An den Grossen Rat **25.5256.02**

FD/P255256

Basel, 26. November 2025

Regierungsratsbeschluss vom 25. November 2025

Motion Anina Ineichen und Konsorten betreffend «Schaffung einer gesetzlichen Grundlage für die Auslagerung von Informatikdienstleistungen»; Stellungnahme

Der Grosse Rat hat an seiner Sitzung vom 17. September 2025 die nachstehende Motion Anina Ineichen und Konsorten dem Regierungsrat zur Stellungnahme überwiesen:

> «Die rasche Entwicklung der Informationstechnologien führt dazu, dass cloud-basierte Lösungen zunehmend an Bedeutung gewinnen. Die Anforderungen an die kantonale Verwaltung gehen vermehrt in Richtung plattformunabhängiger Zugänge sowie «mobile Arbeit jederzeit und überall». Gleichzeitig setzen viele Anbieter:innen verstärkt auf cloud-basierte Systeme und bieten kaum noch On-Premises-Lösungen an. Auch der Regierungsrat hat am 8. April 2025 beschlossen, Microsoft 365 einzuführen – eine cloud-basierte Lösung.
> Mit der Nutzung von Cloud-Technologien ist zwangsläufig eine Auslagerung von Informatikdienstleistungen verbunden. Diese erfolgt ausserhalb der kantonalen Rechenzentren und bringt neue Herausforderungen für Informationssicherheit, Datenschutz und Archivierung.
>
> Gemäss § 3 Abs. 5 des Informations- und Datenschutzgesetzes vom 9. Juni 2010 (IDG) liegt bei einer Auslagerung von Personendaten eine Datenbearbeitung vor. Obwohl §7 Abs. 1 IDG die Bearbeitung durch Dritte unter bestimmten Bedingungen erlaubt, reicht die bestehende gesetzliche Grundlage für besonders umfangreiche oder risikobehaftete Auslagerungen nicht aus. Zudem regelt das IDG die Auslagerung von Personendaten nicht ausdrücklich.
>
> Die Nutzung cloud-basierter Dienstleistungen wie Microsoft 365 birgt eine Reihe faktischer und rechtlicher Risiken (Vgl. Vernehmlassungsunterlagen Solothurn):
>
> - Mangelnde Transparenz über Serverstandorte,
> - Datenbearbeitungen und eingesetzte Sicherheitsmassnahmen;
> - Eingeschränkte Kontrollrechte;
> - Begrenzter Vertragsgestaltungsspielraum bei Standardanwendungen;
> - Erschwerte Durchsetzung von Rechtsansprüchen (z. B. bei Datenrückübertragung);
> - Risiko des Datenzugriffs durch ausländische Behörden (z. B. US-CLOUD Act);
> - Erhöhte Abhängigkeit von einzelnen Anbietern;
> - Gefahr der Zweckentfremdung und des Data Mining von Metadaten.
>
> Diese Risiken können durch geeignete Massnahmen – etwa klare Regelungen zu Kontrollrechten, Beschränkung der auszulagernden Datenarten oder starke Verschlüsselung – reduziert werden.
>
> Eine neue gesetzliche Grundlage soll klare Regelungen zu Voraussetzungen, Zuständigkeiten, Verantwortlichkeiten und zum Risikomanagement bei der Auslagerung von Informatikdienstleistungen schaffen. Insbesondere ist zu klären, ob und welche Personendaten in Clouds ausgelagert werden sollen; dies insbesondere im Hinblick auf besondere Personendaten. Aber es sind nicht nur

Personendaten, sondern auch Sachdaten zu berücksichtigen, sofern sie ein öffentliches Interesse betreffen.

Die Motionär:innen fordern den Regierungsrat auf, aus obengenannten Gründen innert einem Jahr eine gesetzliche Grundlage für die Auslagerung von Informatikdienstleistungen zu schaffen.

