des InfoDG soll im kantonalen Recht ebenfalls keine Rechenschaftspflicht eingeführt, jedoch ähnlich wie in den Kantonen ZH und LU eine Pflicht zur Einhaltung des Datenschutzes mit technischen und organisatorischen Massnahmen festgehalten und konkretisiert werden. Nachweise, dass die Pflicht zur Sicherstellung des Datenschutzes durch technische und organisatorische Massnahmen der Datensicherheit erfüllt wird, können die Behörden insbesondere durch Konzepte und andere Führungsmittel erbringen, wie beispielsweise Zertifizierungen im Bereich Datenschutz und Datensicherheit, Informationssicherheits- und Datenschutzkonzepte (ISDS-Konzepte), spezifische Informatiksicherheits- und Zugriffskonzepte, allgemeine Organisationskonzepte, Datenschutzmanagementsysteme (DSMS) oder um Datenschutzaspekte angereicherte Informationssicherheits-Managementsysteme (ISMS). Damit werden auch die Vorgaben der europäischen Rechtsordnungen erfüllt.

Datensicherheit (Abs. 1 Bst. c):

Gegenüber dem bisherigen Text wird als Schutzziel nicht nur die Verhinderung eines unbefugten Bearbeitens festgehalten, sondern allgemein die Einhaltung der Datensicherheit in Abhängigkeit zu den Risiken bei der Datenbearbeitung als Schutzziel genannt. Die Datensicherheit konsolidiert die Anforderungen des Datenschutzes durch technische und organisatorische Massnahmen und zielt allgemein auf den Schutz und die Sicherheit der von den Behörden und Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeitern bearbeiteten Daten ab. Die Datensicherheit hat grundsätzlich die Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit bei der Datenbearbeitung zum Ziel. Der Umfang der technischen und organisatorischen Massnahmen richtet sich gemäss dem Prinzip der Angemessenheit nach dem Stand der Technik, der Art und dem Umfang der bearbeiteten Daten sowie dem Risiko, welches die Bearbeitung für die Grundrechte und Persönlichkeit der Betroffenen mit sich bringt. Der Regierungsrat kann die Vorgaben an die Datensicherheit in der InfoDV präzisieren.

Datenschutz durch technische und organisatorische Massnahmen und datenschutzfreundliche Voreinstellungen (Abs. 1 Bst. d):

Datenschutz durch technische und organisatorische Massnahmen beinhaltet eine grundsätzliche Pflicht der verantwortlichen Behörde. Sie muss ab dem Zeitpunkt der Planung, Auswahl und Entwicklung von Systemen, Anwendungen und Prozessen, mit welchen eine Datenbearbeitung erfolgt oder erfolgen soll, diese technisch und organisatorisch so ausgestalten, dass bei deren Anwendung ein Verstoss gegen Datenschutzvorschriften verunmöglicht oder zumindest das Risiko erheblich vermindert wird (sog. «privacy by design»).[1] Schutzzweck dieser Vorschrift ist die Einhaltung der Grund- und Persönlichkeitsrechte der Betroffenen durch entsprechende Vorkeh-

[1] Vgl. Botschaft nDSG, 7028 f.

rungen bei der Ausgestaltung der Datenbearbeitung. Dabei fallen insbesondere die Zweckbindung und Verhältnismässigkeit ins Gewicht. So kann beispielsweise durch Design und Umsetzung entsprechender Zugriffs- und Berechtigungskonzepte die Bearbeitung auf die notwendigen Funktionen eingeschränkt (Least Privilege) oder durch Festlegung von Fristen die Aufbewahrungsdauer sowie allfällige Pflichten zum Löschen oder Anonymisieren sichergestellt werden. Die Anforderungen an die technischen und organisatorischen Vorkehrungen, mit welchen der Datenschutz sichergestellt wird, müssen angemessen sein. Sie müssen sich insbesondere am Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko ausrichten, welches die Bearbeitung für die Grundrechte und Persönlichkeitsrechte der betroffenen Personen mit sich bringt.

Das Gebot zur Verwendung von datenschutzfreundlichen Voreinstellungen ergibt sich aus dem Grundsatz der Datenminimierung bzw. der Datensparsamkeit, welcher wiederum aus dem Prinzip der Verhältnismässigkeit (§ 16 Abs. 1 Bst. a InfoDG) abgeleitet werden kann. Datenbearbeitungen sind so auszugestalten, dass die Bearbeitung von Personendaten stets auf einem Mindestmass gehalten wird bzw. nicht mehr Personendaten bearbeitet werden, als wirklich zur Zweckerreichung erforderlich sind (sog. «privacy by default»).[1] Die datenschutzfreundliche Ausgestaltung von Voreinstellungen (z.B. in Bezug auf Softwarekonfigurationen oder Formularfelder) ist eine – nicht aber die einzige – Massnahme zur Datenminimierung. Alle IT-Anwendungen und jegliche Art von Datenerfassungen sind standardmässig so zu konfigurieren, dass möglichst wenige, bzw. ausschliesslich die funktional notwendigen Personendaten erhoben und bearbeitet werden.

§ 16bis (visuelle Überwachung)
Die IDSB rät den Behörden die Ausgestaltung einer Videoüberwachung in einem Betriebsreglement festzuhalten. Rechtlich handelt es sich um Weisungen. Solche Weisungen sind eine wichtige flankierende Massnahme zur Einhaltung des Datenschutzes bei Videoüberwachungen. Die vorliegende Revision bietet die Gelegenheit, die bereits angewendete Praxis rechtlich zu kodifizieren und somit die Rechtssicherheit zu stärken.

In den Weisungen sind alle wichtigen Aspekte in Bezug auf eine konkrete Videoüberwachung zu regeln, wie insbesondere die Bezeichnung der verantwortlichen Behörde (s. dazu unten, zu § 30^{quater} InfoDG), der konkrete Zweck der Überwachung, die räumliche und zeitliche Ausdehnung, die Art und Form der Überwachung, Hinweise zu den Rechten der betroffenen Personen und die Festlegung der angewendeten Massnahmen zur Gewährleistung der Datensicherheit. Die bzw. der IDSB kann Unterlagen wie ein Merkblatt oder eine Musterweisung zur Verfügung stellen.

Der Kanton BS (§ 18 IDG-BS) verlangt ebenfalls den Erlass eines Reglements im Zusammenhang mit Videoüberwachungsanlagen.

Diese Änderung gründet nicht auf Entwicklungen im übergeordneten Recht.

§ 16ter (Weitergabe visuell aufgezeichneter Daten)
In Absatz 1 wird eine redaktionelle Bereinigung vorgenommen («Behörden» statt «Amtsstellen»).

§ 16^{quater} (Pilotversuche)
Die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen bedarf gemäss geltendem Recht einer ausdrücklichen Grundlage in einem Gesetz im formellen Sinn oder muss zur Erfüllung einer in einem Gesetz im formellen Sinn klar umschriebenen Aufgabe unentbehrlich sein (§ 15 Abs. 2 Bst. a und b InfoDG). Die Einwilligung (§ 15 Abs. 2 Bst. d In-

[1] Vgl. Botschaft nDSG, 7030.

foDG) taugt nur im Einzelfall als Rechtsgrundlage. Die Konstellation, in der die betroffene Person die Daten allgemein bekanntgemacht hat (§ 15 Abs. 2 Bst. c InfoDG), ist von geringer Bedeutung. Oft ist es aufgrund der erheblichen Investitionen in die geplanten Datenbearbeitungen und der Schwierigkeit, im Voraus deren konkrete Ausgestaltung abzuschätzen, sinnvoll Pilotversuche durchzuführen, noch bevor die erforderlichen gesetzlichen Grundlagen geschaffen sind. Die vorgeschlagene Bestimmung lässt dies unter gewissen Voraussetzungen zu.

Voraussetzung ist zunächst, dass eine Vorabkonsultation (vgl. nachfolgend, zu § 30bis Abs. 4 und § 32 Abs. 1 Bst. h InfoDG) der bzw. des IDSB erfolgt ist (Abs. 1). Eine solche ist wegen der Sensibilität der anvisierten Datenbearbeitungen unentbehrlich. Sodann müssen die Aufgaben, die durch das geplante Vorhaben erfüllt werden sollen, in einem bereits in Kraft stehenden Gesetz im formellen Sinn umschrieben sein (Bst. a). Dabei wird es sich in der Regel um ein kantonales Gesetz handeln. Die Voraussetzung ist aber auch erfüllt, wenn die Aufgabe in einem Bundesgesetz geregelt ist und der Kanton sie umsetzen muss, eine kantonalgesetzliche Regelung aber noch aussteht. Ferner sind hinreichende Massnahmen zur Minimierung von (durch den Pilotversuch bewirkten) Grundrechtseingriffen zu ergreifen (Bst. b). Es ist hier etwa an anerkannte technische und organisatorische Massnahmen zur Gewährleistung der Informationssicherheit zu denken (z.B. Berechtigungskonzepte, Verschlüsselungen etc.). Schliesslich muss ein Pilotversuch für die Realisierung des Vorhabens unentbehrlich sein (Bst. c). Der Begriff «unentbehrlich» wird auf Verordnungsstufe weiter konkretisiert werden. Gemäss Artikel 32 DSV ist ein Pilotversuch unentbehrlich, wenn eine der folgenden, abschliessend aufgezählten Bedingungen erfüllt ist:

- Die Erfüllung einer Aufgabe erfordert technische Neuerungen, deren Auswirkungen zunächst evaluiert werden müssen.

- Die Erfüllung einer Aufgabe erfordert bedeutende organisatorische oder technische Massnahmen, deren Wirksamkeit zunächst geprüft werden muss, insbesondere bei der Zusammenarbeit zwischen Organen des Bundes und der Kantone.

- Die Erfüllung einer Aufgabe erfordert, dass die Personendaten im Abrufverfahren zugänglich sind.

Die Pilotversuche müssen nach einer gewissen Zeit evaluiert werden, damit rechtzeitig erkannt wird, ob sich das Vorhaben bewährt. Je nach Ergebnis der Evaluation ist das Vorhaben abzubrechen oder weiterzuentwickeln und die gesetzlichen Grundlagen sind zu schaffen. Um die demokratische Legitimation zu gewährleisten, sind Pilotversuche auf maximal fünf Jahre zu befristen (Abs. 2).

Die Gerichtsverwaltungskommission soll unter den gleichen Voraussetzungen Pilotversuche für die Gerichte, der Gemeinderat für die Gemeinde bewilligen können (Abs. 3).

Der Wortlaut der vorgeschlagenen Bestimmung orientiert sich weitestgehend an Artikel 35 DSG sowie an der vergleichbaren Bestimmung im Informations- und Datenschutzgesetz des Kantons BS (§ 9a IDG-BS). Diverse andere Kantone, namentlich die Kantone FR (Art. 22 DSchG-FR) und SG (Art. 16a DSG-SG), haben vergleichbare Bestimmungen in ihren Rechtsordnungen vorgesehen. Das europäische Recht regelt Pilotversuche in ähnlicher Weise.

§ 17 (Bearbeitung durch Auftragsdatenbearbeiterin bzw. Auftragsdatenbearbeiter)
Die Richtlinie (Art. 22 Abs. 3) und die DSGVO (Art. 28 Abs. 3) sehen vor, dass eine Datenbearbeitung durch Gesetz oder Vereinbarung an einen Dritten übertragen werden kann.

Für den Fall einer solchen Übertragung der Datenbearbeitung durch Vereinbarung, welche auch als Auslagerung oder Outsourcing bezeichnet wird, werden verbindliche Mindestvorgaben zu Datenschutz und Datensicherheit festgelegt, insbesondere hinsichtlich Wahrung der Rechte Betroffener sowie der Einhaltung angemessener technischer und organisatorischer Massnahmen.

Diese gesetzlich vorgesehenen Mindestanforderungen müssen im Rahmen einer vertraglichen Vereinbarung umgesetzt werden. Die insbesondere im InfoDG festgelegten Mindestvorgaben zum Inhalt und zur Umsetzung der Auftragsdatenbearbeitung können vom Regierungsrat auf Verordnungsstufe konkretisiert und erweitert werden.

Im Gesetz über die Auslagerung von Informatikdienstleistungen (Auslagerungsgesetz, AusG; BGS 114.5)[1] werden für die Behörden der kantonalen Verwaltung die Voraussetzungen, Zuständigkeiten und Verantwortlichkeiten für die Auslagerung von Informatikdienstleistungen geregelt. Die Bestimmungen des AusG gehen als lex specialis den Bestimmungen des InfoDG vor. Das InfoDG, insbesondere § 17 InfoDG, bleibt auch für die Behörden der kantonalen Verwaltung anwendbar, sofern sie Dienstleistungen, die nicht unter den Anwendungsbereich des AusG fallen, auslagern oder anderweitig Rechte und Pflichten nach InfoDG betroffen sind. Es ist geplant, den Geltungsbereich des AusG auf die Gemeinden und weitere Behörden im Sinne von § 3 InfoDG auszuweiten. Bis dies umgesetzt ist, werden die Anforderungen des europäischen Rechts an die Auftragsdatenbearbeitung für diese Behörden bereits mit dem Inkrafttreten der vorliegenden Änderung des InfoDG normiert. Ob § 17 InfoDG für die geplante Auslagerung auch tatsächlich eine genügende Rechtsgrundlage bildet, muss die Behörde im Einzelfall prüfen.

Die Änderungen in § 17 InfoDG sind aufgrund der Richtlinie und der DSGVO notwendig und wurden vom Bund und den meisten Kantonen bereits umgesetzt.

