KANTON solothurn

Regierungsratsbeschluss

vom 22. Oktober 2024

Nr. 2024/1680

Gesetz über die Auslagerung von Informatikdienstleistungen (Auslagerungsgesetz, AusG)
Kenntnisnahme vom Vernehmlassungsergebnis und weiteres Vorgehen

---

1. Vernehmlassungsverfahren

Der Regierungsrat hat am 30. April 2024 den Vernehmlassungsentwurf zum «Gesetz über die Auslagerung von Informatikdienstleistungen (Auslagerungsgesetz, AusG)» beraten und beschlossen. Das Finanzdepartement wurde ermächtigt und beauftragt, über den Entwurf ein öffentliches Vernehmlassungsverfahren durchzuführen. Die Vernehmlassungsfrist endete am 31. August 2024.

1.1 Eingereichte Vernehmlassungen

Am Vernehmlassungsverfahren haben sich nachstehende Organisationen beteiligt (geordnet nach Eingangsdatum):

- SP Kanton Solothurn (1)
- SVP Kanton Solothurn (2)
- Solothurner Handelskammer (3)
- FDP.Die Liberalen Kanton Solothurn (4)
- Evangelische Volkspartei (5)
- Grüne Kanton Solothurn (6)
- Die Mitte Kanton Solothurn (7)

1.2 Verzicht auf eine Vernehmlassung

Auf eine Vernehmlassung ausdrücklich verzichtet haben:

- glp Kanton Solothurn

2. Grundsätzliche Haltung zum Gesetzesentwurf

In den Vernehmlassungsantworten wird eine gesetzliche Regelung zur Auslagerung von Informatikdienstleistungen grundsätzlich begrüsst. Diese sei schon seit Jahren überfällig und dringend nötig (2) und wichtige Grundlage für das Vorwärtstreiben der Digitalisierung in der Solothurner Verwaltung (3). Das Gesetz sei eine wichtige Massnahme, um den Kanton für die Zukunft zu wappnen und seine Wettbewerbsfähigkeit zu sichern (4) und wichtiger Meilenstein für

den Erfolg der Digitalisierungsstrategie (6) sowie zur Fortführung des Impulsprogrammes SO!Digital (7).

Währenddem sich die Vernehmlassungsadressatinnen darin einig sind, dass Auslagerungen grundsätzlich möglich sein sollen, so wurden doch in einigen Vernehmlassungsantworten Bedenken geäussert, resp. ergab es Fragen bezüglich der Behandlung der besonders schützenswerten Daten (1, 2, 4, 6). Ebenfalls waren Wirtschaftlichkeit (2, 3, 4, 6, 7), Transparenz (2, 5), Zuständigkeiten und Verantwortung (2, 4) sowie die Exitstrategie (1, 6) wiederkehrende Themen.

Die Anliegen der Vernehmlassungsadressatinnen zu diesen Themen werden im Folgenden zusammengefasst wiedergegeben und zusammen mit der Stellungnahme des Finanzdepartementes dargestellt. Anschliessend erfolgen Erwägungen zu den weiteren einzelnen Themen in den Vernehmlassungsantworten.

2.1 Behandlung der besonders schützenswerten Daten

2.1.1 Vernehmlassungen

Die Vernehmlassungsadressatinnen umtreibt die Sorge um die Behandlung der besonders schützenswerten Daten (1, 2, 4, 6). In mehreren Vernehmlassungsantworten wird auf die erhöhte Sorgfalt im Umgang mit besonders schützenswerten Daten hingewiesen. Dass auch diese Daten ausgelagert werden können, darüber besteht Einigkeit. Uneins ist man sich allerdings in dem Punkt, ob eine Auslagerung an einen Dritten ausserhalb der Schweiz möglich sein soll.

Eine Vernehmlassungsadressatin (2) verlangt, dass besonders schützenswerte, sensible oder heikle Daten zwingend nur in der Schweiz bearbeitet werden dürfen. Eine weitere Vernehmlassungsadressatin (6) schliesst sich dieser Forderung an und verlangt, dass eine Bearbeitung von Daten im Ausland wo immer möglich zu vermeiden und für besonders schützenswerte Daten zu verbieten sei. Sollten Daten ausserhalb der Schweiz ausgelagert werden, dann nur an Dritte, die sie auf Servern in der Schweiz oder der EU mit geltendem EU Datenschutzgesetz speichern; besonders schützenswerte Daten dürfen unter keinen Umständen in eine Public Cloud, sondern nur in eine private Cloud, ausgelagert werden und der Gerichtsstand müsse in der Schweiz liegen. Eine Vernehmlassungsadressatin (4) erwägt, dass besonders schützenswerte Daten wenn immer möglich in der Schweiz zu bearbeiten seien und dass der Auslagerungsentscheid nicht allein von der Verwaltung getroffen werden könne, sollte ein Bearbeiten von besonders schützenswerte Daten ausserhalb der Schweiz in Erwägung gezogen werden.

Zwei Vernehmlassungsadressatinnen (2, 4) erwarten eine präzisere, detailliertere und verbindliche Liste von Massnahmen zur Risikominimierung (Ziffer 5.2 der Botschaft).