Anina Ineichen, Salome Bessenich, Bruno Lötscher-Steiger, Tobias Christ, Tonja Zürcher, Michael Graber, Adrian Iselin, Barbara Heer, Andrea Strahm, Fleur Weibel»

Wir nehmen zu dieser Motion wie folgt Stellung:

1. Zur rechtlichen Zulässigkeit der Motion

1.1 Grundlagen des Motionsrechts

Mit einer Motion kann der Grosse Rat den Regierungsrat verpflichten, eine Verfassungs- oder Gesetzesvorlage oder eine Vorlage für einen Grossratsbeschluss vorzulegen (§ 42 Abs. 1 GO) oder eine Massnahme zu ergreifen (§ 42 Abs. 1bis GO). Der Grosse Rat kann dem Regierungsrat also sowohl in seinem eigenen Zuständigkeitsbereich als auch im Zuständigkeitsbereich des Regierungsrats Aufträge erteilen.

Das Recht setzt dem Grossen Rat bezüglich Motionsbegehren allerdings auch Schranken, die in der Gewaltenteilung, im Gesetzmässigkeits-, im Föderalismus- und im Demokratieprinzip gründen. So darf eine Motion nicht gegen höherrangiges Recht verstossen (wie Bundesrecht, interkantonales Recht oder kantonales Verfassungsrecht). Zudem ist gemäss § 42 Abs. 2 GO eine Motion unzulässig, die einwirken will auf

- den verfassungsrechtlichen Zuständigkeitsbereich des Regierungsrats,
- einen Einzelfallentscheid,
- einen in gesetzlich geordnetem Verfahren zu treffenden Entscheid, oder
- einen Beschwerdeentscheid.

1.2 Motionsforderung

Mit der vorliegenden Motion wird der Regierungsrat beauftragt, «innert einem Jahr eine gesetzliche Grundlage für die Auslagerung von Informatikdienstleistungen zu schaffen».

1.3 Rechtliche Prüfung

Bei der alleinigen Durchsicht der Motionsforderung ist unklar, was genau gefordert wird. Erst im Zusammenspiel mit den vorangehenden Ausführungen erhellt sich, dass nicht gefordert ist, dass die Informatikdienstleistungen ausgelagert werden müssen. Vielmehr wird verlangt, dass ein Gesetz die Regelungen festhält, die eingehalten werden müssen, soweit Informatikdienstleistungen ausgelagert werden. Ein so verstandenes Gesetz kann vom Grossen Rat verlangt werden. Mit der Motion wird der Regierungsrat mit der Ausarbeitung eines Gesetzesentwurfes beauftragt. Der Erlass von Gesetzesbestimmungen fällt in die Zuständigkeit des Grossen Rates. Zudem verlangt die Motion nicht etwas, was sich auf den verfassungsrechtlichen Zuständigkeitsbereich des Regierungsrates, auf einen Einzelfallentscheid, auf einen in gesetzlich geordnetem Verfahren zu treffenden Entscheid oder einen Beschwerdeentscheid bezieht. Es spricht auch kein höherrangiges Recht wie Bundesrecht oder kantonales Verfassungsrecht gegen den Motionsinhalt.

1.4 Schlussfolgerung

Die Motion ist als rechtlich zulässig anzusehen.

2. Anliegen der Motion

Davon ausgehend, dass eine Rechtslücke besteht, fordert die Motion die Schaffung einer gesetzlichen Grundlage für die Auslagerung von Informatikdienstleistungen innert Jahresfrist. Diese soll Regeln zu Voraussetzungen, Zuständigkeiten, Verantwortlichkeiten und zum Risikomanagement bei Auslagerungen festlegen. Dabei sei im Besonderen zu klären, ob und welche Personendaten – namentlich besonders schützenswerte –, aber auch Sachdaten von öffentlichem Interesse in Clouds ausgelagert werden sollen.

