Solothurn, im März 2026

Staatskanzlei

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

Bemerkungen zu einzelnen Bestimmungen und weitere Anliegen

A. Bemerkungen zu einzelnen Bestimmungen

§ 2 (Geltungsbereich):

Die Angleichung an das europäische Datenschutzrecht werde abgelehnt (14).

§ 6 InfoDG (Begriffe):

Die Aktualisierung der Begriffe – insbesondere die Einführung von *Profiling* als eigenständigem Begriff und dessen rechtliche Gleichstellung mit besonders schützenswerten Personendaten schaffe klare Rechtsgrundlagen für den Einsatz datengestützter Systeme in der Verwaltung (13).

Die Angleichung an das europäische Datenschutzrecht werde abgelehnt (14).

§ 15 Abs. 3 InfoDG (Rechtsgrundlage):

Da im Gesetz der Begriff des «Persönlichkeitsprofils» beibehalten wird, müsste er auch in Absatz 3 erwähnt werden (13).

Die Angleichung an das europäische Datenschutzrecht werde abgelehnt (14).

§ 16 InfoDG (Grundsätze):

Die Angleichung an das europäische Datenschutzrecht werde abgelehnt (14).

Es sei schwierig, abzuschätzen, ob der neue Bst. c mit seinen offenen Begriffen geeignet ist, die gewünschte Funktion zu erfüllen. Es werde unterstützt, dass die Umsetzung dem DSG folgend keine Rechenschaftspflicht verankern will (20).

§ 16bis Abs. 3 InfoDG (visuelle Überwachung):

Es sei nachvollziehbar, dass der Begriff «verantwortliche» Behörde nicht mehr verwendet werden soll. Die Formulierung sei aber unpräzise, wenn lediglich «Behörde» erwähnt werde. Es könnte der Begriff «zuständige Behörde» verwendet werden, so auch an anderer Stelle, etwa in § 18ter InfoDG (13).

§ 17 InfoDG (Auftragsdatenbearbeiter und Auftragsdatenbearbeiterinnen):

Die Angleichung an das europäische Datenschutzrecht werde abgelehnt (14).

Eine Kaskadenbeauftragung mit sensiblen Daten werde kritisch betrachtet (Abs. 3). Die Kontrolle solcher Delegationen scheine in der Praxis kaum möglich, auch wenn sich der Artikel am DSG orientiere. Wichtig sei, Aufträge vor allem an Anbieter zu erteilen, die diesen möglichst ohne weitere Delegation erfüllen könnten (20).

§ 18bis InfoDG (Informationspflicht):

Die Angleichung an das europäische Datenschutzrecht werde abgelehnt (14).

Dass die Informationspflicht immer dann entfallen solle, wenn die Datenbearbeitung in einem Gesetz oder einer Verordnung vorgesehen ist und dass dafür bereits mittelbare Rechtsgrundlagen (d.h. wenn die Datenbearbeitung nicht explizit, sondern nur eine Aufgabenerfüllung geregelt ist) genügen sollen, sei bedenklich. Diese Lösung möge auf Bundesebene plausibel erscheinen, weil dort die Rechtsgrundlagen oft viel bestimmter seien. Auf kantonaler Ebene, wo unbestimmte, mittelbare Rechtsgrundlagen verbreitet seien, führe dies zu einem grossen Transparenzdefizit. Eine Rechtsgrundlage sollte nur dann die Informationspflicht entfallen lassen, wenn für die betroffene Person aus ihr alle nach der Informationspflicht zu liefernden Angaben klar erkennbar seien. Für diese Variante habe sich z.B. auch der Gesetzgeber im Kanton Basel-Stadt entschieden. Sie werde von diversen Stimmen in der Lehre auch für den Bund vertreten[1] (16).

§ 18ter InfoDG (Informationspflicht bei einer automatisierten Einzelentscheidung):

Die Regelung werde ausdrücklich unterstützt, die Möglichkeit einer menschlichen Überprüfung sei zwingend (11, 13, 16). Allerdings zeichne sich bereits ab, dass die Beschränkung der Pflicht auf vollautomatisierte Entscheidungen für eine Umsetzung der KI-Konvention des Europarates nicht genügt[2]. Es werde daher angeregt, die Informationspflicht auch auf teilweise automatisierte Entscheide auszuweiten (16).

Die Angleichung an das europäische Datenschutzrecht werde abgelehnt (14).