Absatz 1: Wie bereits oben zum Begriff der Auftragsdatenbearbeiterin bzw. des Auftragsdatenbearbeiters erläutert (vgl. oben, zu § 6 InfoDG), kennen die Richtlinie und die DSGVO die Rollen der bzw. des Verantwortlichen und der Auftragsdatenbearbeiterin bzw. des Auftragsdatenbearbeiters (vgl. auch unten, zu § 30^{quater} InfoDG). Das InfoDG spricht aktuell nur von Dritten, was unpräzise ist. Der neue Wortlaut stellt klar, dass eine Auftragsdatenbearbeiterin bzw. ein Auftragsdatenbearbeiter im Auftrag einer Behörde Daten bearbeitet. Es ist sicherzustellen, dass durch eine Auslagerung der Datenbearbeitung der Datenschutz und die Datensicherheit sowie insbesondere das Legalitätsprinzip und die Rechte der Betroffenen nicht beeinträchtigt werden. Betroffenen Personen darf durch die Auslagerung kein Nachteil entstehen. Deshalb präzisiert die vorgeschlagene Bestimmung die Mindestvorgaben der Auftragsdatenbearbeitung. Die Behörde muss insbesondere sicherstellen, dass die Auftragsdatenbearbeiterin bzw. der Auftragsdatenbearbeiter die übertragenen Daten nur so bearbeitet, wie sie selbst diese bearbeiten dürfte. Um dies zu gewährleisten, bieten sich in der Praxis vor allem sogenannte Auftragsdatenbearbeitungsvereinbarungen an, welche die Behörde mit der Auftragsdatenbearbeiterin bzw. dem Auftragsdatenbearbeiter abschliesst und i.d.R. vertraglich in die Dienstleistungsvereinbarung integriert sind. Darin werden konkret die Vorgaben und Rahmenbedingungen der Datenbearbeitung durch die Auftragsdatenbearbeiterin bzw. den Auftragsdatenbearbeiter festgelegt (u.a. auch die Nennung der Unterbeauftragten – s. Abs. 3).

Absatz 2: Die Anforderung, dass die Behörde sich zu vergewissern hat, dass die Auftragsdatenbearbeiterin bzw. der Auftragsdatenbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten, entspricht der Regelung in Artikel 9 Absatz 2 DSG. Mit dieser Vorschrift wird eine zu Artikel 55 OR analoge Pflicht der Behörde begründet, die Auftragsdatenbearbeiterin bzw. den Auftragsdatenbearbeiter sorgfältig auszuwählen, angemessen zu instruieren und so weit als nötig zu überwachen. Es handelt sich dabei einerseits um eine eigenständige Voraussetzung der Übertragung, mit welcher sichergestellt wird, dass nur Dienstleisterinnen und Dienstleister beauftragt werden dürfen, welche über die notwendigen Fähigkeiten, Kenntnisse und Ressourcen zur Gewährleistung der angemessenen Datensicherheit verfügen. Andererseits beinhaltet diese Vorgabe eine Instruktions- respektive Weisungs- und Kontrollpflicht der Behörde, welche sich über die gesamte Laufzeit der Datenbearbeitung erstreckt. Die Auftragsdatenbearbeiterin bzw. der Auftragsdatenbearbeiter kann sich dabei beispielsweise auf eine anerkannte Zertifizierung

[1] Botschaft und Entwurf des Regierungsrates an den Kantonsrat von Solothurn vom 12. November 2024, RRB Nr. 2024/1809.

entsprechend Artikel 13 DSG stützen und diese mit Angaben zu weiteren angemessenen technischen und organisatorischen Massnahmen der Datensicherheit ergänzen. Zusätzlich kommt im Rahmen der Überwachung insbesondere die Durchführung von Audits durch die Behörde oder einen hierfür beauftragten Dritten in Frage. Im Falle von Unterbeauftragungen (s. unten, zu Absatz 3) ist durch die Auftragsdatenbearbeiterin bzw. den Auftragsdatenbearbeiter sicherzustellen, dass die Kontrollrechte auf die Unterbeauftragte bzw. den Unterbeauftragten übertragen werden.

Absatz 3: Es ist von grosser Relevanz, dass die Behörde sämtliche Auftragsdatenbearbeiterinnen bzw. Auftragsdatenbearbeiter kennt, die Personendaten, welche in ihrer Verantwortung liegen, bearbeiten. Nur wenn die Behörde diese Kenntnis hat, kann sie eine risikobasierte Einschätzung zur Eignung für die entsprechende Datenbearbeitung vornehmen. Deshalb ist ihre vorgängige Kenntnis und schriftliche Zustimmung Voraussetzung für eine Delegation von Bearbeitungskompetenzen von einem Auftragsdatenbearbeiter an einen anderen (sog. Unterauftragsdatenbearbeiterinnen bzw. Unterauftragsdatenbearbeiter). Absatz 3 entspricht inhaltlich der Regelung in Artikel 9 Absatz 3 DSG.

§ 18 (Erheben von Daten)
Der Inhalt des bisherigen § 18 InfoDG wird neu in zwei Bestimmungen umschrieben. Die Informationspflicht wird im neuen § 18bis InfoDG geregelt (vgl. unten). Der bisherige § 18 InfoDG wird dadurch kürzer; materiell erfährt er keine Änderungen.

§ 18bis (Informationspflicht)
Leitlinien der Revisionen auf europäischer Ebene und Bundesebene waren namentlich die Schaffung von mehr Transparenz bei der Bearbeitung von Personendaten und die Stärkung der Rechte der betroffenen Personen.[1] Dies sind demnach die Grundgedanken der erweiterten Informationspflicht. Nur wer weiss, dass seine Personendaten bearbeitet werden und wie sie bearbeitet werden, ist tatsächlich in der Lage, gegebenenfalls seine Betroffenenrechte auszuüben. Vorgaben für die Informationspflicht ergeben sich aus dem europäischen Recht (Art. 13 Richtlinie; Art. 13 f. DSGVO; Art. 8 SEV 108+). Der KdK-Leitfaden sieht in Anlehnung an diese Vorgaben eine umfassende Informationspflicht mit restriktiven Ausnahmen vor. Die im KdK-Leitfaden vorgesehene Informationspflicht wurde von vielen Kantonen in ihren Datenschutzgesetzen übernommen (etwa die Kantone AG [§ 13 IDAG-AG], BL [§ 14 IDG-BL], SG [Art. 20a f. DSG-SG] und ZG [§ 6a f. DSG-ZG]). Im DSG wurde die Informationspflicht ebenfalls umfassender als bisher geregelt (Art. 19 f. DSG). Die Informationspflicht des DSG geht aber inhaltlich deutlich weniger weit als die Informationspflicht der DSGVO und beschränkt sich auf das Wesentliche.[2] Das DSG und der KdK-Leitfaden unterscheiden sich zudem bei einer für Behörden sehr wichtigen Ausnahme von der Informationspflicht: Während der KdK-Leitfaden die Behörden von der Informationspflicht nur befreit, wenn eine ausdrückliche gesetzliche Grundlage die Datenbearbeitung vorsieht, genügt es gemäss DSG bereits, wenn die Datenbearbeitung gesetzlich vorgesehen ist. Die Botschaft zum DSG hält bei den Erläuterungen zu dieser Ausnahme fest, dass Bundesorgane ohnehin nur Daten bearbeiten dürfen, wenn dafür eine gesetzliche Grundlage besteht. Gemäss dem Basler Kommentar hat die Ausnahme von Artikel 20 Absatz 1 Buchstabe b DSG zur Folge, dass die Informationspflicht bei Bundesorganen bei fast all ihren Datenbearbeitungen entfällt und nur zur Anwendung kommt, wenn Bundesorgane gemäss Artikel 34 Absatz 4 DSG ausnahmsweise ohne gesetzliche Grundlagen Daten bearbeiten.[3] Gemäss dem KdK-Leitfaden soll die Informationspflicht der Behörden hingegen nur dann wegfallen, wenn die betroffenen Personen aus den gesetzlichen Grundlagen mit hinreichender Präzision herauslesen können, welche Daten über sie zu welchem Zweck bearbeitet werden. Dies wäre bei den Datenbearbeitungen,

[1] Vgl. Botschaft nDSG, 6971.
[2] Vgl. CORRADO RAMPINI/PHILIPPE FUCHS/CHRISTIAN KUNZ, in: DAVID VASELLA/GABOR P. BLECHTA, BSK-DSG, Art. 19 N 4.
[3] Vgl. PHILIPPE FUCHS/CHRISTIAN KUNZ, in: BSK-DSG, DAVID VASELLA/GABOR P. BLECHTA, Art. 20 N 21 mit Verweis auf KURT PÄRLI/NATHALIE FLÜCK, in: BRUNO BAERISWYL/KURT PÄRLI/DOMINIKA BLONSKI, SHK DSG, Art. 20 N 8; a.A. ADRIAN BIERI/JULIAN POWELL, in: ADRIAN BIERI/JULIAN POWELL, OFK-DSG, Art. 20 N 12, wonach die Informationspflicht für Bundesorgane nur dann entfällt, wenn die entsprechende gesetzliche Bestimmung die gemäss Art. 19 DSG erforderliche Transparenz herzustellen vermag.

welche sich auf § 15 Absatz 1 Buchstabe b und § 15 Absatz 2 Buchstabe b InfoDG stützen, in aller Regel nicht der Fall. Der vorliegende Entwurf orientiert sich in Bezug auf die Informationspflicht am DSG, zumal bereits aus den öffentlich zugänglichen Verzeichnissen der Bearbeitungstätigkeiten gemäss § 24 InfoDG eine ausreichende Transparenz über die Datenbearbeitung geschaffen wird.

Bereits das geltende InfoDG kennt eine Informationspflicht (§ 18 Abs. 1 Satz 2 InfoDG). Hier wird diese Pflicht im Hinblick auf das europäische Recht konkretisiert. Die vorgeschlagene Regelung orientiert sich sprachlich eng an der Regelung des DSG. In den Absätzen 1 und 2 werden der Inhalt und der Umfang der Informationspflicht umschrieben und im folgenden Absatz 3 die Ausnahmen von der Informationspflicht. Von besonderer Bedeutung für die Behörde ist § 18bis Absatz 3 Buchstabe b InfoDG, wonach die Informationspflicht entfällt, wenn die Datenbearbeitung eine Grundlage in einem Gesetz oder in einer Verordnung hat. In allen Fällen, in welchen die Behörden Personendaten gestützt auf eine Rechtsgrundlage gemäss § 15 Absatz 1 Buchstabe a oder b bzw. gemäss § 15 Absatz 2 Buchstabe a oder b InfoDG bearbeiten, entfällt die Informationspflicht. Somit verbleibt die Informationspflicht faktisch vor allem in den Fällen, bei welchen die Behörden Personendaten gestützt auf eine Einwilligung gemäss § 15 Absatz 1 Buchstabe d oder § 15 Absatz 2 Buchstabe d InfoDG bearbeiten. Weil beim Einholen einer Einwilligung aber bereits heute über die wichtigsten Elemente der vorgesehenen Datenbearbeitung informiert werden muss, hat die neue Informationspflicht auch in diesen Fällen keine grossen Auswirkungen. Weil bereits heute über den Bearbeitungszweck und eine allfällige Weitergabe der Daten informiert werden muss, ist lediglich die Nennung der Kontaktdaten der Behörde neu. Von Bedeutung ist die Informationspflicht hingegen in den eher selten vorkommenden Anwendungsfällen von § 15 Absatz 3 und § 21bis Absatz 2 Buchstabe d InfoDG. In diesen Fällen muss die betroffene Person über die Datenbearbeitung informiert werden. Meistens wird es sich um eine Informationspflicht gemäss § 18bis Absatz 2 handeln.

In § 18bis Absatz 4 InfoDG werden in Anlehnung an Artikel 20 Absatz 3 DSG weitere Ausnahmen von der Informationspflicht aufgeführt. Die Wahrung der öffentlichen Sicherheit kann unter Umständen als wichtiges öffentliches Interesse zu einer Einschränkung der Informationspflicht führen. Ebenso ist es möglich, dass die Gefährdung einer Ermittlung, einer Untersuchung oder die Gefährdung eines behördlichen Verfahrens die Informationspflicht einschränken kann.

Auch wenn sich aus § 18bis InfoDG für Behörden in den wenigsten Fällen eine direkte Informationspflicht ergibt, werden Behörden künftig wohl immer häufiger auf freiwilliger Basis aus Transparenzgründen in sogenannten Datenschutzerklärungen über ihre Datenbearbeitungen informieren.

§ 18ter (Informationspflicht bei automatisierten Einzelentscheidungen)
Neu wird eine Informationspflicht bei automatisierten Einzelentscheidungen vorgesehen. Die Bestimmung ist sprachlich und inhaltlich an Artikel 21 DSG angelehnt. Dieser bezweckt, die Anforderungen der Richtlinie (Art. 11) und der SEV 108+ (Art. 9 Abs. 1 Bst. a) zu erfüllen.[1] Die DSGVO kennt eine ähnliche Bestimmung (Art. 22). Der Begriff der automatisierten Einzelentscheidung wird in § 18ter InfoDG gleich wie im DSG umschrieben: Automatisiert ist eine Entscheidung dann, wenn sie ausschliesslich auf einer automatisierten Bearbeitung beruht. Dies ist der Fall, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person vorgenommen werden. Automatisierte Einzelentscheidungen fallen nur dann unter § 18ter InfoDG, wenn sie für die betroffene Person mit einer Rechtsfolge verbunden sind oder die betroffene Person erheblich beeinträchtigen. Bei der Auslegung des Begriffs wird man sich an der Praxis zu Artikel 21 DSG orientieren können. Als Beispiel für eine automatisierte Einzelentscheidung kann die im kantonalen Recht kürzlich eingeführte Veranlagung mithilfe von algorithmischen Systemen nach § 148bis des Gesetzes über die Staats- und Gemeindesteuern (Steuergesetz; BGS 614.11) genannt werden.