Eine Vernehmlassungsadressatin (1) weist schliesslich auf die praktischen Schwierigkeiten hin, die sich im Umgang mit den verschiedenen Datenkategorien ergeben. Eine Klassifikation von Daten mache aus rechtlicher Sicht wohl Sinn, bewähre sich in der Praxis aber nicht, da die meisten Personen den Unterschied bei diesen Daten nicht kennen und nur Spezialisten wissen, wo die Daten abgelegt und gesichert werden.

2.1.2 Stellungnahme

Besonders schützenswerte Personendaten und Sachdaten mit erhöhtem Schutzbedarf sind mit grösster Sorgfalt zu behandeln; dies speziell dann, wenn sie zur Bearbeitung an einen Dritten ausgelagert werden. Die gesetzliche Grundlage von § 17 Abs. 1 des Informations- und Datenschutzgesetzes vom 21. Februar 2001 (InfoDG; BGS 114.1) erlaubt es Dienststellen bereits heute besonders schützenswerte Personendaten zur Bearbeitung auszulagern, wenn deren Schutz durch Vereinbarung, Auflagen oder in anderer Weise sichergestellt ist. Art. 85 Abs. 1 Bst. c der

Verfassung des Kantons Solothurn vom 8. Juni 1986 (KV; BGS 111.1) sieht vor, dass Verwaltungsaufgaben ausnahmsweise nach Massgabe des Gesetzes Privaten übertragen werden können. Der Rechtsschutz der Bürger und die Aufsicht des Regierungsrates müssen sichergestellt sein (Abs. 2).

Der Kanton Solothurn verfügt somit bereits heute über eine verfassungsmässige und gesetzliche Regelung, um in einem gewissen Umfang Informatikdienstleistungen Dritter in Anspruch zu nehmen. Aufgrund des sachlichen Geltungsbereichs des InfoDG fehlt aber eine allgemeine Rechtsgrundlage für die Auslagerung von Sachdaten. Die bestehenden Rechtsgrundlagen regeln zudem ungenügend, wie bei besonders bedeutsamen, umfangreichen oder risikobehafteten Auslagerungen (wie beispielsweise bei gewissen Cloud-Lösungen) vorzugehen ist. Das Auslagerungsgesetz ist die weitergehende Rechtsgrundlage, die auch besonders bedeutsame, umfangreiche oder risikobehaftete Auslagerungen von Informatikdienstleistungen möglich macht. Das Auslagerungsgesetz hat aber nicht zum Zweck jede Auslagerung zu legitimieren. Es regelt vielmehr nur die Voraussetzungen, Kompetenzen und Verantwortlichkeiten, die bei einer Auslagerung von Informatikdienstleistungen durch die kantonale Verwaltung einzuhalten sind. Die Zulässigkeit einer Auslagerung muss im Einzelfall geprüft werden und ist vom Ergebnis der Gesamtrisikobewertung abhängig. Die in Ziffer 5.2 der Botschaft angeführte Aufzählung der Massnahmen zur Risikominimierung ist nicht abschliessend. Sind die Voraussetzungen des Auslagerungsgesetzes und ebenfalls der massgebenden datenschutz-, finanz- und submissionsrechtlichen Bestimmungen erfüllt, kann die Datenbearbeitung oder -speicherung von besonders schützenswerten Personendaten und Sachdaten mit erhöhtem Schutzbedarf ausserhalb der Schweiz erfolgen.

Wir stimmen den Vernehmlassungsadressatinnen aber zu, dass die Auslagerung von besonders schützenswerten Personendaten und Sachdaten mit erhöhtem Schutzbedarf grundsätzlich in der Schweiz zu erfolgen hat. Sollte eine Auslagerung an einen Dritten ausserhalb der Schweiz erfolgen, dann nur unter Beachtung von Anhang 1 der Verordnung über den Datenschutz vom 31. August 2022 (Datenschutzverordnung; SR 235.11). Ebenfalls ist grundsätzlich vertraglich die Anwendung von Schweizer Recht vorzubehalten und ein Gerichtsstand in der Schweiz zu vereinbaren, wobei begründete Ausnahmen im Einzelfall zulässig sind. Die Vorlage wird in diesen Punkten angepasst.

Die Begriffe Private Cloud bzw. Public Cloud lassen viel Interpretationsspielraum zu und bieten weitere Unterkategorien an. Die grossen Cloud-Anbieter bieten Public Cloud Lösungen an mit verschiedenen Sicherheitsmechanismen (z.B. Verschlüsselung der Daten). Im Merkblatt Cloudservices der kantonalen Verwaltung ist beschrieben, welche Art von Daten in welchen Cloud-Kategorien unter welchen Bedingungen bearbeitet werden können. Das Auslagerungsgesetz lässt die Bearbeitung in Public Clouds grundsätzlich zu, sofern die gesetzlichen Voraussetzungen dazu erfüllt sind und das Ergebnis der Gesamtrisikobewertung dies zulässt.