§§ 24 und 25 InfoDG (Verzeichnis der Bearbeitungstätigkeiten):

§§ 24, 25 und 43bis InfoDG seien wie folgt anzupassen (5):

§ 24 Abs. 3 (geändert), Abs. 4 (streichen)
3 Das Verzeichnis ist zu veröffentlichen. Der Regierungsrat kann in einer Verordnung Ausnahmen vorsehen.
4 ~~Die Behörden melden ihre Verzeichnisse dem oder der Beauftragten.~~

§ 25 Abs. 1 (streichen)
~~1 Der oder die Beauftragte führt ein Register der Bearbeitungstätigkeiten der Behörden. Diesesenthält die Angaben nach § 24 Absatz 2 und wird veröffentlicht.~~

§ 43bis (neu) Abs. 2 (geändert)
2 Die Behörden veröffentlichen ihre Verzeichnisse nach § 24 Absatz 3 innert dreier Jahre nach Inkrafttreten dieses Gesetzes. Das zentrale Register der Datensammlungen ist noch während dreier Jahre nach Inkrafttreten dieses Gesetzes bei dem oder der Beauftragten einsehbar.

Die vorliegend beantragten Änderungen würden der Version entsprechen, wie sie im Rahmen des Mitberichtsverfahrens erarbeitet worden sei. Die IDSB müsste hingegen für die Umsetzung einer zentralen digitalen Publikationsmöglichkeit eine Applikation beschaffen mit Kosten in oberer sechsstelliger Höhe[3]. Diese Kosten würden bei der Regelung gemäss Mitberichtsfassung nicht anfallen. Die Behörden könnten ihre Verzeichnisse selbst und mit einfacheren Mitteln publizieren, bspw. durch Aufschaltung auf ihrer Website oder durch periodische Bekanntgabe im Amtsblatt. Damit würde auch die Meldepflicht mit dem entsprechenden Aufwand in der Umsetzung wegfallen. Auch inhaltlich seien keine Vorteile einer zentralen Publikation gegenüber der behördenseitigen Publikationspflicht erkennbar. Die verantwortlichen Behörden seien (wie bereits heute im Rahmen der Datensammlungen) zur Führung des Datenbearbeitungsverzeichnisses verpflichtet. Ein solches Verzeichnis diene der Compliance. Es verschaffe den jeweils verantwortlichen Behörden Wissen über die bei ihr stattfindenden Bearbeitungstätigkeiten, was Vo-

[1] Vgl. OFK DSG-Bieri/Powell, Art. 20 N 11 und CR DSG-Flückiger, Art. 20 N 6.
[2] Vgl. dazu Julian Powell/Liliane Obrecht, Anforderungen der KI-Konvention des Europarats an automatisierte Einzelentscheidungen, SJZ 3/2026. Vgl. auch Bundesamt für Justiz, Rechtliche Basisanalyse im Rahmen der Auslegeordnung zu den Regulierungsansätzen im Bereich künstliche Intelligenz vom 31. August 2024, S. 71.
[3] Gemäss Erfahrungswerten des EDÖB im Zusammenhang mit der Plattform «Datareg».

raussetzung für deren Steuerung und Prüfung darstelle. Ebenfalls werde dadurch die Gewährleistung der Betroffenenrechte besser sichergestellt (z.B. im Rahmen des Auskunftsrechts). Denn diese seien stets bei der verantwortlichen Behörde geltend zu machen (5).

Alle Datenbearbeiter zur Führung von Verzeichnissen zu verpflichten, welche dann wiederum in einem Register geführt würden, gehe zu weit (grosser Aufwand für alle Beteiligten) (8).

Die Angleichung an das europäische Datenschutzrecht werde abgelehnt (14).

Auch die Verzeichnisse von externen Auftragsdatenbearbeitenden sollten der bzw. dem IDSB geschickt und im zentralen Register geführt werden müssen (20).

§ 30bis InfoDG (Datenschutz-Folgenabschätzung [DSFA]):

Die DSFA sei nicht notwendig und verursache für die Gemeinden zusätzlichen administrativen Aufwand. Sie sei für das Miliz-System nicht tauglich und bedürfe einer klaren Neuregelung bzw. einer gänzlichen Streichung (3, 19). Es sei darauf zu achten, dass der Datenaustausch unter den Gemeinden, mit den Sozialdiensten und den kantonalen Stellen uneingeschränkt möglich sei und nicht mit weiteren Hürden erschwert werde (19).

Die Einführung müsse pragmatisch erfolgen und dürfe Digitalisierungsvorhaben nicht verhindern. Für die Prüfung der DSFA durch die bzw. den IDSB sei eine Frist von einem Monat einzuführen, analog Art. 23 Abs. 2 DSG (6). Die Prüfung der DSFA durch die bzw. den IDSB müsse zeit- und praxisnah erfolgen (20).