[1] Vgl. Botschaft nDSG, 7056.

Absatz 1 enthält eine Kennzeichnungspflicht und dient der Transparenz. Behörden müssen neu automatisierte Einzelentscheidungen als solche transparent ausweisen. Betroffene Personen sind darüber zu informieren, dass eine Entscheidung automatisiert, ohne Dazutun und ohne Überprüfung einer natürlichen Person, erfolgt.

Absatz 2: Kommen automatisierte Einzelentscheidungen zur Anwendung, so muss die Behörde sicherstellen, dass die verwendete Datengrundlage sowie das Verfahren korrekt sind. Dies ist periodisch zu überprüfen. Der Regierungsrat kann hierzu weitergehende Vorgaben im Rahmen der InfoDV regeln.

Absatz 3 sieht zwei Betroffenenrechte vor. Zunächst sollen betroffene Personen die Möglichkeit erhalten, ihren eigenen Standpunkt zur fraglichen automatisierten Einzelentscheidung darzulegen. Sie sollen insbesondere die Gelegenheit erhalten, ihre Ansicht zum Ergebnis der Entscheidung zu äussern. Es kann sinnvoll sein, dass die betroffene Person bereits vor der Entscheidung auf gewisse konkrete Umstände hinweisen kann, welche aus ihrer Sicht bei der automatisierten Entscheidung nicht ausreichend gewürdigt werden. Von grosser Bedeutung ist sodann das Recht der betroffenen Personen, die menschliche Überprüfung einer automatisierten Einzelentscheidung zu verlangen.

Absatz 4 stellt klar, dass die Vorgaben aus Absatz 3 nicht greifen, wenn der betroffenen Person vor dem Entscheid das rechtliche Gehör nicht gewährt werden muss. In welchen Konstellationen dies der Fall ist, ergibt sich aus § 23 Absatz 3 des Gesetzes über den Rechtsschutz in Verwaltungssachen (Verwaltungsrechtspflegegesetz; BGS 124.11) und aus weiteren Gesetzen. Beispielsweise ist im Verfahren der Steuerveranlagung kein Recht auf vorgängige Anhörung vorgesehen. Diese Einschränkung des rechtlichen Gehörs wird durch die in diesem Massenverfahren bestehende Einsprachemöglichkeit (§ 149 Steuergesetz) kompensiert.

§ 21 Absatz 3 (Abrufverfahren); aufgehoben
Die gesetzliche Grundlage für das «Abrufverfahren» gemäss Absatz 3 kann gleich wie auf Bundesebene (Art. 36 DSG) aufgehoben werden. Diese Änderung führt nicht zu einer Schwächung des Schutzes der Personendaten, denn die Bekanntgabe muss weiterhin stets im Rahmen der gesetzlichen Datenschutzvorschriften erfolgen.

§ 21 Absatz 6 (Schutzfristen)
§ 25 Absatz 2 des Gesundheitsgesetzes (GesG; BGS 811.11) sieht vor, dass Einrichtungen des Gesundheitswesens mit öffentlichen Aufgaben Patientendokumentationen nach Ablauf der Aufbewahrungsfristen den zuständigen Archiven anbieten müssen und diesbezüglich vom Berufsgeheimnis entbunden sind. Der Regierungsrat wies in der Botschaft zur Totalrevision des Gesundheitsgesetzes darauf hin, dass im Rahmen der anstehenden Revision des InfoDG geprüft werden müsse, wie die Persönlichkeitsrechte der betroffenen Personen zusätzlich geschützt werden.[1] Er wies darauf hin, dass dies insbesondere auch durch eine Verlängerung der in § 21 Absatz 5 InfoDG vorgesehenen Schutzfristen denkbar sei. Es erscheint sachgerecht, für Daten, die einem Berufsgeheimnis nach Artikel 321 des Schweizerischen Strafgesetzbuches (StGB; SR 311.0) oder § 16 GesG unterstehen, die Schutzfristen um 30 Jahre zu verlängern. Von den verlängerten Schutzfristen sind insbesondere die Patientenakten der Solothurner Spitäler AG (soH) betroffen. Es erschiene stossend, wenn diese Akten bereits 30 Jahre nach dem Tod der Patientin oder des Patienten keinem Schutz mehr unterliegen würden und deshalb öffentlich werden könnten. Die in Absatz 6 neu vorgesehene Schutzfrist beträgt 60 Jahre seit dem Tod, 140 Jahre seit der Geburt bzw. 110 Jahre seit der letzten Aufzeichnung, wenn weder der Todes- noch der Geburtstag bekannt ist. Diese Regelung ist vergleichbar mit den Regelungen anderer Kantone, welche verlängerte Schutzfristen im Zusammenhang mit Berufsgeheimnissen kennen (ZH: 120 Jahre; TG: 100 Jahre nach Dossierschluss). Die Einsichtgewährung in Patientendokumentationen während der Schutzfrist erfordert eine Entbindung vom Berufsgeheimnis (§ 16 Abs. 2 GesG).

[1] Totalrevision des Gesundheitsgesetzes und Änderung des Gebührentarifs, Botschaft und Entwurf des Regierungsrates an den Kantonsrat von Solothurn vom 29. Mai 2018, RRB Nr. 2018/820, S. 37.

§ 21bis Grenzüberschreitende Bekanntgabe
Die Anpassung ist primär redaktioneller Natur. § 21bis Absatz 2 Buchstabe d InfoDG sieht bereits heute vor, dass eine Bekanntgabe auch in einen Drittstaat ohne angemessenes Datenschutzniveau erfolgen darf, wenn die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen. Im Zuge der Einführung der neuen Rechtsgrundlage in § 15 Absatz 3 InfoDG soll sichergestellt werden, dass der Schutzumfang bei einer Auslandbekanntgabe nebst der betroffenen Person auch Drittpersonen umfasst, soweit innerhalb einer angemessenen Frist keine Einwilligung eingeholt werden kann. Damit wird eine inhaltlich analoge Regelung zum Bundesrecht sichergestellt, welche eine entsprechende Auslandbekanntgabe in Artikel 17 Absatz 1 Buchstabe d DSG vorsieht.

§ 24 (Verzeichnis der Bearbeitungstätigkeiten)
Absatz 1: Die Behörden müssen nach dem geltenden Recht Verzeichnisse über ihre Datensammlungen erstellen. Anstelle des bisherigen Begriffs «Datensammlung» wird in Anlehnung an die Terminologie des DSG neu der Begriff «Bearbeitungstätigkeiten» verwendet. Zu den Bearbeitungstätigkeiten zählen alle Bearbeitungen von Personendaten, welche für die Erfüllung des gesetzlichen Auftrags erforderlich sind (zum Beispiel Prüfung eines Baugesuchs und Erteilung einer Baubewilligung, Prüfung der Steuerklärung und Erstellung der Steuerveranlagung, Führung des Einwohnerregisters, Unterricht an Schulen, Behandlung von Patienten durch die Spitex), die Bearbeitungen von Daten, welche indirekt für die Erfüllung des gesetzlichen Auftrags erforderlich sind (zum Beispiel Personaladministration, Rechnungswesen, Betrieb einer Website, allfälliger Betrieb einer Videoüberwachung) sowie die Bearbeitung von Personendaten, welche aufgrund einer Einwilligung erfolgen (zum Beispiel Versand eines Newsletters). Mit der Pflicht zur Führung von Verzeichnissen der Bearbeitungstätigkeiten wird das europäische Recht nachvollzogen (Art. 24 Richtlinie sowie Art. 30 DSGVO).

Da die Behörden ihre Verzeichnisse dem oder der Beauftragten melden müssen und diese oder dieser sie neu publizieren muss, kann das im bisherigen Absatz 1 festgehaltene Einsichtsrecht aufgehoben werden.

Absatz 2: Die im Verzeichnis aufgeführten Angaben korrelieren im Wesentlichen mit denjenigen Angaben, die den betroffenen Personen aufgrund der Informationspflicht (vgl. oben, zu § 18bis InfoDG) und des Auskunftsrechts (§ 26 InfoDG) zustehen. Das Verzeichnis soll eine generelle Umschreibung der Datenbearbeitungstätigkeiten sein, woraus Art und Umfang ersichtlich werden. Das Verzeichnis ist insofern ein Mittel zur Datenschutz-Compliance.[1] Buchstabe d kann entsprechend den Bestimmungen auf europäischer Ebene und im DSG dahingehend vereinfacht werden, dass die Kategorien von Empfängerinnen bzw. Empfängern im Verzeichnis aufzuführen sind, denen Daten bekanntgegeben werden. Durch die Verwendung der Bezeichnung «Empfänger» wird die Bestimmung an die Informationspflicht (vgl. oben, zu § 18bisAbs. 1 Bst. c InfoDG) und an die Terminologie des DSG angeglichen. Aufzunehmen ist – wiederum in Anlehnung an das europäische Recht und an das DSG – auch eine Pflicht zur Nennung der Aufbewahrungsdauer von bearbeiteten Daten (Bst. e). Wenn die Aufbewahrungsdauer nicht genau definiert werden kann, muss das Verzeichnis zumindest die Kriterien enthalten, nach denen die Aufbewahrungsdauer festgelegt wird.[2] In Bezug auf die Form der Verzeichnisse werden keine gesetzlichen Vorgaben gemacht. Es wird im Gesetz auch nicht geregelt, wie die Gesamtheit aller Bearbeitungstätigkeiten einer Behörde zum Zweck des Verzeichnisses aufgesplittet werden muss. Die Behörden können selbst entscheiden, ob sie sich beim Erstellen der Verzeichnisse an den einzelnen (Fach-)Applikationen, an den sachlich zusammenhängenden Datenbearbeitungen oder an anderen Kriterien orientieren wollen.

Absatz 4: Das Verzeichnis dient auch der Herstellung von Transparenz gegenüber den Bürgerinnen und Bürgern. Dies wird so umgesetzt wie auf Bundesebene (Art. 12 und 56 DSG), nämlich

[1] Vgl. DAVID ROSENTHAL, Das neue Datenschutzgesetz, Jusletter vom 16. November 2020, N 144.
[2] Vgl. Botschaft nDSG, 7036.

indem die Behörden ihrer Verzeichnisse dem oder der Beauftragten melden und diese oder dieser sie publiziert (s. unten, zu § 25). Die Verzeichnisse der Auftragsdatenbearbeiterinnen und -bearbeiter sind hingegen – wie auf Bundesebene – nicht zu melden und zu publizieren, müssen jedoch der oder dem Beauftragten auf Anfrage zur Verfügung gestellt werden (Art. 24 Abs. 3 Richtlinie; Art. 30 Abs. 4 DSGV).

§ 25 (Register)
Die Regelung entspricht Artikel 56 DSG (s. oben, zu § 24).

§ 26 (Auskunft und Einsicht)
Die Änderung ist rein redaktioneller Natur und trägt der Aufhebung des Begriffes «Datensammlung» Rechnung (vgl. oben, zu § 6 Abs. 6 InfoDG).

§ 28 (Rechtsansprüche) und § 29 (Unterlassen, Beseitigen, Feststellen); aufgehoben
Das europäische Recht verlangt, dass das Recht von betroffenen Personen auf Löschung oder Vernichtung ihrer Daten explizit gesetzlich verankert wird. Ein solcher Anspruch wird bereits heute von der Rechtsprechung und Lehre anerkannt.[1] Dieser Anspruch soll neu auch im InfoDG ausdrücklich festgehalten werden. Als gelöscht gelten Daten, wenn sie keine Personendaten mehr darstellen, d.h. sobald entweder keine Mittel zur Wiederherstellung des Personenbezuges bestehen oder der Einsatz solcher Mittel für diejenigen Personen, die Zugang zu den Daten haben, einen unverhältnismässigen Aufwand erfordern würde.[2] Die Löschung von Daten lässt sich beispielweise durch deren Anonymisierung erreichen. Vernichten ist als Steigerung der Löschung zu verstehen und impliziert die unwiederbringliche Zerstörung der Daten.[3]

Der Bund (Art. 41 Abs. 2 Bst. a DSG) und zahlreiche Kantone (z.B. die Kantone AG [§ 28 Abs. 1 Bst. a IDAG-AG], SG [Art. 20 Abs. 2 Bst. a DSG-SG] und VS [Art. 33 Abs. 1 Bst. a GIDA-VS]) haben das Recht auf Löschung oder Vernichtung explizit gesetzlich normiert.

Die Ansprüche auf Löschung und Vernichtung verkörpern das sogenannte Recht auf Vergessenwerden.[4] Dieses gilt indessen nicht absolut. Vielmehr ist das Interesse am Persönlichkeitsschutz der betroffenen Person gegen das öffentliche Interesse an der Meinungs- und Informationsfreiheit abzuwägen.[5] Zudem können gesetzliche Dokumentations- und Aufbewahrungspflichten dem Recht auf Löschung und Vernichtung vorgehen (s. z.B. § 30 InfoDG, nachfolgend).