3. Einleitung

Der Regierungsrat anerkennt die Relevanz des in der Motion aufgeworfenen Themas. Er stimmt der Grundprämisse zu, dass die Auslagerung von Informatikfunktionen, einschliesslich Cloud-Diensten, in der öffentlichen Verwaltung gängige Praxis und notwendig ist. Seit Jahrzehnten werden Informatikfunktionen auch in öffentlichen Verwaltungen (nicht nur im Kanton Basel-Stadt) an spezialisierte Anbieter ausgelagert, weil sie bestimmte Aufgaben besser wahrnehmen können. Ebenso teilt der Regierungsrat das Anliegen der Motionärinnen und Motionäre, dass der Schutz von Daten und die Gewährleistung der Informationssicherheit bei der Auslagerung von Informatikdienstleistungen höchste Priorität haben müssen.

Hingegen widerspricht er der zentralen Forderung der Motion, eine neue gesetzliche Grundlage sei nötig bzw. angezeigt, wie nachfolgend dargelegt wird.

4. Bestehender Rechtsrahmen Kanton Basel-Stadt

Mit Inkrafttreten am 1. Januar 2025 wurden das Gesetz über die Information und den Datenschutz vom 9. Juni 2010 (Informations- und Datenschutzgesetz, IDG; SG 153.260) sowie die Verordnung über die Information und den Datenschutz vom 9. August 2011 (Informations- und Datenschutzverordnung, IDV; SG 153.270) umfassend revidiert und an übergeordnetes Recht angepasst[1]. Bereits die alte Fassung von 2010 enthielt in § 7 aIDG eine gesetzliche Grundlage für die Auslagerung von Informatikdienstleistungen und mit § 23 IDG eine Regelung zur Übermittlung von Personendaten ins Ausland. Mit der Revision wurden § 7 und weitere Regeln des IDG zur Auslagerung ergänzt und verschärft. Das geltende Recht deckt damit das zentrale Anliegen der Motion bereits ab.

Nachfolgend wird dargelegt, wie das IDG die Informationssicherheit und den Datenschutz bei Auslagerungen umfassend und angemessen gewährleistet.

4.1 § 3 IDG Definition von Daten bzw. Informationen

Was als Daten zu verstehen ist, ergibt sich aus der Definition des Begriffs «Informationen» in §3 IDG Abs. 2: «alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen». Personendaten werden in § 3 Abs. 3 IDG als eine Unterkategorie von Informationen definiert und in Abs. 4 werden besondere Personendaten präzisiert.

[1] Im Besonderen: Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1, und Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung, SR 0.235.11; Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (EU-Datenschutz-Richtlinie), ABl. L 119 vom 4.5.2016, 89 ff.; vgl. den Ratschlag des Regierungsrates zu einer Änderung des Gesetzes über die Information und den Datenschutz vom 9. Juni 2010 (Informations- und Datenschutzgesetz, IDG) und weiterer Gesetze (Anpassung an die europäischen Datenschutzreformen und weitere Anpassungen); 21.1239.01.

4.2 § 7 IDG als rechtliche Grundlage für Auslagerung von Informatikdienstleistungen

Der juristische Fachbegriff für die Auslagerung von Datenbearbeitungen bei Informatikdienstleistungen ist «Auftragsdatenbearbeitung». Die Auftragsdatenbearbeitung wird in § 7 IDG geregelt:

§ 7 Bearbeiten im Auftrag
[1] Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, wenn:
a) keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und
b) sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte.
[2] Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.
[3] Eine Auftragsdatenbearbeiterin beziehungsweise ein Auftragsdatenbearbeiter darf ohne vorgängige schriftliche Zustimmung des auftraggebenden öffentlichen Organs die Datenbearbeitung keiner weiteren Auftragsdatenbearbeiterin und keinem weiteren Auftragsdatenbearbeiter übertragen.

Die Bekanntgabe von Daten an Auftragsdatenbearbeitende, d.h. die Auslagerung von Daten, ist selbst eine Datenbearbeitung.