Trotz der grundsätzlich anerkennenswerten Zielsetzung sei die vorgesehene Regelung kritisch zu beurteilen, v.a. betr. den erheblichen zusätzlichen administrativen, organisatorischen und personellen Aufwand, der mit der DSFA verbunden wäre. Bei «entsprechenden Projekten» sei eine umfassende Prüfung vorzunehmen und diese auch dokumentiert nachzuweisen. Jedes grössere Digitalisierungsvorhaben – etwa die Einführung neuer Einwohnerdienste-Portale, neuer Fachsoftware, Cloud-Lösungen, Schnittstellen zu kantonalen Systemen oder neue Kommunikationsplattformen – müsste nicht nur technisch und finanziell geplant, sondern zusätzlich datenschutzrechtlich formalisiert beurteilt werden. Dies binde Ressourcen und verzögere Projekte. Viele, auch grössere, Gemeinden verfügten nicht über spezialisiertes juristisches, datenschutzrechtlich geschultes Fachpersonal. Die Folge wäre eine Mehrbelastung bestehender Verwaltungsstellen oder der Zwang, externe Beratungsleistungen mit entsprechenden Mehrkosten beizuziehen. Der Gesetzestext lasse auch offen, bei welchen Projekten eine DSFA zwingend erforderlich sei und welche Anforderungen konkret erfüllt werden müssten. Die Unklarheit werde in der Praxis dazu führen, dass Gemeinden aus Vorsicht zu häufig DSFA durchführen oder – aus Ressourcenmangel – darauf verzichten und damit rechtliche Risiken eingehen würden. Eine solche Situation sei weder im Sinne der Rechtssicherheit noch im Sinne eines effizienten Verwaltungshandelns und könnte zu unnötigen Doppelspurigkeiten führen (10).

Gemäss Art. 23 DSG seien die DSFA der verschiedenen Behörden nur dann dem Eidgenössischen Datenschutzbeauftragten (EDÖB) zur Stellungnahme zu unterbreiten, wenn die geplante Bearbeitung trotz der vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge habe. Abs. 4 sei ersatzlos zu streichen. Denn es dürfe erwartet werden, dass die DSFA durch die betroffene Behörde eine Qualität erreicht, die nicht nochmals kosten- und personalintensiv überprüft werden muss (12).

Die Verpflichtung zu einer vorgängigen DSFA sei ein klassisches Beispiel für ein bürokratisches Monster, das keinen messbaren Sicherheitsgewinn für den Bürger bringe, aber die Verwaltung massiv lähme. Diese führe in der kantonalen sowie kommunalen Verwaltung zu prozessualem Leerlauf. Einwohnergemeinden und Zweckverbände verfügten weder über die personellen noch über die finanziellen Ressourcen, um für jedes neue Projekt komplexe, theoretische Risikoanalysen zu erstellen. Die Folge wäre eine kostspielige Abhängigkeit von externen Beratern und ein weiterer Ausbau der Verwaltung auf Kosten der Steuerzahler. In einer Zeit, in der der Kanton Solothurn sowie zahlreiche Gemeinden mit massiven strukturellen Defiziten kämpften, sei es

unverantwortlich, neue administrative Hürden zu schaffen, die den geschätzten Mehrbedarf an Stellenprozenten weiter befeuerten (14).

Eine DSFA für besonders schützenswerte Daten könne sinnvoll sein und werde begrüsst, doch seien die genauen Auswirkungen auf die Verwaltung und die Mehrbelastung, die dadurch allenfalls entstehe, schwer abschätzbar (20).

§ 30ter InfoDG (Meldung von Verletzungen der Datensicherheit) und § 30quater InfoDG (Verantwortung):

Die Angleichung an das europäische Datenschutzrecht werde abgelehnt (14).

§ 32 Abs. 1 InfoDG (Aufgaben):

Der gesetzliche Auftrag zur Sensibilisierung der Bevölkerung (Bst. b) sei zentral. Es sei notwendig, hierbei insbesondere Minderjährige sowie besonders verletzliche Personen in den Fokus zu nehmen (11).

Der erweiterte Aufgabenkatalog, insbesondere die Prüfung von DSFA im Rahmen von Vorabkontrollen und die Entgegennahme von Meldungen über Datensicherheitsverletzungen, stärke die Stellung der Aufsichtsbehörde zusätzlich (13).