Da es nicht zweckmässig erscheint, den Anspruch auf Berichtigung von den anderen Ansprüchen getrennt zu behandeln, werden §§ 28 und 29 InfoDG in eine einzige Bestimmung vereinigt. Diese Änderung vereinfacht die Rechtsansprüche und führt so zu mehr Klarheit und Kohärenz.

§ 30 (Archivierte und für die Archivierung bestimmte Personendaten)
Absatz 1: Die Änderung steht im Zusammenhang mit § 28 InfoDG (s. oben). Mit der expliziten Aufnahme des Löschungs- und Vernichtungsrechts in § 28 InfoDG wird klargestellt, dass sich diese Ansprüche – gleich wie jene auf Sperrung und Berichtigung – nicht auf archivierte Personendaten erstrecken.

Absatz 2 ist neu und bezieht sich auf Personendaten, die zur Ablieferung an das Staatsarchiv bestimmt sind, diesem jedoch noch nicht abgeliefert worden sind. Er greift erst, wenn die einschlägigen Aufbewahrungsfristen für die archivbestimmten Daten abgelaufen sind. Die Aufbewahrungsfristen können sich aus § 19 InfoDG oder aus Spezialerlassen ergeben, wie beispielsweise aus Artikel 958f Absatz 1 des Obligationenrechts (OR; SR 220) oder § 18 Absatz 3 GesG bzw. § 15 der Vollzugsverordnung zum Gesundheitsgesetz (GesV; BGS 811.12). Absatz 2 bezieht sich nicht

[1] Vgl. CAMILLE DUBOIS/BETTINA BACHER, Zum Stand der Revision des Datenschutzgesetzes, in: ASTRID EPINEY/DANIELA NÜESCH, Die Revision des Datenschutzes in Europa und die Schweiz, S. 129 ff. und S. 142 m.w.H.
[2] Ausführlich DAVID ROSENTHAL, Löschen oder doch nicht löschen, digma 2019, S. 190 ff. und S. 192.
[3] Vgl. Botschaft nDSG, 7021.
[4] Vgl. Urteil des EuGH vom 13. Mai 2014, Rs. C-131/12 («Google Spain»).
[5] Vgl. Botschaft nDSG, 7077.

auf alle Dokumente, welche dem Staatsarchiv gemäss § 8 Absatz 2 des Archivgesetzes (BGS 122.51) angeboten werden müssen, sondern nur auf jene, für welche bereits eine Abgabe gemäss § 8 Absatz 4 Archivgesetz vereinbart worden ist. Die abzugebenden Dokumente und die Aufbewahrungsfristen werden in den Registraturplänen (§ 1 Abs. 2 Bst. b der Archivverordnung [ArchivVO; BGS 122.511]) aufgeführt. Die Registraturpläne bilden die Grundlage für die Archivierung der Dokumente im Staatsarchiv (§ 1 Abs. 1 ArchivVO) und sind integrierender Bestandteil der Schriftgutvereinbarung. Die abzugebenden Dokumente müssen in diesen Dokumenten genügend klar umschrieben sein. Wenn vereinbart wurde, dass eine bestimmte Auswahl an Dokumenten bzw. Akten an das Staatsarchiv abzuliefern ist (z.B. jedes zehnte Dossier oder Zufallsauswahl), muss die konkrete Auswahl bereits vollzogen sein. Absatz 2 gilt nicht für die Gemeinden, denn diese liefern ihre Akten nicht an das Staatsarchiv ab, sondern organisieren ihr Archivwesen nach den Vorgaben des Gemeindegesetzes (GG; BGS 131.1) eigenständig.

Neuer Titel 5.5. Besondere Pflichten der Behörden
Die Bestimmungen zur Datenschutz-Folgenabschätzung, zur Meldung von Verletzungen der Datensicherheit sowie zur Verantwortung lassen sich nicht ohne Weiteres in die aktuelle Systematik des InfoDG einreihen. Es bietet sich an, hierfür einen eigenen Abschnitt im 5. Titel des Gesetzes einzufügen. Die vorgeschlagene Formulierung «Besondere Pflichten» zeugt davon, dass es sich bei den drei Bestimmungen keineswegs um die einzigen Pflichten handelt, die Behörden treffen.

§ 30bis (Datenschutz-Folgenabschätzung)
Das europäische Recht hat die Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung eingeführt (Art. 27 Richtlinie; Art. 35 DSGVO; Art. 10 Abs. 2 SEV 108+). Zweck der Datenschutz-Folgenabschätzung ist die frühzeitige Erkennung von Risiken für die Grundrechte der betroffenen Personen oder von Risiken, welche zu einem Vertrauensverlust in die Behörden führen können, die sich aus geplanten Datenbearbeitungen ergeben. Grundsätzlich handelt es sich demnach um eine Risikobewertung, wie sie auch in der Informationssicherheit bekannt ist, aber mit Fokus auf Personendaten. Nur wenn die Risiken einer geplanten Datenbearbeitung bekannt sind, können geeignete Massnahmen zur Risikominimierung ergriffen werden.

Die Richtlinie (Art. 27) und das DSG (Art. 22) sehen die Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung für Datenbearbeitungen vor, die voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen können. Gewisse Kantone, z.B. die Kantone AG (§ 17a Abs. 1 IDAG-AG) und SG (Art. 8a Abs. 1 DSG-SG), haben sich am Wortlaut des DSG orientiert. Andere Kantone verlangen in ihren revidierten Gesetzen in Anlehnung an SEV 108+, dass bei allen Datenbearbeitungen Datenschutz-Folgenabschätzungen vorgenommen werden müssen, darunter namentlich die Kantone ZH (§ 10 Abs. 1 IDG-ZH), BL (§ 11a Abs. 1 IDG-BL) und ZG (§ 7b Abs. 1 DSG-ZG). Der neue § 30bis InfoDG orientiert sich am Wortlaut von Artikel 22 DSG und begrenzt sich damit auf Datenbearbeitungen, welche voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der Betroffenen mit sich bringen.

Absatz 1: Ob voraussichtlich ein hohes Risiko vorliegt, ermittelt die Behörde anhand der sogenannten Schwellwertanalyse. Dabei handelt es sich um ein Instrument, welches auf relativ einfache Weise eine schnelle Einschätzung des Risikos ermöglicht. Die bzw. der IDSB kann dazu Vorlagen und Muster zur Verfügung stellen. Die Datenschutz-Folgenabschätzung ist «vorgängig» durchzuführen, spätestens in der Initialisierungsphase einer geplanten Datenbearbeitung. Die Datenschutz-Folgenabschätzung stellt damit ein wichtiges Instrument zur Umsetzung der Grundsätze des Datenschutzes durch technische und organisatorische Massnahmen sowie der Verhältnismässigkeit dar.

Absatz 2: Der Begriff des hohen Risikos wird in Anlehnung ans DSG näher ausgeführt. Massgebend ist das Risiko, welches ohne Risikobehandlung z.B. durch risikominimierende Massnahmen besteht. Dieses Risiko wird auch als Bruttorisiko bezeichnet.

Absatz 3 regelt den Inhalt der Datenschutz-Folgenabschätzung.

Absatz 4: Die Datenschutz-Folgenabschätzung muss der bzw. dem IDSB zur Prüfung eingereicht werden (s. § 32 Abs. 1 Bst. h InfoDG). Es wird auf Verordnungsstufe zu bestimmen sein, wie lange die Datenschutz-Folgenabschätzung aufzubewahren ist (im Bund gilt gemäss Art. 14 DSV eine Aufbewahrungsfrist von 2 Jahren nach Beendigung der Datenbearbeitung).

§ 30ter (Meldung von Verletzungen der Datensicherheit)
Das europäische Recht führt eine Pflicht zur Meldung gewisser Verletzungen der Datensicherheit an die Datenschutzaufsichtsstelle ein (vgl. Art. 30 f. Richtlinie; Art. 33 ff. DSGVO; Art. 7 Abs. 2 SEV 108+).

Meldepflicht (Abs. 1):
Gemäss der Richtlinie (Art. 30) und der DSGVO (Art. 33) ist grundsätzlich jede Verletzung der Datensicherheit meldepflichtig, es sei denn, sie führe voraussichtlich zu keinem Risiko für die Grundrechte der betroffenen Personen. Der Bundesgesetzgeber ist diesem strengen Ansatz nicht vollständig gefolgt. Er unterstellt Verletzungen der Datensicherheit nur dann der Meldepflicht, wenn diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führen. Dies entspricht auch der SEV 108+. Bis anhin haben sich einige Kantone der strengeren Meldepflicht nach europäischem Vorbild angeschlossen (z.B. die Kantone AG [§ 17c Abs. 1 IDAG-AG], BL [§ 15a Abs. 2 IDG-BL] und SZ [§ 22a Abs. 1 ÖDSG-SZ]), wie sie auch im KdK-Leitfaden empfohlen wird (vgl. Ziff. 6.4 KdK-Leitfaden), während andere Kantone dem Ansatz des DSG gefolgt sind (darunter die Kantone FR [Art. 43 Abs. 3 DSchG-FR], LU [§ 7 Abs. 1 DSG-LU] und SG [Art. 9a DSG-SG]). Die in § 30ter InfoDG neu vorgesehene Meldepflicht lehnt sich eng an Artikel 24 DSG an. Behörden müssen Verletzungen der Datensicherheit der bzw. dem IDSB melden, wenn die Verletzung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Bagatellen sind nicht meldepflichtig.[1] Massgeblich für die Risikobeurteilung sind insbesondere die Art der Datensicherheitsverletzung, die Sensibilität und der Umfang der betroffenen Personendaten, die Anzahl und Kategorien betroffener Personen sowie die Schwere der Folgen für die betroffenen Personen.[2] Bei der Auslegung dieser Bestimmung wird man sich an der Praxis zu Artikel 24 DSG orientieren können. Die Meldepflicht besteht unabhängig von weiteren gesetzlichen oder organisatorischen Meldepflichten, beispielsweise an das Bundesamt für Cybersicherheit (BACS)[3] oder das Amt für Informatik und Organisation (AIO).

Verzichtet wird, wie der Bundesgesetzgeber und soweit ersichtlich bis anhin alle Kantone, auf eine konkrete Meldefrist. Die Richtlinie (Art. 30 Abs. 1) und die DSGVO (Art. 33 Abs. 1) sehen diesbezüglich zwar eine Frist von 72 Stunden vor, doch kann diese Frist mit hinreichender Begründung erstreckt werden. Im Ergebnis erscheint es sachgerechter, auf den Einzelfall abzustellen und festzulegen, dass die Meldung so rasch als möglich zu erfolgen hat. Der Regierungsrat kann weiterführende Vorgaben zur Dokumentation der Meldung in der Verordnung festlegen, insbesondere zur Aufbewahrungsdauer (im Bund gilt gemäss Art. 15 Abs. 4 DSV eine Aufbewahrungsfrist von 2 Jahren nach der Meldung).

Inhalt der Meldung (Abs. 2):
Absatz 2 definiert Mindestinhalte der Meldung. Ohne die genannten Informationen würde die Meldung in eine reine Formalität verfallen, ohne dass die bzw. der IDSB den Vorfall nachvollziehen und gegebenenfalls angemessene Massnahmen anordnen bzw. ergreifen könnte.

Der Wortlaut basiert auf der vergleichbaren Bestimmung in Artikel 24 Absatz 2 DSG.

---

[1] Ähnlich auch Botschaft nDSG, 7064.
[2] Vgl. dazu auch Europäischer Datenschutzausschuss (EDSA), Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäss der DSGVO, N 103 ff; Abrufbar unter: https://www.datenschutzstelle.li/application/files/3117/3099/1068/edpb_guidelines_202209_personal_data_breach_notification_v2.0_de_0.pdf
[3] Vgl. Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG; SR 128).

Verletzung der Datensicherheit (Abs. 3):
Für die Umschreibung der Verletzung der Datensicherheit wird die Legaldefinition des Bundes übernommen (vgl. Art. 5 Bst. h DSG). Der Tatbestand der Verletzung der Datensicherheit erfasst insbesondere den Verlust von Datenträgern, den Zugriff von unbefugten Dritten auf Informatiksysteme, die Einschränkungen der Verfügbarkeit von Daten aufgrund technischer Störungen sowie die Bekanntgabe von Daten an Unberechtigte.

Meldung durch die Auftragsdatenbearbeiterin bzw. den Auftragsdatenbearbeiter (Abs. 4):
Die Meldepflicht kann nur wirksam sein, wenn die Behörden tatsächlich Kenntnis von allfälligen Verletzungen der Datensicherheit haben. Deshalb ist wichtig, dass ihnen ihre Auftragsdatenbearbeiterinnen bzw. Auftragsdatenbearbeiter solche Verletzungen rasch melden. Das DSG sieht dazu vor, dass Auftragsdatenbearbeiterinnen bzw. Auftragsdatenbearbeiter der Behörde *jede* Verletzung der Datensicherheit ungeachtet des Risikos melden müssen. Dies ist auch der Mechanismus, den die Richtlinie und die DSGVO sowie zahlreiche Kantone gewählt haben. Ein solch strikter Ansatz vernachlässigt aber Sinn und Zweck der Meldepflicht – den Schutz der Grundrechte der betroffenen Personen – und ist wenig praktikabel. Denn es kommen durchaus auch Verletzungen der Datensicherheit vor, die offenkundig unbedeutend sind für die Grundrechte. Wenn etwa die Mitarbeitenden einer Auftragsbearbeiterin bzw. eines Auftragsdatenbearbeiters wegen einer technischen Störung während wenigen Minuten telefonisch nicht erreichbar sind und dieser Vorfall ohne weitere Folgen bleibt, liegt offensichtlich kein entsprechendes Risiko vor.