§ 7 IDG stellt die für Auslagerungen benötigte gesetzliche Grundlage dar. § 7 IDG erlaubt Auslagerungen von Informatikdienstleistungen nicht generell, sondern stellt dafür spezielle Voraussetzungen auf:

- Gemäss § 7 Abs. 1 lit. a IDG darf der Auslagerung keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegenstehen. Darunter fallen insbesondere vertragliche Zusicherungen des öffentlichen Organs gegenüber Dritten, die eine Weitergabe der Daten an externe Dienstleistende untersagen, z.B. Geheimhaltungsvereinbarungen. Entgegenstehende rechtliche Bestimmungen können z.B. gesetzliche Schweigepflichten sein, soweit keine gesetzeskonforme Ausgestaltung der Auftragsdatenbearbeitung möglich ist.
- Im Rahmen der Auslagerung von Informatikdienstleistungen finden Datenbearbeitungen bei der oder dem Auftragsdatenbearbeitenden statt. Diese darf die Daten des öffentlichen Organs aber nicht nach Belieben bearbeiten, sondern muss nach § 7 Abs. 1 lit. b IDG verpflichtet werden, die Daten nach den gleichen Regeln zu bearbeiten, die für das öffentliche Organ gelten. Zu diesem Zweck muss ein Auftragsdatenbearbeitungsvertrag (ADV) mit der oder dem Dienstleistenden abgeschlossen werden. Damit wird diese zu den gleichen grundlegenden (oder strengeren) Schutzmassnahmen verpflichtet wie das öffentliche Organ.
- Die Verantwortung verbleibt gemäss § 7 Abs. 2 IDG stets beim auslagernden öffentlichen Organ, sie kann nicht an den externen Dienstleistende delegiert werden. Das öffentliche Organ haftet auch nach der Auslagerung für die Einhaltung sämtlicher Vorschriften. Bei Auslagerungsvorhaben, die mehrere öffentliche Organe betreffen (z.B. eine gemeinsame Cloud-Lösung), schreibt zudem § 6 Abs. 2 IDG vor, dass die Zuständigkeit untereinander zu regeln ist und eine Stelle mit der Gesamtverantwortung betraut werden muss.
- Mit der Revision des IDG per 1. Januar 2025 wurde in § 7 Abs. 3 eine wichtige zusätzliche Schranke der Auftragsdatenbearbeitung eingeführt: Auftragsdatenbearbeitende dürfen die ihnen anvertrauten Daten nicht ohne vorherige schriftliche Zustimmung des öffentlichen Organs an weitere Subunternehmen («Sub-Auftragsdatenbearbeitende») weitergeben. Die Bestimmung verhindert, dass unkontrollierte und intransparente Ketten von Sub-Auftragsdatenbearbeitungen entstehen, bei denen der Kanton die Hoheit und Kenntnis darüber verlieren könnte, wer seine Daten wo und wie bearbeitet.

In Verbindung mit § 3 Abs. 2 bzw. 3 und 4 IDG erstreckt sich der Anwendungsbereich von § 7 IDG sowohl auf Personendaten als auch auf Sachdaten, und ist bei sämtlichen Auslagerungen von Informatikdienstleistungen, also auch Public Cloud-Lösungen, anzuwenden. so dass ein weiteres Anliegen der Motion abgedeckt wird.

Ferner wurden Begriffsbestimmungen in § 3 der neue Abs. 8 hinzugefügt, der den Begriff «Auftragsdatenbearbeiterin/Auftragsdatenbearbeiter» erläutert.