§ 33ter InfoDG (Datenschutzberater oder Datenschutzberaterin):

Die Funktion der Datenschutzberaterin bzw. des Datenschutzberaters müsse mit den bestehenden Strukturen einer Gemeinde wahrgenommen werden können. Eine unabhängige «Mini-Datenschutzbeauftragte»-Funktion müsste auf Gemeindeebene in der Praxis wohl mit einer separaten Anstellung gelöst werden. Dies sei mit Blick auf die Arbeitsabläufe in den Gemeinden nicht effizient und finanziell nicht vertretbar (3, 19). Ausserdem sollte mit Blick auf die Gemeindeautonomie die Kompetenz zur Festlegung von adäquaten Strukturen und Rollen im Datenschutzbereich beim Gemeinderat statt beim Regierungsrat liegen (3). Die Einführung bedeute unnötige Bürokratie mit einem Stellen- und Kostenwachstum (8). Der in Abs. 2 verankerte Grundsatz, dass mehrere Behörden gemeinsam eine Datenschutzberaterin oder einen Datenschutzberater ernennen können, sei prioritär umzusetzen (12).

Für die Stadtpolizei Solothurn müsste eine entsprechende Funktion geschaffen oder zumindest formell zugewiesen werden. Zwar könne gerade im strafrechtlichen Bereich mit dem erhöhten datenschutzrechtlichen Risiko eine interne Fachverantwortung sinnvoll sein. Dennoch sei kritisch festzuhalten, dass diese Pflicht in der Praxis nicht ohne zusätzliche personelle Ressourcen erfüllbar sei. Innerhalb der Stadtverwaltung Solothurn übernehme der Rechtsdienst heute die Aufgaben der bzw. des kommunalen IDSB im Sinne von § 31 Abs. 6 InfoDG. Der Aufgabenbereich umfasse ebenfalls die datenschutzrechtlichen Fragestellungen der Stadtpolizei. Weiter könne die erforderliche Unabhängigkeit einer Datenschutzberaterin oder eines Datenschutzberaters innerhalb der bestehenden Organisationsstrukturen nicht gewährleistet werden. Dies würde die Schaffung einer neuen Stelle oder die Auslagerung mit entsprechenden Mehrkosten bedeuten. Es sei weiter nicht ersichtlich, welche Voraussetzungen die Funktion in fachlicher Hinsicht konkret erfüllen müsse (10).

Die Einführung einer Pflicht für Strafverfolgungs-, Strafgerichts- und Strafvollzugsbehörden sowie die Stadtpolizei Solothurn, Datenschutzberaterinnen und -berater zu ernennen, sei ein wichtiger Schritt zur Professionalisierung des Datenschutzes in besonders sensiblen Bereichen. Gefordert werde aber, dass diese Funktion nicht als rein administrative Aufgabe verstanden, sondern mit ausreichenden personellen und finanziellen Ressourcen ausgestattet wird, um ihre Beratungs- und Kontrollfunktion wirksam wahrnehmen zu können (13). Es fehle innerhalb der Departemente an Knowhow im Bereich des Datenschutzes. Gemäss DSGVO müsse jede öffentliche Dienststelle eine Datenschutzberaterin oder einen Datenschutzberater benennen, was aber aufgrund der teilweise kleinen Ämter wenig sinnvoll wäre. Im Sinne einer pragmatischen Minimal-

lösung werde daher angeregt, analog zur Regelung im Kanton Basel-Stadt[4], die Einführung von internen Datenschutzberaterinnen oder -beratern für alle Departemente der kantonalen Verwaltung, die Gerichte sowie die Einwohner- und Bürgergemeinden vorzusehen (16).

Die Angleichung an das europäische Datenschutzrecht werde abgelehnt (14).

§ 36 ff. InfoDG (Schlichtungsverfahren):

Es werde begrüsst, dass sich die Vorlage in verschiedenen Punkten am Öffentlichkeitsgesetz des Bundes (BGÖ) orientiere. Dies erhöhe die Rechtssicherheit für Nutzende der entsprechenden Rechte, da auf Bundesebene eine breite Rechtspraxis und klare Leitlinien bestünden (2).

Es werte das Schlichtungsverfahren auf, dass der Instanzenweg zwingend über ein solches führe (§ 37 Abs. 2 InfoDG). Durch den Austausch von Verwaltung und Gesuchstellenden könne im besten Fall eine Lösung gefunden und könnten die Gerichte entlastet werden (2).

Die Möglichkeit, dass die Nichteinhaltung von Fristen bei der Schlichtungsstelle gerügt werden kann (§ 36 Abs. 1 InfoDG), werde begrüsst (2, 14). Diese Neuerung sei die zwingende Konsequenz aus der Einführung verbindlicher Erledigungsfristen. Bisher seien die Zugangsrechte durch exzessive Bearbeitungszeiten behindert worden. Mit der Rügemöglichkeit bei der Schlichtungsstelle erhalte der Bürger ein niederschwelliges Instrument, um die Verwaltung an ihre Pflichten zu erinnern (14).