Information der betroffenen Personen (Abs. 5):
Das europäische Recht und das DSG sehen schliesslich vor, dass unter gewissen Umständen die betroffenen Personen selbst über die Verletzung der Datensicherheit zu informieren sind, sofern dies zu ihrem Schutz erforderlich ist oder durch die Datenschutzaufsichtsstelle angeordnet wird. Es geht etwa um Fälle, in denen die betroffenen Personen selbst Vorkehrungen treffen können, um das Risiko der Verletzung zu minimieren, z.B. durch die Änderung von Zugangsdaten und Passwörtern. Absatz 5 übernimmt diese Informationspflicht.

Die Aufnahme einer Bestimmung zur Meldung von Verletzungen der Datensicherheit wird vom europäischen Recht verlangt.

§ 30quater (Verantwortung)
Das europäische Recht sowie das DSG verlangen eine klare Zuordnung der Verantwortung, insbesondere bei gemeinsamen Datenbearbeitungen. Sie haben den Begriff des «Verantwortlichen» eingeführt (Art. 3 Ziff. 8 Richtlinie; Art. 4 Ziff. 7 DSGVO, Art. 2 Bst. d SEV 108+; Englisch: «controller»*;* Art. 5 Bst. j und Art. 33 DSG). Als «Verantwortlicher» wird dabei jene Person (oder Behörde) definiert, die über den Zweck und die Mittel der Datenbearbeitung entscheidet und somit auch primäre Ansprechperson für betroffene Personen ist, etwa zur Geltendmachung der Betroffenenrechte sowie weiterer Rechtsansprüche. Sie ist ebenfalls zuständig für die Einhaltung der besonderen Pflichten wie die Datenschutz-Folgenabschätzung und die Meldung von Verletzungen der Datensicherheit. Der «Verantwortliche» grenzt sich von der Auftragsdatenbearbeiterin bzw. vom Auftragsdatenbearbeiter ab. Zu beachten ist, dass als «Verantwortlicher» auf europäischer und auf Bundesebene auch Privatpersonen gelten können.

Verantwortliche Behörde (Abs. 1):
Im kantonalen Informations- und Datenschutzgesetz muss die Verantwortung aufgrund des Legalitätsprinzips hingegen daran anknüpfen, wer Trägerin der öffentlichen Aufgabe ist, deshalb die Personendaten zur Erfüllung ihrer gesetzlichen Aufgaben bearbeitet oder bearbeiten lässt und die Verfassungsmässigkeit der dazu erforderlichen Datenbearbeitungen verantwortet. Es handelt sich bei diesen ausschliesslich um Behörden i.S.v. § 3 InfoDG, welche von den Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeitern zu unterscheiden sind. Analog den europäischen und bundesrechtlichen Kriterien liegt die Verantwortung nicht nur dann bei einer Behörde, wenn sie allein über den Zweck und die Mittel der Bearbeitung entscheidet. Es reicht aus,

wenn die Entscheidung gemeinsam mit anderen getroffen werden kann. Ob der Zweck der Datenbearbeitung die Erfüllung von gesetzlichen oder vertraglichen Pflichten ist oder ob die Datenbearbeitung freiwillig erfolgt, ist für die Beurteilung, ob es sich um die verantwortliche Behörde handelt, nicht von Bedeutung[1]. Mit den Mitteln sind nicht die finanziellen Mittel gemeint, sondern die angewandten (z.B. technischen) Mittel.

Gemeinsame Bearbeitung (Abs. 2):
Erfolgt die Bearbeitung durch eine Behörde gemeinsam mit einer anderen Behörde, insbesondere durch gemeinsam verwendete Datenbanken oder Aufgabenteilungen, so sind die beteiligten Behörden verpflichtet, ihre jeweiligen Verantwortungsbereiche zu regeln und dies transparent auszuweisen. Damit werden Lücken in der Verantwortlichkeit vermieden und für die Betroffenen wird sichergestellt, dass sie ihre Rechte wahren können. Die Behörden müssen insbesondere festlegen, wer für die Pflichten gemäss §§ 30bis und 30ter InfoDG, die Datensicherheit und die Wahrung der Betroffenenrechte verantwortlich ist.

In welcher Form die Behörden eine solche Regelung festhalten, ist inhaltlich nicht vorgeschrieben und kann namentlich durch technische Weisungen, Nutzungsbedingungen, Konzepte oder Vereinbarungen erfolgen. Legen die Behörden keine Verantwortlichkeiten untereinander fest, so gelten sie gleichermassen als für die gesamte Datenbearbeitung verantwortlich. So ist beispielsweise denkbar, dass eine Gesamtapplikation für die Personalverwaltung durch eine Behörde zur Verfügung gestellt wird, welche die entsprechenden technischen Mittel für die ICT-Grundversorgung verantwortet. Sie kann regeln, welches Datenschutz- und Datensicherheitsniveau mit diesen Mitteln sichergestellt wird. Jede Behörde, welche die Applikation zur Verwaltung ihrer Personaldaten verwendet, ist für die dabei bearbeiteten Personendaten verantwortlich (in der Praxis oft auch als «Dateneigner» oder «Dateneignerin» bezeichnet), legt weitergehende technische und organisatorische Massnahmen fest (so muss sie bspw. die behördeninternen Zugriffsrechte vergeben) und ist Ansprechpartnerin für die Betroffenenrechte der Mitarbeitenden.

§ 31 (Wahl und Stellung)
Wahl (Abs. 1):
Der Passus «[der Kantonsrat] wählt auf Antrag des Regierungsrates […]» wird aufgehoben. Mit dem Wegfall des Wahlvorschlags durch den Regierungsrat als Wahlvoraussetzung wird die Unabhängigkeit der bzw. des IDSB gestärkt, wie es auch für die Chefin bzw. den Chef der Finanzkontrolle geregelt ist (s. § 63 Abs. 2 des Gesetzes über die wirkungsorientierte Verwaltungsführung [WoV-G; BGS 115.1]). Künftig soll die Ratsleitung oder eine parlamentarische Kommission das Rekrutierungsverfahren durchführen und dem Kantonsrat Wahlvorschläge unterbreiten. Dies entspricht auch der Regelung auf Bundesebene. Nach Artikel 43 Absatz 1 DSG kommt dem Bundesrat für die Wahl des EDÖB kein Vorschlagsrecht zu.

Amtsenthebung (Abs. 2):
Die im geltenden Recht vorgesehenen Gründe für die Auflösung des Dienstverhältnisses der bzw. des IDSB entsprechen nicht den Anforderungen der Richtlinie (Art. 43 Abs. 4) und der DSGVO (Art. 53 Abs. 4). Diese erlauben eine Amtsenthebung nur bei schwerer Verfehlung oder wenn die Voraussetzungen für die Aufgabenerfüllung nicht mehr gegeben sind. Das InfoDG sieht eine Auflösung des Dienstverhältnisses gemäss § 28 des Gesetzes über das Staatspersonal (StPG; BGS 126.1) beim Vorliegen *wichtiger Gründe* vor. Diese Formulierung ist zu weit gefasst, um den Anforderungen des europäischen Rechts zu genügen. Eine solche Regelung wurde denn auch in den Schengen-Empfehlungen gerügt (Empfehlung Nr. 2). Die Regelung lehnt sich an Artikel 44 Absatz 3 DSG an.

[1] Vgl. GABOR P. BLECHTA/LUCA DAL MOLIN/KIRSTEN WESIAK-SCHMIDT, in: BSK-DSG, a.a.O., Art. 5 N 183 m.w.H.

Neu soll eine Amtsenthebung nur möglich sein, wenn die bzw. der IDSB vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat (Bst. a), dauernd an der Aufgabenerfüllung verhindert ist (Bst. b) oder wegen eines Verbrechens oder eines mit der Ausübung des Amtes nicht zu vereinbarenden Vergehens rechtskräftig verurteilt worden ist (Bst. c). Der Katalog ist abschliessend. Um schwere Amtspflichtverletzungen im Sinne von Buchstabe a handelt es sich, wenn diese derart gravierend sind, dass das Vertrauen in die bzw. den IDSB in einer Weise angeschlagen ist, dass sie bzw. er das Amt nicht mehr ordnungsgemäss erfüllen kann. Als Beispiele können etwa genannt werden: schwere Straftaten im Zusammenhang mit der Amtsausübung, Mobbing oder sexuelle Belästigung am Arbeitsplatz[1]. Inhaltlich ist Buchstabe b an Artikel 44 Absatz 3 Bst. b DSG angelehnt, gemäss welchem die Bundesversammlung die bzw. den IDSB des Amtes entheben kann, wenn sie bzw. er die Fähigkeit zur Amtsausübung auf Dauer verloren hat. Im Vordergrund steht die Amtsunfähigkeit infolge Krankheit oder Unfall. Es sind aber auch andere Gründe denkbar, welche zu einer dauerhaften Verhinderung an der Amtsausübung führen können (beispielsweise Verschollenheit oder Entführung). Ab wann von einer dauerhaften Verhinderung an der Amtsausübung auszugehen ist, muss im Einzelfall beurteilt werden. Handelt es sich um eine krankheits- oder unfallbedingte Verhinderung an der Amtsausübung, wird sich der Kantonsrat in Bezug auf die Beurteilung der Dauerhaftigkeit in der Regel auf ärztliche Berichte abstützen müssen. Im Gegensatz zur Regelung beim Staatspersonal (vgl. § 30 StPG) führt eine dauerhafte Verhinderung an der Amtsausübung nicht zur automatischen Amtseinstellung, sondern es bedarf dafür eines Beschlusses des Kantonsrates. Sollte die bzw. der IDSB am Ende einer Amtsdauer arbeitsunfähig sein und nicht wiedergewählt werden, endet das Anstellungsverhältnis mit dem Ende der Amtszeit. Losgelöst von der Frage der Amtseinstellung muss der Anspruch auf Lohnfortzahlung bei Krankheit und Unfall beurteilt werden. Letzterer richtet sich nach den Regelungen für das Staatspersonal gemäss § 47 StPG. Demnach besteht bei Krankheit und Unfall ein voller Lohnfortzahlungsanspruch während zwölf Monaten (§ 47 Abs. 1 Bst. b StPG). Der Anspruch auf Taggeldleistungen richtet sich nach § 47bis StPG. Eine positivrechtliche Normierung des Anspruchs auf Lohnfortzahlung und Taggeldleistungen im InfoDG ist aufgrund der subsidiären Geltung des Staatspersonalrechts (§ 31 Abs. 3bis InfoDG) nicht erforderlich. Buchstabe c sieht vor, dass eine Amtsenthebung auch bei einer rechtskräftigen Verurteilung wegen eines Verbrechens oder eines mit der Ausübung des Amts nicht zu vereinbarenden Vergehens möglich ist. Die Aufzählung ist abschliessend. Dieser Amtsenthebungsgrund ist im DSG nicht aufgeführt; es wäre aber stossend, wenn gravierende Verfehlungen im Privatbereich nicht zu einer Amtsenthebung führen könnten. Zu den Vergehen, welche mit der Amtsführung nicht vereinbar sind, zählen insbesondere ungetreue Geschäftsbesorgung, Geldwäscherei oder unbefugtes Beschaffen von Personendaten. Während beispielsweise eine Verurteilung wegen fahrlässiger Körperverletzung die erforderliche Schwelle kaum erreichen dürfte, könnte eine solche wegen fahrlässiger Tötung unter Umständen ausreichen. Neu wird der Antrag auf Amtsenthebung nicht mehr vom Regierungsrat gestellt, sondern der Kantonsrat wird selbst festlegen müssen, welche Kommission für die vorbereitenden Handlungen und den Antrag zuständig ist.

Das Verfahren zur Amtsenthebung richtet sich sinngemäss nach den Regelungen zur disziplinarischen Verantwortlichkeit im Verantwortlichkeitsgesetz.

Verwarnung (Abs. 2bis):
Neu wird die Möglichkeit vorgesehen, dass die bzw. der IDSB verwarnt werden kann, wenn sie bzw. er eine Amtspflichtverletzung begeht. Die Bestimmung ist an Artikel 44a DSG angelehnt. Es handelt sich um eine Kann-Bestimmung. Die entsprechende Zuständigkeit liegt bei der Ratsleitung. Der Umstand, dass die Ratsleitung eine Verwarnung aussprechen kann, ändert an der Unabhängigkeit der bzw. des IDSB nichts. Diese gilt weiterhin uneingeschränkt. Auch die Ratsleitung darf sich nicht in die Art und Weise, wie die bzw. der IDSB ihre bzw. seine Funktion ausübt, einmischen. Sie darf Verwarnungen nur dann aussprechen, wenn die bzw. der IDSB Amtspflichten verletzt. Die Verwarnung ist die einzige Disziplinierungsmöglichkeit gegenüber der

[1] Vgl. RENÉ HUBER, in: DAVID VASELLA/GABOR P. BLECHTA, BSK-DSG, Art. 44 N 45.

bzw. dem IDSB. Insbesondere die in § 25 des Verantwortlichkeitsgesetzes (BGS 124.21) aufgezählten Massnahmen können gegenüber der bzw. dem IDSB nicht verhängt werden, da das Verantwortlichkeitsgesetz in Bezug auf die disziplinarische Verantwortlichkeit nicht auf die bzw. den IDSB anwendbar ist. In Bezug auf die vermögensrechtliche Verantwortlichkeit bleibt es aber auf die bzw. den IDSB anwendbar. Aufgrund des Grundsatzes von Treu und Glauben ist eine Verwarnung in der Regel geboten, bevor ein Amtsenthebungsverfahren eingeleitet wird.