4.3 § 23 IDG Bekanntgabe von Daten ins Ausland

- Anders als im Motionstext festgehalten regelt das IDG die grenzüberschreitende Auslagerung von Personendaten, und zwar in § 23 IDG. Diese Bestimmung stellt für die Bekanntgabe von Personendaten ins Ausland zusätzliche Anforderungen auf, die den Datenschutz gewährleisten: Erfolgt die Bekanntgabe von Personendaten in einen Staat, der dem Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (SR 0.235.1) nicht beigetreten ist, muss entweder die dortige Gesetzgebung einen angemessenen Schutz gewährleisten (lit. a) oder dieser Schutz muss durch spezifische vertragliche Garantien sichergestellt werden (lit. b).
- Zur Bestimmung, ob die Gesetzgebung von Drittstaaten einen angemessenen Datenschutz gewährleistet, hat der Bundesrat in Anhang 1 der Verordnung des Bundes über den Datenschutz (Datenschutzverordnung, DSV) vom 31. August 2022 (SR 235.11) eine Staatenliste herausgegeben. § 11 IDV verweist wie das in der Motion angesprochene Solothurner Auslagerungsgesetz auf diese Staatenliste. Die USA sind seit dem Inkrafttreten des «Swiss-U.S. Data Privacy Framework» am 15. September 2024 unter Vorbehalt erneut auf der Liste aufgeführt. Das Datenschutzabkommen der Schweiz mit den USA sieht eine Zertifizierung vor, welche US-Unternehmen durchlaufen müssen, damit Personendaten aus der Schweiz an diese Unternehmen übermittelt werden dürfen. Mit der Zertifizierung für US-Unternehmen wird sichergestellt, dass die vorgesehenen Datenschutzmassnahmen und Datenschutzgarantien eingehalten werden. Namentlich dürfen diese Unternehmen die Daten nur für diejenigen Zwecke bearbeiten, für die sie erhoben wurden. Die Weitergabe an Dritte wie beispielsweise an nicht zertifizierte Unternehmen ist nicht zulässig. Beim Zugang durch US-Behörden auf Personendaten, die von der Schweiz bekanntgegeben werden, sind verschiedene Garantien vorgesehen, einschliesslich eines Beschwerdemechanismus. Gewährleistet das Recht des Empfängerstaates keinen angemessenen Schutz, müssen gemäss § 23 lit. b IDG vertragliche Garantien einen solchen Schutz sicherstellen. Über die getroffenen Sicherheitsvorkehrungen bei solchen Auslagerungen ins Ausland ist die oder der Datenschutzbeauftragte vorab zu informieren (§ 11 Abs. 2 IDV).

4.4 §12a IDG-Datenschutz-Folgenabschätzung (DSFA) und Risikoanalyse

Jede Auslagerung verändert die mit der Datenbearbeitung verbundenen Risiken. Ein mögliches Risiko ist, dass Auftragsdatenbearbeitende ihre vertraglichen und gesetzlichen Pflichten verletzen (z.B. Fahrlässigkeit von Mitarbeitenden, unbefugte Weitergabe von Daten, etc.). Ausgelagerte Daten können ferner Ziel für Cyberangriffe durch kriminelle Dritte (z.B. Hacker) werden. Solche Risiken bestehen aber auch bei Bearbeitung durch das öffentliche Organ selbst. Eine Auslagerung bezweckt gerade, diese Risiken zu senken. Bei der Nutzung globaler Cloud-Anbieter ist z.B. der mögliche Zugriff ausländischer Behörden auf die gespeicherten Daten (sog. "Lawful Access"), selbst wenn die Server in Europa bzw. in der Schweiz stehen, ein weiteres Risiko.

Mit der Revision des IDG per 1. Januar 2025 wurde die Datenschutz-Folgenabschätzung (DSFA) gemäss § 12a IDG eingeführt, wie sie auch Bund und EU kennen. Ziel der DSFA ist es, Risiken für die Grundrechte von Personen bei neuen Datenverarbeitungsvorhaben – insbesondere auch bei Auslagerungen – frühzeitig zu erkennen und zu minimieren.

In einem ersten Schritt verlangt § 12a Abs. 1 IDG bei jedem Vorhaben eine Prüfung, ob voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht (sog. Schwellenwertanalyse, SWA). Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien (z.B. Public Cloud-Vorhaben), aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Ein hohes Risiko besteht z.B. in jedem Fall auch technologieunabhängig, wenn Daten von mehr als 10'000 Personen betroffen sind.

Besteht voraussichtlich ein hohes Risiko, ist in einem zweiten Schritt gemäss § 12a Abs. 2 IDG eine DSFA durchzuführen. Diese enthält gemäss § 12a Abs. 3 IDG mindestens eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge (lit. a), eine Bewertung der in Bezug auf die Grundrechte der betroffenen Personen bestehenden Risiken (lit. b) sowie eine Darstellung und Bewertung der geplanten Massnahmen, durch die der Schutz der Grundrechte der Personen sichergestellt und der Nachweis erbracht werden soll, dass das IDG eingehalten wird.