§§ 38 und 38bis InfoDG (Verfügungskompetenz der bzw. des IDSB):

Die Einführung einer Verfügungskompetenz würde die bzw. den IDSB unverhältnismässig gegenüber den anderen Behörden stärken. Dies werde abgelehnt (4, 8, 12). Dies sei auch verfassungsrechtlich fragwürdig und die von der Botschaft angesprochene Notwendigkeit nicht hinreichend plausibilisiert (4).

Entgegen der Regelung im DSG gestehe die Vorlage der bzw. dem IDSB auch bei einer «drohenden Verletzung» die Kompetenz zu, Verfügungen zu erlassen, was abgelehnt werde. Damit werde der bzw. dem IDSB ein zu weiter Interpretationsspielraum eröffnet (20).

§ 43bis InfoDG (Übergangsbestimmung):

Sollte auf die beantragte Anpassung von §§ 24 und 25 InfoDG verzichtet werden, sei § 43bis InfoDG wie folgt anzupassen (5):

§ 43bis (neu) Übergangsbestimmungen zur Gesetzesänderung vom … 2026 (Abs. 2 geändert)
[2] Der oder die Beauftragte veröffentlicht das Register nach § 25 innert *vier* Jahren nach Inkrafttreten dieses Gesetzes. *Die gemeldeten Verzeichnisse der Bearbeitungstätigkeiten sind während dieser Zeit bei der oder dem Beauftragten einsehbar.*

§ 29bis Abs. 1, § 31bis Abs. 3 JUVG und § 41 Abs. 2 Gesetz über die Kantonspolizei:

Die Angleichung an das europäische Datenschutzrecht werde abgelehnt (14).

[4] § 16b IDG BS.

B. Zusätzliche Anliegen

In Bezug auf das Öffentlichkeitsprinzip:

Das Verhältnis des InfoDG zum Gemeindegesetz (GG) müsse geklärt werden. Aufgrund von Praxiserfahrungen seien dabei mit Blick auf die §§ 31 und 31bis GG folgende Punkte von Bedeutung:

- Gesetzliche Grundlagen für die Einsicht in nichtöffentliche Gemeinderatsprotokolle,

- Gesetzliche Grundlage für die Einsichtnahme in Akten, welche der Gemeinderat beim Entscheidungsfindungsprozess verwendet hat.

In diesem Bereich werde eine konsequente Berücksichtigung der Gemeindeautonomie gefordert, welche insbesondere nicht durch eine Übersteuerung des Gemeindegesetzes (GG) mit dem teilrevidierten InfoDG beschränkt werden dürfe (3).

Es sollte eine Regelung zum gebührenfreien Zugang zu amtlichen Dokumenten vorgesehen werden. Mindestens auf Verordnungsebene sei festgehalten, was als «ausserordentlicher Aufwand» gelte. Dabei müsse der ideelle Wert des Öffentlichkeitsprinzips schwerer wiegen als die beim Bund geltenden acht Stunden gebührenfreier Aufwand. Weiter sei eine Statistik über gutgeheissene, abgelehnte oder teilweise abgelehnte Zugangsgesuche einzuführen (2).

Für die Schnittstelle Datenschutz / Öffentlichkeitsprinzip wird eine analoge Regelung wie auf Bundesebene wie folgt beantragt (5):

§ 14 Zugang zu amtlichen Dokumenten mit Personendaten
[1] Amtliche Dokumente, die Personendaten enthalten, sind nach Möglichkeit vor dem Zugang zu anonymisieren.
[2] Für Personendaten, die nicht anonymisiert werden können, gelten die Bestimmungen dieses Gesetzes über die Bekanntgabe von Personendaten (§ 21 – 23).

§ 21 Rechtsgrundlage
1bis Behörden dürfen im Rahmen der amtlichen Information nach den Bestimmungen dieses Gesetzes (§ 7 – 10) oder gestützt auf ein Zugangsgesuch nach den Bestimmungen dieses Gesetzes (§ 12 – 14) auch Personendaten bekannt geben, wenn

a) die betreffenden Personendaten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen; und
b) an deren Bekanntgabe ein überwiegendes öffentliches Interesse besteht.

