GRÜNE Kanton Solothurn
Niklaus Konradstr. 18
4500 Solothurn
sekretariat@gruene-so.ch

Olten, 31. August 2024

Finanzdepartement
Departements Sekretariat
Rathaus
Barfüssergasse 24
4509 Solothurn

Vernehmlassung zum «Gesetz über die Auslagerung von Informatikdienstleistungen (Auslagerungsgesetz; AusG)»

Sehr geehrter Herr Landamman Hodel,

Sehr geehrte Damen und Herren,

Gerne nutzen wir die Gelegenheit, uns zum Gesetzesentwurf für das geplante Auslagerungsgesetz zu äussern. Vorausschickend möchten wir festhalten, dass wir es sehr begrüssen, dass eine gesetzliche Grundlage geschaffen wird für die Beurteilung und Vergabe von Informatikdienstleistungen. Dies ist eine wichtige Grundvoraussetzung für die fortschreitende Digitalisierung von öffentlichen Dienstleistungen und verwaltungsinternen Prozessen. Wir stehen als Partei hinter der Digitalisierungsstrategie des Kantons und begreifen den vorliegenden Gesetzesentwurf als wichtigen Meilenstein, um dieser zum Erfolg zu verhelfen. Für uns ist der Fokus auf einen effektiven Datenschutz entscheidend, dieser ist sowohl durch technische als auch organisatorische und vertragliche Massnahmen sicherzustellen.

Allgemeine Überlegungen zur Vorlage:

- Zu „4. Geltungsbereich“ Wir begrüssen, dass bereits die nächsten Erweiterungen des AusG geplant sind, in denen auch die Auslagerung von Informatikdienstleistungen der Gemeinden geregelt werden sollen. Die Komplexität der Materie macht es unumgänglich, dass hier gewisse kantonale Vorgaben geschaffen werden müssen, da eine vertiefte Einarbeitung bzw. Erarbeitung solcher Regelungen auf Gemeindeebene ein zu hohes Risiko birgt und zu möglicher ungleicher Handhabung im Umgang mit Personen und Sachdaten führen würde. Für uns ist eine kantonal einheitliche Regelung essentiell, ebenso wie ein einheitlicher Umgang mit den entsprechenden Risiken gepflegt werden muss.

- Weiter gehen wir davon aus, dass der Kanton für weitere Körperschaften, die im Auftrag des Kantons Leistungen erbringen (Kantonsschulen, SoH, Fachhochschulen), Vorgaben macht, wonach diese Regelungen bzw. Prozesse definieren müssen, wie im Falle der Auslagerung von Informatikdienstleistungen an Dritte der Schutz von Personen- und sensiblen Sachdaten durch die jeweilige Körperschaft sichergestellt wird. Sollte dies nicht bereits Teil der Leistungsvereinbarung sein, so wäre dies unbedingt zu ergänzen.
- Es ist sicher wichtig, dass für Informatikprojekte Prozesse definiert sind, um die damit verbundenen Risiken zu ermitteln und zu mitigieren wie unter 5.3 aufgeführt (Schutzbedarfsanalyse, ISDS-Konzept). Aus Sicht der GRÜNEN ist hier aber auch wichtig, dass die entsprechenden Prozesse auch regelmässig geschult und die Umsetzung und Einhaltung der Massnahmen jederzeit sichergestellt werden. Entsprechende Schulungskonzepte müssten im ISDS-Konzept aufgenommen werden.
- Zu „9.4 Wirtschaftlichkeit“ Wirtschaftlichkeitsüberlegungen sollten nicht allein im Fokus der Auslagerung stehen. Auslagerungen sind denkbar, um von allgemeinen Entwicklungen in der Digitalisierung zu profitieren und an den entsprechenden Skaleneffekten teilzuhaben. Jedoch zeigt sich vielfach, dass mit den notwendigen Investitionen in die Security Infrastruktur sowie, die personellen Aufwände um die Prozesse der Risikominimierung einzuhalten, die Kosteneinsparungen weniger ins Gewicht fallen. Kompromisse im Datenschutz aus Kostenüberlegungen sind auf jeden Fall auch künftig zu vermeiden.
- Gerade beim Einsatz von Office 365 gilt besondere Vorsicht. Die Anwendungen wie Teams sind so konzipiert, dass sie möglichst grosse Transparenz schaffen wollen. Vom Grundsatz her sind also sämtliche Daten für möglichst viele Personen zugänglich und der Zugriff muss aktiv beschränkt werden. Im Umgang mit besonders schützenswerten Daten gilt genau das Gegenteil. Daten sind grundsätzlich nicht zugänglich und können nach Prüfung des Need-to-know Prinzips freigeschaltet werden. Daher müssen Microsoft 365 Anwendungen besonders sorgfältig konfiguriert und der Umgang damit, insbesondere im Hinblick auf Datenschutz regelmässig geschult und geprüft werden.
- Als Risikominimierende Massnahme muss der Umgang mit den Systemen der Leistungsnehmer sowie entsprechende Datenschutzmassnahmen geschult werden. Dazu ist jeweils ein Schulungskonzept zu erstellen und aufzuzeigen wie Mitarbeitende eingeführt werden, um einen verantwortungsvollen Umgang mit den Systemen sicherzustellen. Dem Faktor Mensch ist dabei grösste Aufmerksamkeit zu schenken, da bekanntermassen ein Grossteil der Datenschutzverletzungen durch menschliche Fehler entstehen. Dies ist bei jedem einzelnen Auslagerungsprojekt zu berücksichtigen. Schulungen müssen auch regelmässig aktualisiert und wiederholt werden, insbesondere da wo besonders schützenswerte Daten bearbeitet werden.
- In den Erläuterungen zu §5 wird eine Bearbeitung von Daten im Ausland erwähnt. Dies ist aus unserer Sicht wo immer möglich zu vermeiden bzw. für besonders schützenswerte Daten zu verbieten. Daten dürfen nur an Dienstleister ausgelagert werden, die sie auf Servern in der Schweiz oder der EU mit geltendem EU Datenschutzgesetz speichern. Eine Auslagerung unter anderen Bedingungen als diesen birgt aus unserer Sicht ein zu grosses Risiko und be-

deutet per se einen zu grossen Eingriff in das Grundrecht auf informationelle Selbstbestimmung.