Mit der DSFA werden die verschiedenen Gefahrenquellen systematisch erfasst, bewertet und durch konkrete Massnahmen adressiert. Dies erfordert eine genaue Analyse der internen Sicherheitsarchitektur des oder der Dienstleistende, wie robust die Systeme gegen Angriffe von aussen geschützt sind, welche Möglichkeiten der oder die Dienstleistende hat, sich im Falle eines «Lawful Access» zu wehren, etc. Die in der DSFA dokumentierten Abhilfemassnahmen müssen sicherstellen, dass das Schutzniveau des externen Anbieters mindestens dem kantonalen Standard gemäss der «Weisung Schutzmassnahmen Informationssicherheit» (Ziff. 4.7.2) entspricht.

4.5 §13 IDG Vorabkonsultation

Ergibt die SWA gemäss § 12a Abs. 1 IDG ein hohes Risiko, ist neben der DSFA eine Vorabkonsultation der oder des Datenschutzbeauftragten erforderlich (§13 IDG). Ziel des frühzeitigen Einbezuges ist es insbesondere, die Ermittlung und Bewertung der Risiken und der geplanten Massnahmen zu überprüfen und dafür zu sorgen, dass gegebenenfalls mit rechtlichen, organisatorischen oder technischen Massnahmen das Risiko weiter reduziert wird.

Am Ende der DSFA und Vorabkonsultation steht eine fundierte, informierte Entscheidung: Die Leitung des verantwortlichen Organs muss das verbleibende Restrisiko bewerten und formell übernehmen. Erscheint dieses Restrisiko als untragbar, muss auf die Auslagerung oder das Vorhaben verzichtet werden.

4.6 § 45 IDG Aufsicht bei Auftragsdatenbearbeitungen

Die Aufsicht der oder des Datenschutzbeauftragten erstreckt sich vollumfänglich auch auf Auftragsdatenbearbeitende. Gemäss § 45 IDG hat die oder der Datenschutzbeauftragte dieselben umfassenden Kontrollbefugnisse wie gegenüber den kantonalen Organen selbst. Diese umfassen insbesondere das Recht, jederzeit Auskunft zu verlangen, Einsicht in alle relevanten Unterlagen zu nehmen und sich Bearbeitungen vorführen zu lassen. Die Auftragsdatenbearbeiter sind gesetzlich verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben umfassend zu unterstützen. Damit wird sichergestellt, dass die Einhaltung der Datenschutzvorschriften auch bei ausgelagerten Informatikdienstleistungen lückenlos kontrolliert werden kann.

Neben den vertragsrechtlichen Folgen drohen den Auftragsdatenbearbeitenden strafrechtliche Sanktionen bei Verstössen gegen den Auftragsdatenbearbeitungsvertrag (ADV). Der Straftatbestand für Auftragsdatenbearbeitende, die Personendaten vertragswidrig bearbeiten (§ 51 Abs. 1 IDG) wurde anlässlich der Revision per 1. Januar 2025 erweitert und verschärft.

4.7 Weitere rechtliche Rahmenbedingungen

Weitere zu erfüllende Voraussetzungen ergeben sich hauptsächlich aus den übrigen Bestimmungen des IDG, der Verordnung über die Information und den Datenschutz (Informations- und

Datenschutzverordnung, IDV) vom 9. August 2011 (SG 153.270), die ebenfalls per 1. Januar 2025 revidiert wurde, sowie der Verordnung über die Informationssicherheit (ISV) vom 13. Dezember 2016 (SG 153.320).