Lohn und Personalrecht (Abs. 3):
Wie bei der Chefin bzw. beim Chef der Finanzkontrolle rechtfertigt es sich auch bei der bzw. dem IDSB aus Gründen der Unabhängigkeit, die Lohnklasse im Gesetz festzulegen (s. § 63 Abs. 4 WoV-G). Für die Einstufung ist weiterhin der Regierungsrat zuständig (§ 2 Abs. 2 der Verordnung über das Personalrecht [PRV; BGS 126.31]). Um die Unabhängigkeit der bzw. des IDSB zu wahren, wird sie bzw. er von der Mitarbeitendenbeurteilung ausgeschlossen. Dies hat zur Folge, dass kein LEBO ausgerichtet wird (§ 134 Abs. 4 des Gesamtarbeitsvertrages [GAV; BGS 126.3]). Diese gelebte Praxis wird neu in Absatz 3 festgehalten. Die subsidiäre Geltung des Personalrechts gemäss dem Gesetz über das Staatspersonal und dem GAV für die bzw. den IDSB (bisher in Abs. 2 integriert) wird in Absatz 3 angefügt.

§ 31bis (Ausstand)
Es erscheint sinnvoll, im Rahmen der Revision neu auch eine Regelung für Ausstandsfälle vorzusehen. Die vorliegende Bestimmung orientiert sich an Artikel 47a DSG.

Absatz 1: In Ausstandsfällen gelten für die bzw. den IDSB sinngemäss die Bestimmungen des Gesetzes über die Gerichtsorganisation (GO; BGS 125.12), namentlich in Bezug auf die Gründe für den Ausstand.

Absatz 2: Zuständig für den Entscheid über ein Ausstandsbegehren gegen die bzw. den IDSB ist die Präsidentin bzw. der Präsident des Verwaltungsgerichts. Es erscheint sachgerecht, diese Kompetenz in die Hände einer unabhängigen Gerichtsinstanz zu legen. Absatz 2 sieht neu die Möglichkeit vor, dass eine ausserordentliche Stellvertretung eingesetzt werden kann, sofern die ordentliche Stellvertretungsregelung nicht zum Tragen kommt, beispielsweise bei ebenfalls bestehenden Ausstandsgründen. Als ausserordentliche Stellvertretung kann insbesondere eine ausserkantonale Beauftragte bzw. ein ausserkantonaler Beauftragter oder eine andere fachlich ausgewiesene Person, beispielsweise eine pensionierte Richterin bzw. ein pensionierter Richter, eingesetzt werden.

Absatz 3: Über den Ausstand des übrigen Personals entscheidet erstinstanzlich die bzw. der IDSB. Als Rechtsmittel wird die Verwaltungsgerichtsbeschwerde vorgesehen. Für diese gilt eine Beschwerdefrist von 10 Tagen; das Verfahren richtet sich nach dem Verwaltungsrechtspflegegesetz (§ 39 Abs. 1 InfoDG).

§ 32 (Aufgaben)
Ausnahmen von der Aufsicht (Bst. a):
Bereits bisher standen der bzw. dem IDSB im Bereich Öffentlichkeitsprinzip keine gesetzlichen Aufsichtsmittel zur Verfügung. Es ist sachlogisch, in Buchstabe a den Passus «über den Zugang zu amtlichen Dokumenten» zu streichen und damit klarzustellen, dass die bzw. der IDSB im Bereich des Öffentlichkeitsprinzips keine Aufsichtsaufgaben ausübt. Dies ist auch nicht notwendig, denn in diesem Bereich sind die Schlichtungsverfahren (§ 36 InfoDG) vorgesehen.

Bisher waren der Regierungsrat und der Kantonsrat von der Aufsicht der bzw. des IDSB ausgenommen. Weil der Geltungsbereich der Datenschutzbestimmungen in § 2 Absatz 3 Buchstabe c InfoDG erweitert wird, fallen neu auch die Gerichte und weitere Justizorgane im Bereich der Verfahren grundsätzlich unter die Bestimmungen des 5. Titels des InfoDG. Aus Gründen der Gewaltenteilung drängt es sich auf, sämtliche Gerichte (inkl. Kantonale Schätzungskommission) von der Aufsicht der bzw. des IDSB auszunehmen. Die Staats- und die Jugendanwaltschaft sind

im Interesse ihrer unabhängigen Verfahrensführung ebenfalls von der Aufsicht auszunehmen, soweit sie justizielle Tätigkeiten ausüben. Staats- und Jugendanwaltschaft sind in der Rechtsanwendung unabhängig und allein dem Recht verpflichtet (Art. 4 Abs. 1 StPO). Die Bearbeitung von Strafverfahren gehört daher zur justiziellen Tätigkeit dieser Strafbehörden. Dies gilt nicht nur bezüglich der hängigen und damit aktuell zu bearbeitenden Verfahren, sondern auch bezüglich der sistierten (vgl. Art. 314 StPO) und zufolge Strafbefehl, Einstellungs- oder Nichtanhandnahmeverfügung aktuell als abgeschlossen geltenden Verfahren. Auch die Bearbeitung dieser Verfahren ist Teil der justiziellen Tätigkeit. Dies ergibt sich schon daraus, dass diese Verfahren gestützt auf die StPO nach dem Eintritt gewisser Bedingungen wieder bearbeitet werden müssen, um zu entscheiden, ob sie wieder auf «hängig» zu stellen sind (vgl. Wiederaufnahme gemäss Art. 315 oder 323 StPO, Revision gemäss Art. 410 ff. StPO).

Die in § 32 Absatz 1 Buchstabe a InfoDG vorgesehene Regelung entspricht jener der Richtline (Art. 45). Auch der Bund hat seine Gerichte und die Bundesanwaltschaft, soweit sie Personendaten im Rahmen von Strafverfahren bearbeitet, von der Aufsicht des EDÖB ausgenommen (Art. 4 Abs. 2 Bst. c und d DSG).

Die Ausnahme von der Aufsicht der bzw. des IDSB bedeutet konkret, dass sie bzw. er in den von der Aufsicht ausgenommenen Bereichen keine Aufsichtsanzeigen (§ 32 Abs. 1 Bst. k InfoDG) behandeln, keine Abklärungen gemäss § 33 Absatz 2 InfoDG durchführen und keine aufsichtsrechtlichen Massnahmen gemäss § 38 InfoDG erlassen kann. Alle anderen in § 32 InfoDG aufgezählten Aufgaben soll die bzw. der IDSB auch in Bezug auf die von der Aufsicht ausgenommenen Bereiche ausüben. Dies bedeutet insbesondere, dass sich der Regierungsrat, der Kantonsrat, die Gerichte, die Staats- sowie die Jugendanwaltschaft von der bzw. dem IDSB beraten lassen können. Diese Behörden sind auch verpflichtet, der bzw. dem IDSB Verletzungen der Datensicherheit zu melden und Datenschutz-Folgenabschätzungen zur Prüfung einzureichen. Stellt sie bzw. er Verletzungen der Datenschutzvorschriften fest, kann sie bzw. er im Sinne der Beratung eine nicht verbindliche Empfehlung gemäss § 38bis InfoDG (s. unten) abgeben. Aufsichtsrechtliche Massnahmen können hingegen nicht verhängt werden.

Schulung und Sensibilisierung (Bst. b):
Im Verhältnis zum Aufgabenkatalog der bzw. des IDSB im geltenden § 32 InfoDG sehen der KdK-Leitfaden, die Richtlinie (Art. 46) und die DSGVO (Art. 57) einen leicht erweiterten Katalog vor. Es handelt sich grundsätzlich um Aufgaben, welche die IDSB in ihrer Praxis bereits heute berücksichtigt. Insofern stellt die Aufnahme der Schulung der Behörden und der Sensibilisierung der Bevölkerung für den Datenschutz (Bst. b) in den Aufgabenkatalog keine materielle Änderung dar. Ein gesetzlicher Auftrag, die Bevölkerung in Bezug auf den Datenschutz zu sensibilisieren, besteht nur im Anwendungsbereich des InfoDG. Darüber hinaus ist die Bestimmung als Ermächtigungsbestimmung zu verstehen. Die bzw. der IDSB kann punktuell und in Ergänzung zu bestehenden Sensibilisierungs- und Aufklärungsarbeiten von anderen Behörden, insbesondere jenen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), der Kantonspolizei und von privaten Einrichtungen (z.B. Pro Juventute, Pro Senectute usw.) tätig werden. Die Bestimmung zur Sensibilisierung ist im Wortlaut an jene des Bundes in Artikel 58 Absatz 1 Buchstabe c DSG angelehnt. Andere Kantone kennen ähnliche Bestimmungen, z.B. der Kanton AG (§ 31 Abs. 1 Bst. e IDAG-AG).

Führung des Registers der Bearbeitungstätigkeiten (Bst. d):
Der bzw. die IDSB führt das Register der Bearbeitungstätigkeiten der Behörden (s. oben, zu §§ 24 und 25 InfoDG).

Vorabkontrollen (Bst. h):
Die Regelung zur Vorabkontrolle erfährt eine redaktionelle Angleichung an die neuen Bestimmungen zur Datenschutz-Folgenabschätzung (§ 30bis InfoDG), welche zur Vorabkontrolle einzureichen ist. Der bzw. dem IDSB stehen auch im Rahmen von Vorabkontrollen die Befugnisse gemäss §§ 38 und 38bis InfoDG zu (s. dazu unten).

Zusammenarbeit (Bst. i):
Die bestehende Bestimmung wird inhaltlich ergänzt, um dem Aufgabenkatalog der bzw. des IDSB gerecht zu werden. Es erscheint zu restriktiv, die Zusammenarbeit der bzw. des IDSB mit anderen Behörden auf die Kontrollaufgaben zu beschränken. Vielmehr soll eine Zusammenarbeit mit Behörden im gesamten Aufgabenbereich möglich sein. Dies gilt insbesondere für die Bereiche des Öffentlichkeitsprinzips und der Rechtsetzung. Die inhaltliche Erweiterung der Bestimmung soll es der bzw. dem IDSB auch ermöglichen, sich im Zusammenhang mit der Aufgabenerfüllung mit der kantonalen Finanzkontrolle auszutauschen.

Verletzungen der Datensicherheit (Bst. j):
Im Einklang mit der neu in § 30ter InfoDG vorgesehenen Meldepflicht von Verletzungen der Datensicherheit wird in Buchstabe j die entsprechende Aufgabe der bzw. des IDSB aufgeführt.

Behandlung von Anzeigen (Bst. k):
Das Recht bei einer Aufsichtsbehörde eine Aufsichtsanzeige einzureichen, ergibt sich bereits aus Artikel 26 der Verfassung des Kantons Solothurn (KV; BGS 111.1) als Anwendungsfall des Petitionsrechts. Im Anwendungsbereich des InfoDG betreffend den Datenschutz ist die bzw. der IDSB die zuständige Aufsichtsbehörde (§ 32 Abs. 1 Bst. a InfoDG). Das europäische Recht sieht vor, dass betroffenen Personen der gerichtliche Rechtsweg offensteht, sofern sich eine Datenschutzaufsichtsbehörde innerhalb von drei Monaten nicht mit einer aufsichtsrechtlichen Anzeige befasst oder nicht über den Stand oder das Ergebnis davon informiert (Art. 53 Abs. 2 Richtlinie; Art. 78 Abs. 2 DSGVO). Es handelt sich dabei um eine Form der Rechtsverweigerung bzw. -verzögerung. Um diesen Überlegungen Rechnung zu tragen, wird in Buchstabe k präzisiert, dass die bzw. der IDSB die anzeigende Person innerhalb von drei Monaten über das Ergebnis oder den Stand der Abklärungen orientiert. Nicht jede aufsichtsrechtliche Anzeige kann innerhalb von drei Monaten erledigt werden. Dies kann z.B. aufgrund eines komplexen Sachverhalts, umfangreicher juristischer Fragestellungen, der Anhörung von Dritten oder der Ressourcen der bzw. des IDSB mehr Zeit in Anspruch nehmen. Die anzeigende Person soll aber in jedem Fall eine Information zum Verfahrensstand erhalten. Im gemäss Buchstabe a von der Aufsicht ausgenommenen Bereich (z.B. Gerichte) kann die bzw. der IDSB keine Aufsichtsanzeigen behandeln.

§ 33 (Arbeitsweise)
Die Änderungen sind rein redaktioneller Natur.

Titel 6.1., neuer Titel 6.1^{bis}.
Der bestehende Abschnittstitel «6.1. Organisation» enthält nur Regelungen zur Organisation der bzw. des IDSB. Die neue Bestimmung betreffend Datenschutzberaterin oder -berater betrifft jedoch die Organisation sämtlicher Behörden im Geltungsbereich des Gesetzes. Dem Abschnittstitel 6.1. ist deshalb ein weiterer Abschnittstitel anzufügen, welcher die Organisation der Behörden betrifft.

§ 33ter (Datenschutzberaterin oder Datenschutzberater)
Absatz 1: Nach der Richtlinie (Art. 32) müssen zumindest Strafverfolgungs-, Strafgerichts- und Strafvollzugsbehörden eine Datenschutzberaterin bzw. einen Datenschutzberater ernennen. Diese Pflicht ist auch ins InfoDG aufzunehmen. Davon betroffen sind insbesondere die Kantonspolizei, die Staatsanwaltschaft, die Jugendanwaltschaft, das Amt für Justizvollzug, die Gerichte in Strafsachen sowie das Polizeikorps der Stadt Solothurn. Die anderen Behörden können, wenn sie dies als sinnvoll erachten, ebenfalls solche Funktionsträger bezeichnen. Die Datenschutzberaterin bzw. der Datenschutzberater muss in jedem Fall die Anforderungen nach Absatz 3 (s. unten) erfüllen.