- Weiter möchten wir anmerken, dass auch mit vielen laufenden Digitalisierungsprojekten und Bestrebungen die Verwaltung zu digitalisieren, der Zugang zu öffentlichen Dienstleistungen auch gewährleistet sein soll ohne digitale Datenspur. Personen die sich nicht digital bewegen möchten oder können soll eine Alternative geboten werden z.B. Zugang zur Dienstleistung vor Ort bei den Ämtern.
- Als letzte grundsätzliche Überlegung (Details dazu unter §5) sollen unter keinen Umständen besonders schützenswerte Daten in eine Public Cloud ausgelagert werden dürfen. Ist eine Auslagerung von besonders schützenswerten Daten erforderlich so ist immer eine private Cloud Lösung zu wählen, um das Risiko von Data Leaks zu minimieren.

Zu folgenden Paragrafen möchten wir uns konkret äussern:

§ 4 Abs. 1 Bst. e

In Fällen bei denen in besonderem Masse schützenswerte Daten bearbeitet werden oder Datenquellen verknüpft werden können, kann der Kanton auch Personensicherheitsprüfungen von den Mitarbeitenden Dritter verlangen, die die entsprechenden Aufgaben ausführen werden

§ 4 Abst. 1 Bst. f

Bei jedem Auslagerungsprojekt ist mit dem Anbieter vertraglich zu regeln, welche Daten für die Langzeitarchivierung vorgesehen sind. Zudem sind bereits in der Projektphase die entsprechenden Prozesse für die Überführung der Daten ins Langzeitarchiv festzulegen. Dies gilt insbesondre in Fällen wo nach wie vor eine physische Archivierung der Daten zusätzlich zur elektronischen Speicherung vorgesehen ist.

§ 4 Abs. Bst g

Vorgelagert zu Rechten und Pflichten der Aufsichtsorgane muss sichergestellt sein, dass die beauftragende Behörde, die gemäss Kapitel 6. des Entwurfs in der Verantwortung für die Aufgabenerfüllung steht, über ausreichende Rechte verfügt, um dieser Verantwortung auch nachzukommen. Zugangsrechte durch die Aufsichtsorgane der beauftragenden Behörde sind erst im zweiten Schritt relevant.

§4 Abs 2

Diese Massnahme ist aus Sicht der GRÜNEN essentiell. Vorfälle wie der Crowdstrike Incident zeigen, wie hoch dieses Risiko ist. Es besteht auch im Bereich von sicherheits- und systemrelevanter IT Infrastruktur eine grosse Abhängigkeit. Ein Business Kontinuitätskonzept mit einem zweiten Serverstandort und einer parallel Infrastruktur ist daher aus unserer Sicht – zumindest für hochsensible und zeitkritische Anwendungen – anzustreben. Ebenfalls ist sicherzustellen, dass nur Software und IT Infrastruktur eingesetzt wird, das auch für die Anwendung innerhalb der Verwaltung mit hochsensiblen Daten freigegeben ist durch den Her-

steller. Zudem sind IT Dienstleister vertraglich zur Dokumentation zu verpflichten und diese ist durch die Besteller regelmässig auf ihre Aktualität und Vollständigkeit zu prüfen.

§5 Abs. 1 Bst. c

Werden besonders schützenswerte Daten zur Bearbeitung und Speicherung in die Cloud ausgelagert, so muss aus Sicht der GRÜNEN immer eine private Cloud Lösung mit Serverstandorten in der Schweiz oder mindestens im EU Raum unter geltendem EU Datenschutzgesetz vorgesehen werden. Zudem muss vertraglich vereinbart werden, dass der Gerichtsstand in der Schweiz zu liegen hat. Nur können diese Daten effektiv und langfristig vor unrechtsmässigem Zugriffen oder versehentlichen Veröffentlichung durch menschliche Fehler geschützt werden. Diese Praxis der private Cloud ist auch in der Privatwirtschaft weitverbreitet um Geschäftsgeheimnisse zu schützen und sicherzustellen, dass Mitarbeitende nicht unwillentlich z.B. in der Zusammenarbeit über Teams schützenswerte Daten veröffentlichen. Siehe dazu auch unsere Ausführungen bezüglich Arbeiten mit Microsoft 365 Tools.

§ 6 Abs. 2

Der Abschnitt ist wie folgt zu ergänzen: „Sie bestimmt die erforderlichen Massnahmen, um die Risiken angemessen zu minimieren **und überprüft deren Umsetzung durch den Leistungserbringer.**“

Wir hoffen auf eine Überarbeitung der Vorlage und danken Ihnen, wenn unsere Einwendungen und Überlegungen Gehör finden.

Mit freundlichen Grüssen
GRÜNE Kanton Solothurn

Laura Gantenbein, Präsidentin GRÜNE Kanton Solothurn

Für Rückfragen:

Anna Engeler, Fraktionspräsidentin GRÜNE Kanton Solothurn, 078 864 03 43