Was die Klassifikation der Daten anbelangt, so nimmt das InfoDG bereits eine Einteilung vor. Beispielsweise unterscheidet das InfoDG zwischen Personendaten und besonders schützenswerten Personendaten. Auch nimmt sich die Schutzbedarfsanalyse, die Risikoanalyse und das ISDS-Konzept projektbezogen gerade diesem Thema an. Insbesondere die Schutzbedarfsanalyse ermittelt, wie hoch der Schutzbedarf in Bezug auf Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Daten und Systemen ist.

2.2 Wirtschaftlichkeit

2.2.1 Vernehmlassungen

Das Thema Wirtschaftlichkeit sowie Kosten und Nutzen von Auslagerungen waren ebenfalls Thema in mehreren der eingegangenen Vernehmlassungsantworten (2, 3, 4, 6, 7).

Erwartet werden Effizienzsteigerungen und Mehrwerte für die Kunden und dass der Nutzen die Kosten überwiegt (3, 4). Die Auslagerung von Aufgaben an Dritte führe zu einer Entlastung der Verwaltung, weshalb Einsparungen erwartet werden (7). Eine Vernehmlassungsadressatin (2) verlangt, dass Auslagerungen zwingend zu Kosteneinsparungen führen müssen und keinesfalls Mehrkosten zur Folge haben dürfen, was in den gesetzlichen Bestimmungen entsprechend festzuhalten sei.

Demgegenüber wird in einer Vernehmlassungsantwort (6) davor gewarnt, dass Wirtschaftlichkeitsüberlegungen allein entscheidend sein sollen für einen Auslagerungsentscheid. Durch Auslagerungen könne vielmehr von den allgemeinen Entwicklungen in der Digitalisierung profitiert werden. Wegen der dafür notwendigen Investitionen in die Security Infrastruktur, der personellen Aufwände und der Prozesse zur Risikominimierung fallen Kosteneinsparungen weniger ins Gewicht. Insbesondere sei auf Kompromisse im Datenschutz aus Kostenüberlegungen zu verzichten.

2.2.2 Stellungnahme

Allein durch den Erlass des Auslagerungsgesetzes ist nicht mit personellen oder finanziellen Konsequenzen zu rechnen. Es ist auch nicht Zweck dieses Gesetzes, finanzielle oder personelle Ressourcenallokationen zu regeln. Dies werden dann im konkreten Projekt zu erfolgen haben. In den Ziffern 9.1 und 9.4 der Botschaft wird auf die personellen, finanziellen und wirtschaftlichen Konsequenzen hingewiesen.

Das Auslagerungsgesetz wird Grundlage sein für weitergehende Entscheide in Bezug auf Projekte, welche die Auslagerung von Informatikdienstleistungen zur Folge haben, insbesondere Projekte mit Cloud-Fokus. Die Realisierung dieser Projekte kann personelle und finanzielle Folgen haben und führt damit nicht unmittelbar zu Kosteneinsparungen. Mittelfristig wird aber als Folge der Realisierung dieser Projekte mit einem Effizienzgewinn gerechnet, d.h. der allgemeine Nutzen aus diesen realisierten IT-Projekten wird die Kosten übersteigen. Deshalb macht es nur wenig Sinn bei der Realisierung von IT-Projekten den Fokus allein auf die Kosten zu richten, vielmehr ist es der erwartete Nutzen, der für die Realisierung entscheidend sein soll.

Grundsätzlich wird darauf hingewiesen, dass die digitale Transformation kein Selbstzweck ist und dass in der kantonalen Verwaltung nur Projekte vorangetrieben werden, von denen eine mittelbare Effizienzsteigerung erwartet wird. Die Frage der gesetzlichen Verankerung der Effizienzsteigerung von IT-Projekten wird eines der Themen des sich in Ausarbeitung befindenden Digitalisierungsgesetzes sein.

2.3 Transparenz

2.3.1 Vernehmlassungen

In zwei Vernehmlassungsantworten (2, 5) wird die Forderung nach mehr Transparenz der erfolgten Auslagerungen gestellt. Auslagerungen müssen öffentlich zugänglich, nachvollziehbar dokumentiert, ausgewiesen sein und dem Parlament und der Öffentlichkeit zeitnah zur Kenntnis gebracht werden. Diese Informationen haben auf der Homepage des Kantons zu erfolgen (2).

2.3.2 Stellungnahme

Die Auslagerung von Informatikdienstleistungen ist ebenfalls als submissionsrechtlicher Vorgang zu verstehen. Im Submissionsrecht ist die Transparenz ein Verfahrensgrundsatz. Sie wird namentlich durch die Veröffentlichung der wichtigsten vergaberechtlichen Verfügungen auf der Internetplattform von Bund und Kantonen, simap.ch, sichergestellt. Im Rahmen des jährlichen Geschäftsberichts des Kantons wird jeweils eine Submissionsstatistik veröffentlicht, aus welcher

die Anzahl sowie die Gesamtsumme der Vergaben pro Globalbudget hervorgeht, aufgeschlüsselt nach angewendetem Vergabeverfahren.

Eine weitergehende gesetzliche Regelung zur Transparenz für Auslagerungen ist nicht nötig. Eine solche Vorgabe wäre auch mit einem zusätzlichen und nicht zu vernachlässigenden administrativen Aufwand verbunden. Einig gehen wir mit den Vernehmlassungsadressatinnen in dem Punkt, dass besonders bedeutsame, umfangreiche oder risikobehaftete Auslagerungsentscheide, die in den Zuständigkeitsbereich des Regierungsrates oder der Gerichtsverwaltungskommission fallen, aufgrund ihrer Bedeutung öffentlich gemacht werden. Die Vorlage wird in diesem Punkt angepasst.