4.7.1 Weitere Pflichten und Voraussetzungen aus dem IDG

Relevant im Kontext der Auftragsdatenbearbeitung sind insbesondere folgende weitere Pflichten:

- Das öffentliche Organ muss durch angemessene organisatorische und technische Massnahmen die Schutzziele der Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit sicherstellen (§ 8 Abs. 2 IDG).
- Eine Bearbeitung von Personendaten ist ferner nur zulässig, wenn dafür eine gesetzliche Grundlage besteht oder sie zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist (§ 9 Abs. 1 IDG).
- Für die Bearbeitung besonderer Personendaten gelten strengere Anforderungen, wie eine ausdrückliche gesetzliche Ermächtigung oder die zwingende Notwendigkeit für die Erfüllung einer gesetzlich klar umschriebenen Aufgabe (§ 9 Abs. 2 IDG).
- Jede Bearbeitung muss zudem verhältnismässig, nach Treu und Glauben und innerhalb des Zwecks der Datenerhebung erfolgen (§§ 9 Abs. 3 und 12 IDG).
- Mit der Revision des IDG per 1. Januar 2025 wurde der Rechtsrahmen um eine explizite Nachweispflicht erweitert: Das öffentliche Organ muss jederzeit nachweisen können, dass es die Datenschutzbestimmungen einhält (§ 6 Abs. 3 IDG). § 14 IDG schreibt neu vor, dass IT-Systeme von Anfang an datenschutzfreundlich gestaltet werden und die Standardeinstellungen die Privatsphäre der Nutzenden schützen müssen («Privacy by Design/Default»).
- Ergänzend schafft das in § 24 IDG vorgeschriebene öffentliche Verzeichnis aller Verfahren mit Personendaten die notwendige Transparenz für die Bevölkerung, um ihre Datenschutzrechte wirksam ausüben zu können.

4.7.2 Verantwortung und Umsetzung der Vorgaben bei Auftragsdatenbearbeitungen in der ISV und der Weisung Schutzmassnahmen Informationssicherheit (Schutzkatalog)

Die ISV übersetzt die gesetzlichen Vorgaben in eine klare Organisationsstruktur mit präzisen Rollen und Kompetenzen.

- Der Regierungsrat trägt die strategische Gesamtverantwortung für die Informationssicherheit im Kanton (§ 3 ISV).
- Er hat die Kompetenz zum Erlass von Weisungen an ein Fachgremium delegiert: Gemäss § 4 Abs. 2 ISV ist das Steuerungsorgan für Informationssicherheit (heute die «Konferenz für Informatik und Informationssicherheit», KIS) befugt, Weisungen zu erlassen und deren Einhaltung zu kontrollieren.
- Die ISV etabliert die operative Verantwortung beim sogenannten «Dateneigner» (§ 8 ISV). Dies entspricht dem öffentlichen Organ gemäss IDG, das für seine Daten zuständig ist und bei einer Auslagerung sicherstellen muss, dass der Schutzbedarf ermittelt, Risiken analysiert und die notwendigen Schutzmassnahmen umgesetzt werden.
- Sie verpflichtet, zusätzlich zu §24 IDG, zudem jedes Departement, ein Verzeichnis über alle Informationsbestände und IKT-Anwendungen zu führen (§ 7 Abs. 3 lit. b ISV). Diese Inventarisierung schafft die grundlegende Transparenz über die gesamte Datenlandschaft des Kantons.

Die von der KIS erlassene «Weisung Schutzmassnahmen Informationssicherheit (Schutzkatalog)» ist das Instrument für die praktische Umsetzung: Sie schliesst die Lücke zwischen abstrakten Rechtsvorgaben und der technischen Realität bei Auslagerungen. Die Weisung wurde per Inkraftsetzung am 31. Januar 2025 auf den neuesten Stand gebracht und enthält seither mehrere Massnahmen für die Auslagerung von Informatikdienstleistungen, im Besonderen für Public Cloud-Vorhaben.