Zur Begründung wird angeführt, die heutige Praxis der IDSB und des Verwaltungsgerichts in Bezug auf den Zugang zu amtlichen Dokumenten mit Personendaten stehe nicht im Einklang mit der grammatikalischen Auslegung von § 14 InfoDG. Diese Praxis richte sich nach der ständigen Rechtsprechung des Bundesverwaltungs- sowie des Bundesgerichts und der herrschenden Lehre zum Öffentlichkeitsprinzip. Aus Gründen der Transparenz und Rechtssicherheit sollte diese Bestimmung revidiert werden. Dabei solle man sich bei der Formulierung der Schnittstelle zwischen Datenschutz und Öffentlichkeitsprinzip an den Bestimmungen des DSG und des BGÖ orientieren. Ein damit verbundener Mehraufwand für die dem Öffentlichkeitsprinzip unterliegenden Behörden sei nicht erkennbar. Auch gemäss dem aktuellen Wortlaut seien sie gestützt auf das Verhältnismässigkeitsprinzip verpflichtet, durch allfällige Schwärzungen einen Zugang nur so weit einzuschränken, als dies zum Schutz überwiegender öffentlicher oder privater Interessen tatsächlich notwendig sei (5).

§ 5bis Abs. 1 Planungs- und Baugesetz (PBG) solle gestrichen werden. Der Zugang zu amtlichen Dokumenten aus Verfahren, welche gestützt auf das Planungs- und Baugesetz geführt werden,

müsse gemäss den Bestimmungen der Aarhuskonvention[5] gewährt werden. Der bestehende § 5bis Abs. 1 PBG verschleiere dieses Recht und vermittle den falschen Anschein, die Dokumente des erstinstanzlichen nichtstrittigen Verfahrens nach PBG seien grundsätzlich nicht einsehbar. Sämtliche übrigen erstinstanzlichen nichtstrittigen Verwaltungsverfahren im Kanton Solothurn unterlägen dem Geltungsbereich des Öffentlichkeitsprinzips. Dessen Anwendung sei unbestritten und bislang habe es keine praktischen Anwendungsschwierigkeiten bei der Umsetzung durch die Behörden gegeben. Die bestehende Regelung von § 5bis Abs. 1 PBG stelle eine singuläre, inhaltlich nicht begründbare Ausnahmebestimmung dar in einem Bereich, in welchem auf internationaler Ebene das öffentliche Interesse am Zugang zu Informationen allgemein als hoch eingestuft werde. Das Streichen dieser Bestimmung sei aus Gründen der Transparenz und Rechtssicherheit unverzichtbar, ohne dass sich für die Behörden Nachteile ergeben würden (5, 16).

Die Praxis zeige, dass eine zunehmend weitgehende Auslegung des (grundsätzlich anerkannten) Öffentlichkeitsprinzips – insb. durch die bzw. den IDSB – die Handlungs- und Verhandlungsfähigkeit von Regierung und Verwaltung erheblich einschränken könne. Dies betreffe vor allem Konstellationen, in denen eine Veröffentlichung zwar formell dem Transparenzgedanken entspreche, materiell jedoch staatliche Interessen beeinträchtige oder sachlich nicht gerechtfertigte Fehlanreize setze. Das Öffentlichkeitsprinzip sei so auszugestalten, dass Transparenz und demokratische Kontrolle gewährleistet sind, ohne die Funktions- und Handlungsfähigkeit des Kantons zu beeinträchtigen. Dazu gehöre auch, dass das Gesetz für bestimmte, klar umschriebene Konstellationen festlege, in welcher Form Transparenz und Kontrolle wahrgenommen würden. Es erscheine zumindest als problematisch, wenn die Auslegung und Durchsetzung des Öffentlichkeitsprinzips in allen Bereichen primär einer einzelnen, nicht demokratisch legitimierten Stelle mit stetig wachsenden Kompetenzen übertragen werde. Stattdessen werde angeregt, das Öffentlichkeitsprinzip in sensiblen Bereichen durch eine verstärkte parlamentarische Kontrolle sicherzustellen, namentlich durch die Geschäftsprüfungskommission (GPK). Diese sei demokratisch legitimiert, plural zusammengesetzt und mit dem Umgang vertraulicher Informationen bestens vertraut. Sie sei damit geeignet, Transparenz und Kontrolle zu gewährleisten, ohne laufende Geschäfte der Exekutive zu beeinträchtigen oder deren Verhandlungsposition zu schwächen. Dies betreffe insbesondere strategisch sensible Geschäfte, wie etwa Kaufverträge über Liegenschaften, wenn der Kanton beabsichtige, diese zu einem späteren Zeitpunkt weiter zu veräussern oder wenn vertraglich Stillschweigen vereinbart worden sei (z.B. arbeitsrechtliche Aufhebungs- oder Abfindungsvereinbarungen). Hier könne eine Veröffentlichung unerwünschte Anreizwirkungen entfalten, die Personalführung erschweren oder Erwartungen schaffen, die einer sachgerechten Behandlung künftiger Einzelfälle entgegenstehen. Es könnten auch weitere sensible Sachverhalte betroffen sein, etwa Vergleichsvereinbarungen oder aussergerichtliche Einigungen, Berichte der kantonalen Finanzkontrolle sowie andere strategische Transaktionen oder Beteiligungsgeschäfte, bei denen eine Offenlegung die Rechtsposition oder die Handlungsfähigkeit des Kantons beeinträchtigen würde. Die konkrete Umschreibung dieser Sachverhalte sei im Gesetzgebungsprozess weiter zu präzisieren. Die GPK solle solche Geschäfte einer Kontrolle hinsichtlich Rechtmässigkeit, Zweckmässigkeit und Nachvollziehbarkeit unterziehen. Die Entscheidkompetenz der Regierung solle gewahrt bleiben; eine Veröffentlichung der geprüften Inhalte sei nicht bzw. nicht umgehend vorgesehen. Die GPK solle auch prüfen, ob und wann die sachlichen Gründe für eine vorübergehende Nichtveröffentlichung entfallen würden (12).