Im Übrigen bleiben die Informations- und Zugangsrechte gemäss InfoDG von diesem Erlass unberührt.

2.4 Zuständigkeiten und Verantwortung

2.4.1 Vernehmlassungen

Zwei Vernehmlassungadressatinnen (2, 4) vermissen in der Vorlage eine Zuständigkeitsmatrix, die aufzeigt wer, wann zuständig und entscheidbefugt ist und in der Verantwortung steht.

2.4.2 Stellungnahme

Der Gesetzesentwurf und auch die Botschaft setzen sich unmissverständlich mit der Zuständigkeit und der Verantwortung auseinander, wobei sich Haftung und Regress nach dem Gesetz über die Haftung des Staates, der Gemeinden, der öffentlich-rechtlichen Körperschaften und Anstalten und die Verantwortlichkeit der Behörden, Beamten und öffentlichen Angestellten und Arbeiter vom 26. Juni 1966 (Verantwortlichkeitsgesetz; BGS 124.21) richten.

2.5 Exitstrategie

2.5.1 Vernehmlassungen

Auf die Wichtigkeit einer Exitstrategie wird in zwei Vernehmlassungsantworten (1, 6) hingewiesen.

Die eine Vernehmlassungsadressatin (1) betont, dass eine Exitstrategie Sinn mache, jedoch aufwändig und kostspielig sei; eine minimale IT-Infrastruktur und entsprechendes Personal müssen vom Kanton bereitgestellt werden. Die Behörde müsse sich Gedanken darüber machen, wie die Aufgaben auch ohne ausgelagerte Informatikdienstleistung erbracht werden könne. Diese Bestimmung sei weder umsetzbar noch kontrollierbar und sollte praxistauglicher formuliert werden. Ein Restrisiko bleibe immer bestehen und sei auch vorhanden, wenn die Dienstleistung innerhalb des Kantons erbracht werde. Für die andere Vernehmlassungsadressatin (6) ist ein Business Kontinuitätskonzept mit einem zweiten Serverstandort und einer parallelen Infrastruktur anzustreben. Ebenfalls sei sicherzustellen, dass nur Software und IT-Infrastruktur eingesetzt werde, die vom Hersteller auch für die Anwendung innerhalb der Verwaltung mit hochsensiblen Daten freigegeben sei. Zudem sei der Dritte vertraglich zur Dokumentation zu verpflichten und diese durch den Besteller regelmässig auf ihre Aktualität und Vollständigkeit zu überprüfen.

2.5.2 Stellungnahme

Mit der Auslagerung von Informatikdienstleistungen ist zwangsläufig eine Abhängigkeit der auslagernden Behörde vom beauftragten Dritten verbunden. Bei ausbleibenden oder ungenügenden Leistungen des beauftragten Dritten muss die staatliche Aufgabenerfüllung jedoch trotzdem gewährleistet sein. Für diesen Fall hat die zuständige Behörde sicherzustellen, dass im

Rahmen des betrieblichen Kontinuitätsmanagements (Business Continuity Management; BCM) geeignete Massnahmen getroffen werden. Als geeignete Massnahmen gelten etwa das Erstellen von Sicherungskopien der ausgelagerten Daten, eine hinreichende Dokumentation der Datenbearbeitungen oder das Bereithalten von Ausweichlösungen für den Fall, dass der Dritte die Informatikdienstleistung nicht oder nur ungenügend erfüllt. Insbesondere die Rückübertragung der ausgelagerten Informatikdienstleistungen muss geplant sein und bei Bedarf jederzeit ausgeführt werden können. Diese Exitstrategie ist periodisch auf ihre Wirksamkeit zu überprüfen und gegebenenfalls an geänderte Verhältnisse anzupassen. Die Botschaft wird entsprechend ergänzt.

3. Weitere Themen in den Vernehmlassungsantworten

3.1 SP Kanton Solothurn

3.1.1 Vernehmlassung

Das Auslagerungsgesetz decke nur einen eingeschränkten Teil von Auslagerungen ab, nämlich die Thematik rund um die Cloud-Dienste, und sollte generell für die Auslagerung von Dienstleistungen, auch ausserhalb der IT, gelten (z.B. für das Erstellen von Bauten, das Kaufen von Lizenzen oder Software). Die Grenze zwischen Dienstleistung und Beschaffung sei im Gesetzesentwurf nicht klar definiert. Ebenfalls fehle die längst überfällige Behandlung elektronischer Wahlen und Abstimmungen; es müsse zumindest erwähnt werden, wo diese Art der Auslagerung geregelt werde.

In § 3 Abs. 1 Bst. c sei bei der Definition des Begriffs des «Dritten» zu berücksichtigen, dass Auslagerungen an den Bund, andere Kantone oder kantonale Institutionen gesetzlich anders zu behandeln seien als Auslagerungen an private Auftragnehmer.