Absatz 2 stellt klar, dass mehrere Behörden zusammen dieselbe Person als Datenschutzberaterin bzw. Datenschutzberater ernennen können.

Absatz 3: Die Datenschutzberaterin bzw. der Datenschutzberater kann ihre bzw. seine Aufgaben nach Absatz 4 nur angemessen erfüllen, wenn sie oder er über die erforderlichen Fachkenntnisse verfügt. Sie bzw. er muss die Funktion der Datenschutzberaterin bzw. des Datenschutzberaters unabhängig und weisungsungebunden ausüben können. Insofern dürfen der Datenschutzberaterin bzw. dem Datenschutzberater aufgrund ihrer bzw. seiner unabhängigen Beratungstätigkeit keine Nachteile erwachsen. Es ist insbesondere zu verhindern, dass sich die Tätigkeit negativ auf die Mitarbeitendenbeurteilung auswirken kann.

Absatz 4: Die Aufgaben der Datenschutzberaterin bzw. des Datenschutzberaters umfassen zunächst die Beratung und Unterstützung der Behörde bei der Einhaltung und beim Vollzug der Datenschutzvorschriften (Bst. a). Diese Aufgabe kann beispielsweise über die Mitwirkung an Datenschutz-Folgenabschätzungen (vgl. oben, zu § 30bis InfoDG), die interne Beurteilung von Verletzungen der Datensicherheit und die Schulung von Mitarbeitenden erreicht werden. Weiter dient die Datenschutzberaterin bzw. der Datenschutzberater gemäss Buchstabe b als Anlaufstelle für betroffene Personen, etwa im Zusammenhang mit Auskunftsgesuchen nach § 26 InfoDG oder der Geltendmachung von anderen Rechtsansprüchen nach § 28 InfoDG. Sie bzw. er ist gleichzeitig aber auch Ansprechperson für die bzw. den IDSB und arbeitet insofern mit dieser bzw. diesem zusammen (Bst. c). Die bzw. der IDSB wird sich bei Datenschutzanliegen im Zusammenhang mit der betreffenden Behörde insofern in erster Linie an die Datenschutzberaterin bzw. den Datenschutzberater wenden.

Absatz 5 sieht vor, dass der Regierungsrat auf Verordnungsstufe die Aufgaben und Stellung der Datenschutzberaterin bzw. des Datenschutzberaters konkretisiert. Ausserdem wird mit Absatz 5 dem Regierungsrat die Kompetenz delegiert, auch weitere Behörden zur Ernennung einer Datenschutzberaterin bzw. eines Datenschutzberaters zu verpflichten. Dies kann etwa bei Behörden, deren Datenbearbeitungen besondere Risiken für betroffene Personen bergen (z.B., weil im grossen Umfang besonders schützenswerte Personendaten bearbeitet werden), sinnvoll sein.

§ 34bis (Anhörung)
Die vorgeschlagene neue Bestimmung lehnt sich an den revidierten Artikel 11 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3) an. Sie dient dem Schutz der Geheimhaltungsinteressen der natürlichen und juristischen Personen, deren Daten in amtlichen Dokumenten enthalten sind und über Zugangsgesuche veröffentlicht werden könnten. Sie weist Parallelen zum verfassungsrechtlichen Anspruch auf rechtliches Gehör (Art. 29 Abs. 2 BV) auf.[1]

Die vorgeschlagene Bestimmung setzt zunächst eine vorläufige Interessenabwägung durch die Behörde voraus. Darin ist zu prüfen, ob die Zugangsgewährung zum verlangten Dokument überhaupt in Betracht fällt. Ist dies der Fall, sind die betroffenen Personen grundsätzlich anzuhören, wozu ihnen die Behörde eine Frist von 10 Tagen setzt. Die Frist kann auf begründetes Ersuchen erstreckt werden. Gestützt auf die Erkenntnisse der Anhörung ist sodann eine definitive Interessenabwägung vorzunehmen und eine Stellungnahme über die Zugangsgewährung abzugeben.[2]

§ 35 (Stellungnahme der Behörde)
Absatz 1: Ausgang für die Ergänzung bildet der Auftrag Rémy Wyssmann (SVP, Kriegstetten) «Verschleppung von Zugangsgesuchen verhindern».[3] Der Regierungsrat hat dem Kantonsrat beantragt, den Auftrag mit geändertem Wortlaut für erheblich zu erklären und vorgeschlagen, diesen mit der vorliegenden Revision umzusetzen.[4] Diesem Antrag ist der Kantonsrat gefolgt.[5]

---
[1] Vgl. ALEXANDRE FLÜCKIGER, Handkommentar BGÖ, Art. 11 N 3.
[2] Vgl. ANNINA KELLER/DANIEL KÄMPFER, Öffentlichkeitsgesetz: Die neuere Rechtsprechung im Lichte des gesetzgeberischen Konzepts und seinen Stolpersteinen, medialex 2017, N 95 ff., N 20.
[3] A 0147/2021.
[4] RRB Nr. 2021/1593 vom 2. November 2021.
[5] KRB Nr. A 0147/2021 vom 11. Mai 2022.

Neu haben Behörden eine Frist von 30 Tagen, um zu einem eingegangenen Zugangsgesuch Stellung zu nehmen. Verursacht das Zugangsgesuch einen besonderen Aufwand, kann die Frist um weitere 30 Tage verlängert werden. Vorbehalten bleiben Zugangsgesuche, die Dokumente betreffen, welche Personendaten enthalten. In diesen Fällen müssen die betroffenen Drittpersonen in aller Regel angehört werden, was eine gewisse Zeit in Anspruch nehmen kann. Doch auch bei diesen Fällen müssen die Zugangsgesuche zügig bearbeitet werden. Die Ergänzung entspricht dem Wortlaut von Artikel 12 Absatz 1 und 2 BGÖ. Allerdings ist eine Erledigung der Zugangsgesuche innert 20 Tagen, so wie es Artikel 12 BGÖ beim Bund vorsieht, erfahrungsgemäss in den meisten Fällen nicht praktikabel. Es soll deshalb eine Erledigungsfrist von 30 Tagen sowie eine mögliche Verlängerung von weiteren 30 Tagen bei besonderem Aufwand vorgesehen werden.

Absatz 1bis: Die Behörde muss den Zugang bis zur Klärung der Rechtslage aufschieben, wenn durch den Zugang die Privatsphäre von Drittpersonen beeinträchtigt werden kann. Die Rechtslage ist geklärt, wenn entweder im Schlichtungsverfahren eine Einigung erzielt wurde, nach einer Empfehlung der bzw. des IDSB keine Verfügung verlangt wird oder eine Verfügung bzw. ein sie betreffender Beschwerdeentscheid rechtskräftig ist. Die Regelung entspricht Artikel 12 Absatz 3 BGÖ.

Absatz 2: Neu muss die Behörde auf Verlangen auch dann eine Begründung abgeben, wenn sie den Zugang gewährt. Dies gilt selbstredend nur für den Fall, dass eine Anhörung Drittbetroffener erfolgt (s. dazu oben, zu § 34bis InfoDG) und die Drittperson die Begründung verlangt.

Absatz 3: Dieser neue Absatz präzisiert den Verfahrensablauf, sofern die Behörde den Zugang zu amtlichen Dokumenten einschränkt, aufschiebt, verweigert oder (entgegen dem Antrag einer betroffenen Drittperson gemäss § 34bis InfoDG) gewährt. Die Behörde muss die gesuchstellende sowie eine allfällige drittbetroffene Person auf ihr Recht, einen Schlichtungsantrag bei der bzw. dem IDSB stellen zu können, hinweisen.

§ 36 (Schlichtung; Empfehlung)
Absatz 1: Es kommt vor, dass Behörden auf Zugangsgesuche nicht reagieren bzw. diese nicht innert angemessener Frist (gemäss § 35 Abs. 1 InfoDG) bearbeiten. Neu soll im Gesetz explizit festgehalten werden, dass in solchen Fällen die gesuchstellende Person einen Schlichtungsantrag stellen kann. Dies entspricht der bestehenden Praxis und stellt keine materielle Neuerung dar. Mit der präzisierenden Ergänzung wird ebenfalls der Auftrag Rémy Wyssmann (SVP, Kriegstetten) «Verschleppung von Zugangsgesuchen verhindern» (s. oben, zu § 35 InfoDG) umgesetzt.

Absatz 1bis: Neu sollen auch angehörte Drittpersonen einen Antrag auf Schlichtung bei der bzw. dem IDSB stellen können, sofern die Behörde beabsichtigt, gegen ihren Willen den Zugang zu amtlichen Dokumenten zu gewähren. Der Bund sieht in Artikel 13 Absatz 1 Buchstabe c BGÖ eine vergleichbare Bestimmung vor.

§ 37 (Verfügung)
Absatz 1 Buchstabe a: An Artikel 15 Absatz 1 BGÖ angelehnt wird eine Frist für das Gesuch um Erlass einer Verfügung vorgesehen. Die Frist beginnt mit dem Empfang der Empfehlung gemäss § 36 Absatz 3 InfoDG zu laufen und beträgt 30 Tage. Wird innert der Frist keine Verfügung verlangt, besteht für die Behörde, den Gesuchsteller oder die Gesuchstellerin wie auch die angehörten Personen Klarheit über den Abschluss des Verfahrens, was der Rechtssicherheit dient.

Absatz 1 Buchstaben b und c: Diese neuen Regelungen lehnen sich an Artikel 15 Absatz 2 BGÖ an. Es soll klargestellt werden, dass die Behörde nicht nur dann eine Verfügung zu erlassen hat, wenn die gesuchstellende Person oder die angehörte Person es verlangt, sondern auch immer dann, wenn die Behörde von der Empfehlung der bzw. des IDSB abweichen möchte, indem sie das Zugangsrecht einschränken, aufschieben oder verweigern will (Bst. b) oder den Zugang trotz schützenswerter Interessen Dritter gewähren will (Bst. c).

Absatz 2: Es wird die Rechtsprechung des Verwaltungsgerichts[1] kodifiziert, wonach ein Schlichtungsverfahren zwingend zu durchlaufen ist, bevor die Behörde eine Verfügung erlassen kann. Wenn die gesuchstellende Person oder eine betroffene Drittperson von der Behörde vorher eine Verfügung verlangt, überweist diese das Gesuch unverzüglich an die bzw. den IDSB zur Behandlung als Antrag auf Schlichtung.

§ 38 (Aufsichtsrechtliche Massnahmen)
Verfügungskompetenz (Absatz 1):
Die europäischen Rechtsordnungen verlangen neu, dass der Datenschutzaufsichtsbehörde die Kompetenz zukommt, bei Datenschutzverletzungen verbindliche Anordnungen erlassen zu können (Art. 47 Abs. 2 Bst. b Richtlinie; Art. 58 Abs. 2 DSGVO; Art. 15 Abs. 2 Bst. c SEV 108+). Die Verfügungskompetenz ist eine zentrale Anforderung der Richtlinie und der DSGVO und wird auch in den Schengen-Empfehlungen hervorgehoben (Empfehlung Nr. 4). Nach dem geltenden Recht steht der bzw. dem IDSB einzig das Instrument der Empfehlung mit anschliessendem Beschwerdeweg zur Verfügung. Es besteht demnach ein klarer Revisionsbedarf.

Absatz 1 hält deshalb neu fest, dass die bzw. der IDSB aufsichtsrechtliche Massnahmen verfügen kann. Die Bestimmung ist als Kann-Bestimmung formuliert. Der bzw. dem IDSB steht ein Entschliessungs- und Auswahlermessen zu. Von der Verhängung einer Verfügung wird sie bzw. er aus Gründen der Verhältnismässigkeit regelmässig absehen, wenn bereits Abhilfe geschaffen wurde oder es sich um eine geringfügige Datenschutzverletzung handelt. Keine Verfügungskompetenz steht der bzw. dem IDSB in den Bereichen zu, die von der Aufsicht ausgenommen sind (§ 32 Abs. 1 Bst. a InfoDG).

Der Bundesgesetzgeber hat den EDÖB ebenfalls mit der Kompetenz ausgestattet, verbindliche Anordnungen zu erlassen (Art. 51 DSG). Diesem Ansatz sind z.B. auch die Kantone AG (§ 32 Abs. 4 IDAG-AG) und BL (§ 44 Abs. 1 IDG-BL) gefolgt.

Vorsorgliche Massnahmen (Abs. 2):
Die Richtlinie (Art. 47 Abs. 2 Bst. c) und die DSGVO (Art. 58 Abs. 2 Bst. f) verleihen der Aufsichtsbehörde die Befugnis, vorsorgliche Massnahmen zu ergreifen. Die Abklärungen, ob wirklich eine Datenschutzvorschrift verletzt ist, dauert eine gewisse Zeit. Es ist denkbar, dass bei gewissen Vorfällen ein aufsichtsrechtliches Einschreiten der bzw. des IDSB notwendig erscheint, noch bevor diese Abklärungen abgeschlossen sind. Absatz 2 regelt deshalb, unter welchen Voraussetzungen die bzw. der IDSB vorsorgliche Massnahmen ergreifen kann: Es müssen genügend Anzeichen vorliegen, dass Datenschutzvorschriften verletzt werden und den betroffenen Personen muss ein nicht leicht wiedergutzumachender Nachteil drohen. Vorsorgliche Massnahmen können maximal für zwölf Monate verhängt werden. In dieser Zeit muss es der bzw. dem IDSB möglich sein, die Abklärungen abzuschliessen und – sofern erforderlich – eine aufsichtsrechtliche Massnahme gemäss Absatz 1 zu verfügen. Falls die Abklärungen ergeben, dass keine Datenschutzvorschriften verletzt sind, muss die bzw. der IDSB die vorsorgliche Massnahme unverzüglich aufheben.