Regelungen zu künstlicher Intelligenz (KI):

Die Teilrevision thematisiere die technologischen Aspekte wenig bis gar nicht. In der Vernehmlassungsvorlage würden insbesondere gesetzliche Rahmenbedingungen und lösungsorientierte regulatorische Ansätze fehlen, welche die Nutzung der enormen Potenziale der KI im Verwaltungsalltag definieren. Die vollständige Ausklammerung des KI-Themenfelds aus der Teilrevision des InfoDG sei eine verpasste Chance (3).

[5] Übereinkommen über den Zugang zu Informationen, die Öffentlichkeitsbeteiligung an Entscheidungsverfahren und den Zugang zu Gerichten in Umweltangelegenheiten (SR 0.814.07).

Gefordert werde die Aufnahme einer Bestimmung über ein öffentliches Verzeichnis algorithmischer Entscheidsysteme nach dem Vorbild des Zürcher IDG. Eine mögliche Formulierung könnte in etwa lauten (13):

§ Y Verzeichnis algorithmischer Entscheidsysteme
[1] Öffentliche Organe führen ein Verzeichnis über den Einsatz algorithmischer Entscheidsysteme, die geeignet sind, Grundrechte oder andere wesentliche Interessen betroffener Personen zu berühren.
[2] Das Verzeichnis enthält mindestens Angaben über den Zweck des Systems, die Art der Datenbearbeitung, die betroffenen Personenkreise, die verwendeten Datenquellen sowie die Verantwortlichkeiten.
[3] Die bzw. der Informations- und Datenschutzbeauftragte führt das Verzeichnis öffentlich zugänglich und unterstützt die öffentlichen Organe bei dessen Führung.
[4] Der Regierungsrat regelt die Einzelheiten in einer Verordnung.

Das Zürcher IDG verpflichte alle öffentlichen Organe, den Einsatz algorithmischer Entscheidsysteme, die Grundrechte berühren können, in ein Verzeichnis einzutragen. Dieses Verzeichnis sei öffentlich zugänglich und schaffe damit maximale Transparenz (13).

Erschwerter und teilweise verunmöglichter Datenaustausch zwischen verschiedenen Staatsebenen:

Die Erfahrungen der Gemeinden (inkl. Sozialregionen und Zweckverbände) zeigten, dass bereits die aktuellen gesetzlichen Grundlagen des InfoDG den sinnvollen und teilweise zwingend notwendigen Austausch von Daten zwischen den verschiedenen Staatsebenen sowie Institutionen erschweren oder teilweise verunmöglichen würden. Es werde auf die immer noch ungeklärten datenschutzrechtlichen Fragestellungen im Projekt «Harmonisierte Fallführung» (HFF) der Sozialregionen hingewiesen. Diesbezüglich bestehe Klärungsbedarf im Verhältnis zwischen dem InfoDG und dem Sozialgesetz (3).

Digitale Souveränität:

Die digitale Souveränität des Kantons sei zu stärken. Der Zugriff ausländischer Behörden auf Daten bei ausländischen Cloud-Anbietern sei ein reales Risiko. Sensible Daten der Bevölkerung dürften nicht indirekt fremden Jurisdiktionen unterstellt werden. Technische Innovation sei zu begrüssen, sie dürfe jedoch nicht zulasten der staatlichen Souveränität und des Schutzes der Bevölkerung gehen. Es werde daher angeregt:

- Open-Source-Lösungen verstärkt zu prüfen und wo möglich zu fördern, um Transparenz und Überprüfbarkeit sicherzustellen;
- bei der Nutzung von Cloud-Diensten konsequent auf Verschlüsselungslösungen zu setzen, bei denen die Schlüssel nicht beim Anbieter liegen;
- technologische Lösungen so zu wählen, dass eine menschliche Überprüfung nachvollziehbar und inhaltlich fundiert erfolgen kann (11).