3.1.2 Stellungnahme

Der Gesetzesentwurf stellt bewusst kein «Cloudgesetz» dar. Der sachliche Anwendungsbereich soll sich auf sämtliche Auslagerungen von Informatikdienstleistungen beziehen, nicht nur auf Clouddienste. Mit dieser Vorlage soll ein Gesetz geschaffen werden, welches die Voraussetzungen, Zuständigkeiten und Verantwortlichkeiten bei jeder Art der Auslagerung von Informatikdienstleistungen regelt. Vom Gesetz betroffen sind aber bewusst nur Auslagerungen von Informatikdienstleistungen, weil sich in diesen Bereichen neue Herausforderungen stellen bezüglich der Informationssicherheit, des Datenschutzes und der Archivierung, die sich bei anderen Beschaffungen nicht stellen. Der Kanton verfügt noch über keine E-Voting Lösung; müsste der Kanton für dieses Projekt Informatikdienstleistungen Dritter beanspruchen, würde das Auslagerungsgesetz zur Anwendung gelangen. Die gesetzlichen Grundlagen zu den übrigen Beschaffungen finden sich im Kantonalen Submissionsrecht.

Das Gesetz soll für jede Art der Auslagerung gelten, also auch für Auslagerungen an den Bund, an eine schweizerische Hochschule oder an eine andere staatliche Institution in der Schweiz. Auch bei diesen Auslagerungen müssen die im Gesetzesentwurf vorgesehenen Voraussetzungen erfüllt sein. Es versteht sich aber von selbst, dass in diesen Fällen die Voraussetzungen für eine Auslagerung in der Regel schneller erfüllt sein werden, weil die Risikobeurteilung günstiger ausfallen wird und sich die Hürden insgesamt als weniger hoch präsentieren als bei einer Auslagerung an einen privaten Dritten.

3.2 SVP Kanton Solothurn

3.2.1 Vernehmlassung

In einer gesetzlichen Bestimmung soll festgehalten werden, dass Dritte kausal für den dem Kanton entstandenen Schaden haften und eine entsprechende Haftpflichtversicherung mit einer ausreichenden Deckung vorzuweisen haben.

Es sei eine Bestimmung ins Auslagerungsgesetz aufzunehmen, wonach im Schadenfall der Regierungsrat zwingend und ausnahmslos auf die IT-Verantwortlichen personalrechtlich regressieren könne und dass Schaden- und Regressfälle jährlich und öffentlich zugänglich zu publizieren seien.

3.2.2 Stellungnahme

Bei Auslagerungen an Dritte werden wie bei anderen Vergaben regelmässig Verträge abgeschlossen, die auch Bestimmungen zur Haftung enthalten. Dazu kommt, dass die AGB SIK (respektive zukünftig die AGB für IKT-Leistungen der Digitalen Verwaltung Schweiz), die bei Verträgen mit Dritten zum Tragen kommen, respektive kommen werden, und sich auf einem guten Niveau befinden, die Haftungsfrage explizit regeln. Zudem haben Anbietende eine Selbstdeklaration auszufüllen und einzureichen, worin auch die Übernahme der Haftungsfrage Thema ist (Leitfaden Beschaffung AIO V2.0). Bei Submissionen kann das Bestehen einer Haftpflichtversicherung in bestimmter Höhe als Eignungskriterium verlangt werden und ist entsprechend auch nachzuweisen. Dazu kommt, dass dort, wo Auslagerungen in Form von privatrechtlichen Verträgen abgeschlossen werden, der Kanton keine gesetzliche Kausalhaftungsregelung erlassen kann. Das Haftungsrecht ergibt sich in diesen Fällen aus dem Bundesprivatrecht. Die Gesetzgebung auf diesem Gebiet ist ausschliesslich Sache des Bundes (Art. 122 BV).

Was Haftung und Regress der Mitarbeitenden der kantonalen Verwaltung anbelangt, so richten sich diese nach den entsprechenden Bestimmungen des Verantwortlichkeitsgesetzes. Dieses Gesetz gilt für alle Mitarbeitenden, die in Ausübung ihrer amtlichen Tätigkeit Dritten Schaden zufügen und auch für Magistratspersonen. Auch der Regress auf den fehlbaren Mitarbeitenden oder auf Magistratspersonen richtet sich nach dem Verantwortlichkeitsgesetz und es besteht keine Veranlassung, bei IT-Projekten anders zu verfahren als bei anderen Schaden- und Regressfällen in der kantonalen Verwaltung. Über Verfahren zu Schaden- und Regressfällen wird eine jährlich aktualisierte Auflistung und Statistik (via Finanzkontrolle) der Geschäftsprüfungskommission des Kantonsrates unterbreitet. Publiziert werden allenfalls entsprechende Gerichtsentscheide in anonymisierter Form (Verwaltungsgericht, Bundesgericht). Bei der Veröffentlichung von Schaden- und Regressfällen von Auslagerungen soll ebenfalls gleich verfahren werden wie bei anderen Schaden- und Regressfällen. Eine gesetzliche Regelung zur jährlichen Veröffentlichung aller Schaden- und Regressfälle müsste im Verantwortlichkeitsgesetz erfolgen und hätte für alle Schaden- und Regressfälle gleichermassen zu gelten.