Der Entwurf des Bundesrates zum nDSG enthielt noch die Befugnis des EDÖB vorsorgliche Massnahmen zu erlassen (Art. 44 Abs. 2 des Entwurfes). Der Gesetzgeber beziehungsweise die vorberatende Kommission haben diese Befugnis – ohne parlamentarische Debatte – aus dem ursprünglichen Entwurf gestrichen. Lehre und Rechtsprechung anerkennen aber, dass Behörden auch im erstinstanzlichen Verfahren vorsorgliche Massnahmen anordnen können.[2] Andere Kantone kennen vergleichbare Regelungen (z.B. die Kantone AG [§ 32 Abs. 3bis IDAG-AG], GL [Art. 58 Abs. 5 IDAG-GL] und LU [§ 24 Abs. 4 DSG-LU]).

Anhörung der betroffenen Behörde (Abs. 3):
Bevor die bzw. der IDSB aufsichtsrechtliche Massnahmen ergreift, hört sie bzw. er die Behörde

[1] Urteil des solothurnischen Verwaltungsgerichts vom 13. Juli 2021, VWBES.2020.405, SOG 2022 Nr. 4.
[2] Vgl. LENA GÖTZINGER/ISABELLE HANSELMANN, in: DAVID VASELLA/GABOR P. BLECHTA, BSK-DSG, Art. 51 N 44 f.

an. Diese Anhörung ist kein Ausfluss des rechtlichen Gehörs, ergibt sich aber aus der Notwendigkeit, den Sachverhalt genügend abzuklären. Von der Anhörung kann abgesehen werden, wenn der Erlass der Aufsichtsmassnahme zeitlich dringlich ist.

Rechtsweg (Abs. 4):
Die von der bzw. dem IDSB erlassenen Verfügungen können einer gerichtlichen Kontrolle unterzogen werden. Die Beschwerdemöglichkeit steht der Behörde zu, an welche sich die Verfügung richtet (Departement, Amt, Abteilung etc.). Das Verfahren richtet sich nach § 66 ff. Verwaltungsrechtspflegegesetz. Die bzw. der IDSB hat im verwaltungsgerichtlichen Beschwerdeverfahren die Stellung der Vorinstanz.

§ 38bis (Empfehlung)
In § 32 Absatz 1 Buchstabe a InfoDG werden der Regierungsrat, der Kantonsrat, die Gerichte sowie die Staats- und die Jugendanwaltschaft (die beiden Letztgenannten soweit die Bearbeitung von Personendaten ein Strafverfahren betrifft) von der Aufsicht der bzw. des IDSB ausgenommen. Falls die bzw. der IDSB feststellen sollte, dass in einem von der Aufsicht ausgenommenen Bereich Datenschutzvorschriften verletzt werden, können keine aufsichtsrechtlichen Massnahmen verhängt werden. Es ist aber dennoch sinnvoll, dass die bzw. der IDSB ihre bzw. seine Erkenntnisse der Behörde mitteilt und empfiehlt, wie der gesetzeskonforme Zustand erreicht werden kann. Eine solche Empfehlung hat beratenden Charakter und ist nicht verbindlich. Die Behörde entscheidet frei, ob sie die Empfehlung umsetzt oder nicht. Die neu in § 38bis InfoDG vorgesehene Empfehlung unterscheidet sich von der im geltenden Recht in § 38 vorgesehenen Empfehlung in der Verbindlichkeit und im Rechtsmittelweg.

Die Empfehlungen gemäss noch geltendem § 38 InfoDG sind verbindliche Aufsichtsmassnahmen. Die bzw. der IDSB kann bei einer Nichtbefolgung ein Rechtsmittel ergreifen. Die Empfehlung gemäss § 38bis InfoDG unterscheidet sich auch klar von der Empfehlung gemäss § 36 Absatz 3 InfoDG, welche nach Abschluss eines Schlichtungsverfahrens erlassen wird. Falls die Behörde beabsichtigt, eine Empfehlung gemäss § 36 Absatz 3 InfoDG nicht umzusetzen, so hat sie dies in den in § 37 Absatz 2 InfoDG aufgezählten Fällen zu verfügen.

§ 41 (Gebühren, Datenschutz)
Die Änderung ist rein redaktioneller Natur und trägt der neuen Bezeichnung «Register der Bearbeitungstätigkeiten» Rechnung (vgl. oben, zu § 25 InfoDG).

§ 43bis (Übergangsbestimmung)
Absatz 1 verdeutlicht, dass die neuen gesetzlichen Vorgaben zu den Grundsätzen «privacy by design» und «privacy by default» (§ 16 Abs. 1 Bst. d InfoDG) und zu den Datenschutz-Folgenabschätzungen (§ 30bis InfoDG) nicht rückwirkend gelten (keine unechte Rückwirkung). Bestehende Datenbearbeitungen müssen nicht an die beiden erwähnten Grundsätze angepasst werden und es müssen auch nicht nachträglich Datenschutz-Folgenabschätzungen durchgeführt werden. Wenn aber der Zweck einer bestehenden Datenbearbeitung geändert wird oder wenn neue Kategorien von Daten bearbeitet werden, ist die Datenbearbeitung als eine neue Datenbearbeitung zu betrachten und alle Bestimmungen des InfoDG sind auf diese neue Datenbearbeitung anwendbar. Neue Datenkategorien meinen nicht neu beschaffte Daten im Einzelfall, sondern neue Arten von Daten, welche bisher nicht bearbeitet worden sind (etwa biometrische Daten, Gesundheitsdaten oder die AHV-Nummer). Dies bedeutet insbesondere, dass bei einem hohen Risiko eine Datenschutz-Folgenabschätzung durchgeführt werden muss, und dass die Grundsätze «privacy by design» und »privacy by default» umgesetzt werden müssen, soweit dies bei der bestehenden Datenbearbeitung technisch möglich ist.

Absatz 2 gewährt der bzw. dem IDSB eine Frist von drei Jahren ab Inkrafttreten der Gesetzesänderung, um das Register der Bearbeitungstätigkeiten zu veröffentlichen (§ 25 InfoDG).

4.2 Kantonsratsgesetz (BGS 121.1)

§ 10 Absatz 1
Die Zuständigkeit, um über die Bewilligung von Nebenbeschäftigungen und öffentlichen Ämtern der bzw. des IDSB zu entscheiden, wird der Ratsleitung des Kantonsrats übertragen (Bst. j). Materiell kommt § 42 StPG zur Anwendung. Gemäss dessen Absatz 2 darf die Nebenbeschäftigung die Aufgabenerfüllung nicht nachteilig beeinflussen (d.h. die Ausübung der Funktion, die Unabhängigkeit und das Ansehen der bzw. des IDSB nicht beeinträchtigen).

4.3 Regierungs- und Verwaltungsorganisationsgesetz (RVOG; BGS 122.111)

§ 26
Absatz 4: Redaktionelle Anpassung.

Absatz 6: Der Kantonsrat hat den Auftrag Rolf Sommer (SVP, Olten) «Offenlegung der Entschädigungen» mit folgendem geändertem Wortlaut erheblich erklärt (KRB Nr. A 0034/2021 vom 6. September 2022):

«Der Regierungsrat wird beauftragt, dem Kantonsrat eine Vorlage zu unterbreiten, mit der die gesetzliche Grundlage dafür geschaffen wird, dass Entschädigungen an Mitglieder von Leitungs- und Aufsichtsorgane[n] der mittelbaren Verwaltung auf kantonaler Ebene öffentlich bekannt gemacht werden müssen, soweit nicht zwingende Bestimmungen des Bundesrechts entgegenstehen.»

Da die §§ 26 und 27 RVOG die Aufsicht über die mittelbare Verwaltung regeln, bietet es sich an, den Auftrag durch eine Anpassung dieser Bestimmungen umzusetzen. Es sind sämtliche Entschädigungen aller Mitglieder der Aufsichtsorgane (Verwaltung) jährlich zu veröffentlichen. Auf welchem Weg die Veröffentlichung erfolgt, wird noch festzulegen sein. Für die Geschäftsleitung werden die Entschädigungen gesamthaft sowie einzeln für dasjenige Mitglied mit der höchsten Entschädigung ausgewiesen. Diese Regelung ist Artikel 734a Absatz 3 OR nachgebildet. Unter dem Oberbegriff «Entschädigungen» wird die Gesamtheit der einem Mitglied ausgerichteten geldwerten Vorteile verstanden, die im Zusammenhang mit der Tätigkeit als Mitglied des jeweiligen Organs stehen. Im Sinne grösstmöglicher Transparenz sind die Angaben für jedes Mitglied einzeln zu machen. Die Entschädigungen sind aufgeteilt auszuweisen, einerseits für die (Brutto-)Vergütungen (etwa Jahreslöhne inkl. 13. Monatslohn und Boni, Pauschalhonorare, Stundenhonorare, Sitzungsgelder und Abgangsentschädigungen), andererseits für die Auslagenentschädigungen (etwa Kilometer-Entschädigungen für die Benutzung des eigenen Motorfahrzeugs, Spesenentschädigungen für Billette des öffentlichen Verkehrs oder Pauschalspesen). Damit wird den berechtigten Transparenzinteressen der Öffentlichkeit, die in den letzten Jahren gerade auch im Bereich von staatlichen Unternehmen vermehrt eingefordert werden, Rechnung getragen.

Betroffen sind alle Organisationen der mittelbaren Verwaltung auf kantonaler Ebene unabhängig von ihrer (öffentlich-rechtlichen oder privatrechtlichen) Organisationsform, so etwa die Solothurnische Gebäudeversicherung, die Ausgleichskasse des Kantons Solothurn und die Solothurner Spitäler AG. Soweit es sich um Organisationen handelt, welche durch interkantonales Recht errichtet wurden (z.B. FHNW) oder bei welchen der Kanton Solothurn lediglich über eine Minderheitsbeteiligung verfügt (z.B. NSNW AG), kann eine solche Veröffentlichung durch das kantonale Recht nicht vorgesehen werden. Auch allfällig entgegenstehendes übergeordnetes (Bundes- oder interkantonales) Recht bleibt vorbehalten.

Die Bestimmung umschreibt den Mindestinhalt der Publikationspflicht. Das Öffentlichkeitsprinzip gemäss InfoDG wird durch die Publikationspflicht nicht eingeschränkt. Allfällige Zugangsgesuche sind im Einzelfall gemäss den Bestimmungen des InfoDG zu prüfen.

4.4 Gesetz über den Justizvollzug (JUVG; BGS 331.11)

§ 29bis Absatz 1 und § 31bis Absatz 3
Die Rechtsgrundlagen für die Datenbearbeitung durch die Behörden des Justizvollzugs sind dahingehend anzupassen, dass auch die Vornahme eines Profilings erfasst wird, sofern dies zur Aufgabenerfüllung notwendig ist (vgl. oben, zu § 6 Abs. 6 InfoDG).

4.5 Gesetz über die Kantonspolizei (BGS 511.11)

§ 41 Absatz 2
Es erscheint zweckmässig vorzusehen, dass die Kantonspolizei für die Strafverfolgung auch ein Profiling vornehmen darf, sofern dies zur Aufgabenerfüllung notwendig ist (vgl. oben, zu § 6 Abs. 6 InfoDG).

5. Erledigung von parlamentarischen Vorstössen

Mit dieser Vorlage wird der vom Kantonsrat erheblich erklärte Auftrag Rémy Wyssmann (SVP, Kriegstetten) «Verschleppung von Zugangsgesuchen verhindern» (KRB Nr. A 0147/2021 vom 11. Mai 2022) umgesetzt (s. Ziff. 4.1, zu § 35 InfoDG). Weiter wird mit dieser Vorlage der vom Kantonsrat erheblich erklärte Auftrag Rolf Sommer (SVP, Olten) «Offenlegung der Entschädigungen» (KRB Nr. A 0034/2021 vom 6. September 2022) umgesetzt (s. Ziff. 4.3, zu § 26 RVOG).

6. Rechtliches

Der Erlass und die Änderung von Gesetzen, die der Kantonsrat mit weniger als zwei Dritteln der anwesenden Mitglieder beschliesst, unterliegen der obligatorischen Volksabstimmung (Art. 35 Abs. 1 Bst. d KV). Werden Gesetze von zwei Dritteln oder mehr der anwesenden Mitglieder beschlossen, unterliegen sie dem fakultativen Referendum (Art. 36 Abs. 1 Bst. b KV).

7. Antrag

Wir bitten Sie, auf die Vorlage einzutreten und dem Beschlussesentwurf zuzustimmen.

Im Namen des Regierungsrates

Sandra Kolly	Yves Derendinger
Frau Landammann	Staatsschreiber

Verteiler KRB

Elektronische Publikation im Ratsinformationssystem
Elektronische Publikation im e-Amtsblatt
Staatskanzlei via Geschäftsverwaltungssystem
Informations- und Datenschutzbeauftragte via Geschäftsverwaltungssystem
GS, BGS
Parlamentsdienste (xxxx/2025)