Verantwortung des Kantons in der praktischen Umsetzung:

Neben der gesetzlichen Ausgestaltung werde der Kanton in der Verantwortung gesehen gegenüber allen Institutionen, die öffentliche Aufgaben wahrnehmen würden. Viele dieser Stellen stünden unter erheblichem Druck, digitale Lösungen effizient einzusetzen. Gleichzeitig verfügten sie nicht immer über die notwendigen Ressourcen oder die fachliche Expertise, um komplexe datenschutzrechtliche Fragestellungen – insbesondere im Umgang mit internationalen Technologiekonzernen – eigenständig zu beurteilen. Der Kanton dürfe diese Verantwortung nicht an einzelne Institutionen delegieren. Es brauche verbindliche Leitplanken, geprüfte Standardlösungen sowie zentrale Beratungs- und Unterstützungsangebote (11).

Open Government Data (OGD):

Gefordert werde die Aufnahme einer OGD-Bestimmung nach dem Vorbild des Zürcher IDG. Eine mögliche Formulierung könnte lauten (13):

§ X Open Government Data
[1] Öffentliche Organe stellen ihre Daten, soweit diese nicht dem Datenschutz, dem Urheberrecht, der Sicherheit oder anderen überwiegenden öffentlichen oder privaten Interessen unterliegen, in offenen, maschinenlesbaren Formaten unentgeltlich zur Verfügung.
[2] Der Regierungsrat regelt die Einzelheiten der Bereitstellung, Nutzung und Lizenzierung offener Behördendaten in einer Verordnung. Er kann die Zusammenarbeit mit Bund, anderen Kantonen und Gemeinden vorsehen.
[3] Die bzw. der Informations- und Datenschutzbeauftragte berät die öffentlichen Organe bei der Umsetzung von Open Government Data und koordiniert die Publikation.

Es fehle eine Bestimmung, die öffentliche Stellen verpflichtet oder ermutigt, nicht personenbezogene Daten proaktiv in offenen, maschinenlesbaren Formaten zur Verfügung zu stellen. OGD seien ein zentraler Baustein moderner Verwaltung. Der Bund verfolge mit der OGD-Strategie 2019–2023 und dem aktuellen Masterplan 2024–2027 das Prinzip «open by default». Zahlreiche Kantone – insbesondere Zürich – hätten diesen Ansatz in ihre Informations- und Datenschutzgesetze integriert. Der Kanton Solothurn habe mit seiner Digitalisierungsstrategie wichtige Grundlagen gelegt. Eine OGD-Regelung im InfoDG würde diese Strategie konsequent ergänzen (13).

Schutz von Daten juristischer Personen:

Die Vorlage behalte bewusst den Schutz von Daten juristischer Personen im InfoDG bei. Begründet werde dies damit, dass andernfalls zahlreiche andere Rechtsgrundlagen (z.B. betr. Amtsgeheimnis) anzupassen wären. Das revidierte DSG beschränke den Schutz auf natürliche Personen. Diese Beschränkung entspreche dem internationalen Standard (DSGVO, Konvention 108+) und trage der Tatsache Rechnung, dass der Datenschutz in erster Linie dem Schutz der Grundrechte natürlicher Personen diene. Geschäftsgeheimnisse und andere Interessen juristischer Personen seien bereits durch andere Rechtsinstitute geschützt (Zivilrecht, Strafrecht, Wettbewerbsrecht). Die Beibehaltung des Schutzes juristischer Personen im Solothurner InfoDG führe zu einer Ungleichbehandlung und Rechtsunsicherheit: Während für private Unternehmen und Bundesbehörden nur natürliche Personen geschützt seien, gelte im Kanton Solothurn ein erweiterter Schutz. Dies erschwere die Rechtsanwendung und könne zu Widersprüchen führen, insbesondere bei grenzüberschreitenden oder interkantonalen Datenbearbeitungen. Es werde empfohlen, den Schutz von Daten juristischer Personen im InfoDG mittelfristig zu streichen und die notwendigen Anpassungen in anderen Erlassen im Rahmen eines separaten Bereinigungserlasses vorzunehmen (13).

Revisionsbedarf in weiteren Gesetzen:

Es werde darauf hingewiesen, dass sich der Harmonisierungsbedarf in Bezug auf die in der EU geänderte Rechtslage nicht auf das InfoDG beschränke und in weiteren Gesetzen Revisionen notwendig seien (16).