3.3 Solothurner Handelskammer

3.3.1 Vernehmlassung

Das Auslagerungsgesetz soll vor allem ein Ermöglichungsgesetz und nicht ein Verhinderungsgesetz sein. Deshalb seien die Chancen der Digitalisierung und nicht die Risiken zu berücksichtigen. Allzu strenge Voraussetzungen, insbesondere im Bereich der nicht besonders schützenswerten Daten, seien zu vermeiden. Auch stelle sich die Frage, ob bei allen Auslagerungen die gleichen sehr strengen Anforderungen gelten müssen, oder ob Kategorisierungen vorgenommen werden können.

Auslagerungen, die ein hohes Risiko für die Grundrechte der betroffenen Personen mit sich bringen, sollen nicht immer vom Regierungsrat beschlossen werden müssen, weshalb die entsprechende Bestimmung des Gesetzesentwurfs gestrichen werden soll. Der Regierungsrat könne die Frage des ausreichenden Datenschutzes nicht besser beantworten als das einzelne Amt, das damit auch nicht die Verantwortung auf den Regierungsrat abschieben könne.

3.3.2 Stellungnahme

Gerade weil die Chancen der Digitalisierung erkannt worden sind, soll mit dem Auslagerungsgesetz die gesetzliche Grundlage geschaffen werden, die Auslagerungen auch in der kantonalen Verwaltung möglich machen. Die Auslagerung von Informatikdienstleistungen und insbesondere der Einsatz von Cloud-Lösungen bergen, im Vergleich zum Betrieb der Anwendungen in den eigenen Rechenzentren der kantonalen Verwaltung, eine Reihe von neuen Risiken und Herausforderungen, denen mit gesetzlichen Bestimmungen oder schriftlichen Vereinbarungen zu begegnen ist. Jedes Auslagerungsprojekt hat deshalb die Voraussetzungen von § 5 zu erfüllen, wird aber individuell beurteilt bezüglich Risiken und Massnahmen. Deshalb werden die Hürden nicht für jede Art der Auslagerung gleich hoch sein. Wird insbesondere kein erhöhter Schutzbedarf festgestellt, sind auch keine besonderen Massnahmen nötig.

Die Ämter werden nicht aus der Verantwortung genommen. Nur bei den Auslagerungsentscheiden, die entweder besonders bedeutsam, umfangreich oder risikobehaftet sind, wird ein Entscheid auf höchster Führungsebene erwartet. In diesen Fällen soll der Regierungsrat, resp. die Gerichtsverwaltungskommission, Auslagerungsentscheide beschliessen. Die Verantwortung für die rechtmässige Aufgabenerfüllung gemäss § 8 obliegt aber nach wie vor bei der Behörde und damit dem Amt, welche Dritte zur Aufgabenerfüllung beizieht. Der Regierungsrat, resp. die Gerichtsverwaltungskommission trägt die Verantwortung für die neuen, aus der Auslagerung entstandenen Risiken. Es müssen auch nicht alle Auslagerungsentscheide, die besonders schützenswerte Personendaten betreffen, vom Regierungsrat oder der Gerichtsverwaltungskommission beschlossen werden, sondern nur diejenigen, die ein hohes Risiko für die Grundrechte der betroffenen Personen mit sich bringen. Dies wird regelmässig dann der Fall sein, wenn die Auslagerung eine grosse Zahl von Datenkategorien umfasst oder eine grosse Anzahl Personen betroffen ist. In allen anderen Fällen kann die auslagernde Behörde die Auslagerung beschliessen und dies kann ein Amt sein.

3.4 Evangelische Volkspartei

3.4.1 Vernehmlassung

Die EVP macht auf den US CLOUD Act aufmerksam, der US-amerikanischen Strafverfolgungsbehörden Zugang zu Daten des Kantons Solothurn ermöglichen könnte.

Die EVP weist ebenfalls auf leistungsfähige Open-Source-Cloudlösungen hin und verlangt eine gesetzliche Regelung, die Open-Source-Lösungen bevorzugt, wo dies sinnvoll ist. Open-Source-IT-Lösungen, welche die volle Datenhoheit durch den Staat garantieren würden, seien zu priorisieren. Erst wenn dies nicht mit vertretbarem Aufwand realisierbar sei, könnten private Anbieter berücksichtigt werden.

Es sei wichtig, dass die Verwaltung über die notwendigen ICT-Kompetenzen verfüge und diese gefördert werden. Gefordert werden kompetente Ansprechpartner, die mit den Dienstleistern kommunizieren können. Es fehle an klaren Regelungen für Risikoanalysen und die Rolle des AIO. Ein weiterer Absatz zu § 7 soll regeln, wie die Behörden das notwendige Wissen erhalten können und in welchen Fällen das AIO ein «Veto-Recht» habe.

3.4.2 Stellungnahme

Der US CLOUD Act erlaubt es der US-Strafverfolgungsbehörde auf Daten von Dritten zuzugreifen, die bei US-Unternehmen gespeichert sind, selbst wenn diese Daten vom US-Unternehmen physisch ausserhalb der USA gespeichert werden. Der US-Cloud Act ist eines der möglichen Risiken, die es bei einer Auslagerung zu berücksichtigen und zu minimieren gilt. Dies hat in der Gesamtbeurteilung der Risikoabwägung einzufliessen.

Sowohl Open-Source- wie auch andere Cloud-Lösungen bieten nicht nur Vor- sondern auch Nachteile, die jeweils projektbezogen evaluiert werden müssen. Es soll bewusst niemand ausgeschlossen werden, weshalb eine gesetzliche Bevorzug von Open-Source-Lösungen nicht angestrebt wird.

Bereits 2019 wurde mit einem Regierungsratsbeschluss die Umsetzung des Konzepts Informationssicherheit verabschiedet, welches unter anderem die Rolle des «Informationssicherheitsverantwortliche/r (ISV)» der Dienststellen beschreibt. Im Bereich Informationssicherheit sind dies die ersten Ansprechpartner für alle Dienststellen. Das AIO verfügt zudem über vertieftes Knowhow in diesem Bereich und dient als Ansprechpartner für die Dienstleister. Das nötige Wissen bezüglich ICT und Betrieb von Services ist im AIO vorhanden und wird laufend erweitert. Das Erstellen von Risikoanalysen ist in IT-Projekten klar geregelt, auch mit Bezug auf Informationssicherheitsthemen. Das AIO prüft Risikoanalysen und ISDS-Konzepte entsprechend.

3.5 Grüne Kanton Solothurn

3.5.1 Vernehmlassung

Die Grünen begrüssen, dass eine Erweiterung des Geltungsbereichs auf die Gemeinden geplant sei. Aufgrund der Komplexität der Materie seien einheitliche kantonale Vorgaben unumgänglich. Es werde davon ausgegangen, dass der Kanton ebenfalls für weitere Körperschaften, die Leistungen im Auftrag des Kantons erbringen (Kantonsschulen, soH, Fachhochschulen) in Leistungsvereinbarungen Vorgaben mache zu Auslagerungen von Informatikdienstleistungen.

Als weitere risikominimierende Massnahme seien Schulungskonzepte zu erstellen. Diese sollen sicherstellen, dass die Prozesse von den Mitarbeitenden eingehalten, Risiken ermittelt und Massnahmen ergriffen werden. Die Schulungen seien regelmässig zu aktualisieren und zu wiederholen, dies insbesondere im Bereich der besonders schützenswerten Daten.

Besondere Vorsicht sei geboten beim Einsatz von Office 365. MS Teams schaffe eine grosse Transparenz und erlaube die Bearbeitung von vielen Daten durch viele Personen, was aber bei besonders schützenswerten Daten gerade nicht gewünscht werde. MS 365 Anwendungen müssen deshalb besonders sorgfältig konfiguriert und der Umgang, gerade im Hinblick auf den Datenschutz, regelmässig geschult und geprüft werden.

Der Zugang zu öffentlichen Dienstleistungen soll auch möglich sein ohne digitale Datenspur zu hinterlassen. Personen, die sich nicht digital bewegen möchten oder können, soll eine Alternative geboten werden.

Die Bestimmung betreffend die Voraussetzungen soll ergänzt werden:
Buchstabe e: Dort wo in besonderem Mass schützenswerte Daten bearbeitet oder Datenquellen verknüpft werden sollen, soll der Kanton die Möglichkeit haben, Personensicherheitsüberprüfungen von den Mitarbeitenden Dritter zu verlangen. Buchstabe f: Bei jedem Auslagerungsprojekt seien vertraglich die Daten für die Langzeitarchivierung und die entsprechenden Prozesse für die Überführung zu definieren. Dies insbesondere in den Fällen, wo nebst der physischen Ar-

chivierung auch die elektronische Archivierung vorgesehen sei. Buchstabe g: Es sei sicherzustellen, dass die auslagernde Behörde auch über die entsprechenden Rechte verfügt um der statuierten Verantwortung nachzukommen.

Die Bestimmung betreffend das Risikomanagement sei im Absatz 2 wie folgt zu ergänzen: «Sie bestimmt die erforderlichen Massnahmen, um die Risiken angemessen zu minimieren und überprüft deren Umsetzung durch den Leistungserbringer.»

3.5.2 Stellungnahme

Vom Geltungsbereich des Auslagerungsgesetzes ausgenommen sind die Solothurner Spitäler AG, die selbständigen öffentlich-rechtlichen Anstalten des Kantons und die Informatikdienstleistungen an den kantonalen Schulen für Unterrichtszwecke. Auch die Gemeinden sind nicht vom Geltungsbereich des Gesetzes erfasst. Der Regierungsrat plant in einem weiteren Schritt, falls dies entsprechend gewünscht wird, die Auslagerung von Informatikdienstleistungen für alle Behörden gemäss dem Behördenbegriff von § 3 InfoDG zu regeln. Dies hat über eine Teilrevision des Auslagerungsgesetzes zu erfolgen.

Wir stimmen zu, dass die Prozesse zum Risikomanagement immer wieder geschult werden müssen. Die Prozesse der Informationssicherheit innerhalb von IT-Projekten sind bereits definiert und beschrieben, werden stetig aktualisiert und erneuert. Die Methodenkompetenz ist in einem kantonalem Projektleitfaden definiert und entsprechende Vorlagen und Anleitungen dazu bestehen. Massnahmen zur Minimierung von Sicherheitsrisiken werden in den jeweiligen Vorhaben innerhalb der ISDS-Konzepte erarbeitet. Dazu gehören auch organisatorische Massnahmen wie Schulungskonzepte und Schulung der Mitarbeitenden. Weiter ist ein eLearning Modul am Entstehen, welches allen Mitarbeitenden der kantonalen Verwaltung zur Verfügung gestellt wird.

Der Aussage zur erhöhten Vorsicht im Umgang mit Office 365 wird vorbehaltlos zugestimmt. Diese Feststellung beschränkt sich aber nicht einzig auf Office 365, sondern trifft auf die gesamte Microsoft 365 Palette zu. Das Auslagerungsgesetz ist kein «Microsoft 365-Gesetz», und wird bezüglich Anbieter und Projekt bewusst offengehalten. Sollte die Einführung von Microsoft 365 als neue Office Version konkret in Betracht gezogen werden, so hat dieses Projekt den gesetzlichen Anforderungen des Auslagerungsgesetzes wie auch den übrigen gesetzlichen Vorgaben der Datenschutz- und Archivgesetzgebung sowie den finanz- und submissionsrechtlichen Bestimmungen zu genügen.

Wir begrüssen es, dass Interessierten der Zugang zu öffentlichen Dienstleistungen ermöglicht werden soll, ohne dabei eine digitale Datenspur zu hinterlassen. Die Schaffung der hierfür nötigen gesetzlichen Grundlagen ist allerdings nicht Thema dieser Vorlage.

Eine Forderung nach Personensicherheitsüberprüfungen für Mitarbeitende Dritter, die mit besonders schützenswerten Daten arbeiten oder Datenquellen verknüpfen, wirft mehrere praktische Fragen auf, bevor die rechtlichen Fragen gelöst werden können. Zunächst müsste der Begriff «Personensicherheitsüberprüfung» klar definiert werden, um zu verstehen, welche Massnahmen darunterfallen und wie diesen rechtlich zu begegnen ist. Auch dürfte die Durchführung solcher Überprüfungen die Verwaltung vor erhebliche praktische Schwierigkeiten stellen, allein schon aufgrund der grossen räumlichen Distanz bei Auslagerungen in komplexe Cloud-Umgebungen. Im Auslagerungsgesetz ist der Begriff der «Personensicherheitsüberprüfung» nicht explizit geregelt. Der Gesetzesentwurf sieht bei den Voraussetzungen die Haftung Dritter für die gehörige Sorgfalt bei der Auswahl, Instruktion und Überwachung ihrer Mitarbeitenden und Hilfspersonen vor. Und Buchstabe g sieht ein Weisungs- und Kontrollrecht für die zuständige und die auslagernde Behörde sowie die Aufsichtsbehörde vor. Wir pflichten den Anliegen in Be-

zug auf die Archivierung zu. Diese sind allerdings vom Wortlaut der Bestimmung zu den Voraussetzungen in Buchstabe f erfasst. Die Weisungs- und Kontrollrechte der auslagernden und der zuständigen Behörde sind in Buchstabe g geregelt.

Die gewünschte Erweiterung in der Bestimmung zum Risikomanagement ist nicht nötig. Die verlangten Kontrollrechte finden sich bereits in der Bestimmung zu den Voraussetzungen in Buchstabe g.

3.6 Die Mitte Kanton Solothurn

3.6.1 Vernehmlassung

Es wird auf die anstehende Revision des Informations- und Datenschutzgesetzes hingewiesen und darauf, dass dieses Vorhaben in der Vorlage hoffentlich mitberücksichtigt worden sei, die Datenschützerin den Gesetzesentwurf begutachtet habe und ihre allfälligen Rückmeldungen aufgenommen wurden.

3.6.2 Stellungnahme

Die Revision des Informations- und Datenschutzgesetzes ist erst im Gang und wurde bei den vorliegenden Gesetzgebungsarbeiten soweit möglich mitberücksichtigt. In den beiden Arbeitsgruppen zu den Gesetzgebungsarbeiten zum Auslagerungsgesetz haben sowohl die Beauftragte für Information und Datenschutz sowie auch zwei ihrer Mitarbeitenden beratend mitgewirkt.

4. Beschluss

4.1 Von den eingegangenen Stellungnahmen wird Kenntnis genommen. Der Regierungsrat dankt allen Organisationen, die sich am Vernehmlassungsverfahren beteiligt haben.

4.2 Das Finanzdepartement wird beauftragt, Botschaft und Entwurf an den Kantonsrat in diesem Sinne auszuarbeiten.

Andreas Eng
Staatsschreiber

Verteiler

Finanzdepartement (2)
Staatskanzlei (4; eng, rol, ett, ff)
Gerichtsverwaltungskommission
Aktuarin der Finanzkommission
Aktuarin der Spezialkommission Digitalisierung Kantonsrat
Parlamentsdienste

Teilnehmer an der Vernehmlassung (7, Versand durch Finanzdepartement)
Medien (elektronischer Versand durch STK Kommunikation)