- Die Weisung liefert dem Dateneigner ein konkretes Pflichtenheft, wie er seine Datenverantwortung zu erfüllen hat. Er muss nachweislich dokumentieren, wie beispielsweise die Verantwortlichkeiten im Cloud-Modell geregelt sind, wie der Zugriff durch externe Administratoren verhindert wird, wie die Portabilität der Sach- und Personendaten sichergestellt ist und wo die Daten gespeichert sind.
- Unter Anderem muss der Dateneigner gemäss der Klassifizierung der Daten bzw. deren Schutzbedarf (Vertraulichkeit, Verfügbarkeit, Integrität, Zurechenbarkeit und Nachvollziehbarkeit) für jeden Dienst die Datenablage festlegen. Diese gilt dann für die einzelnen Mitarbeitenden.
- Die Weisung hält fest, dass als “geheim” klassifizierte Daten, wie beispielsweise Informationen zum Landesschutz oder Adoptionsdaten, grundsätzlich nicht in einer Public Cloud, sondern nur in der IT-Infrastruktur des Kantons bearbeitet werden dürfen.
- Für als «vertraulich» eingestufte Daten, d.h. Informationen mit erhöhtem Schutzbedarf (z.B. besondere Personendaten), gelten strenge Auflagen, wie etwa die Datenhaltung in der Schweiz oder einem Staat mit angemessenem Datenschutzniveau und die obligatorische Verschlüsselung.

5. Vergleich mit dem Kanton Solothurn

Die Motion führt den Kanton Solothurn als Vergleichsgrundlage an. Festzuhalten ist, dass die Kantone Basel-Stadt und Solothurn unterschiedliche Strategien bei der Regulierung der Auslagerungen von Informatikdienstleistungen verfolgt haben. Wie sich aus den Solothurner Materialien ergibt, sah sich der Kanton Solothurn aufgrund seines überholten Informations- und Datenschutzgesetzes (InfoDG) vom 21. Februar 2001 (BGS 114.1) aus dem Jahr 2001 gezwungen, das Gesetz über die Auslagerung von Informatikdienstleistungen (Auslagerungsgesetz, AusG) vom 29. Januar 2025 (BGS 114.5) zu schaffen. Das bisherige Recht wies erhebliche Regelungslücken auf:

- Die Auftragsbearbeitung war nur sehr allgemein geregelt und bot keine konkreten Leitplanken für komplexe Cloud-Vorhaben.
- Eine explizite Grundlage für die Auslagerung sensibler Sachdaten fehlte.
- Die Zuständigkeiten für strategische Auslagerungsentscheide und die Risikotragung waren unklar geregelt.

Das Solothurner Auslagerungsgesetz schloss diese Lücken, es war eine notwendige Reaktion auf das unzureichende InfoDG SO.

Diese Ausgangslage ist nicht mit der Situation im Kanton Basel-Stadt vergleichbar. Das IDG wurde per 1. Januar 2025 umfassend an moderne schweizerische und europäische Standards angepasst. Bereits die alte Fassung des IDG von 2010 enthielt die genannten Lücken des Solothurner InfoDG SO aus dem Jahr 2001 nicht. Anstatt ein neues Gesetz zu erlassen, wurde das bestehende Recht in Basel-Stadt gezielt, orientiert an der europäischen Rechtsentwicklung im Bereich des Datenschutzes, revidiert und um prozessorientierte Instrumente zur Steuerung von Auslagerungsrisiken (z.B. DSFA, § 12a IDG) und um weitere Grundsätze (z.B. Privacy by Default/Design, § 14 IDG) ergänzt.

Ein legislativer Trend, Spezialgesetze für die Auslagerung von Informatikdienstleistungen zu erlassen, ist bei den Kantonen nicht erkennbar. Der Sonderweg des Kantons Solothurn erklärt sich aus einer historischen Regulierungslücke. Es besteht kein Anlass, diesem Sonderweg zu folgen.

6. Anpassung der kantonalen Rechtsgrundlagen nicht angezeigt

6.1 Rechtsrahmen adressiert die angesprochenen Risikobereiche

Wie nachfolgend dargelegt wird, adressiert der bestehende Rechtsrahmen die von den Motionärinnen und Motionären angesprochenen Risikobereiche umfassend und systematisch:

- **Kontrollrechte:** Die Pflicht zur Sicherstellung einer korrekten Bearbeitung (§ 7 Abs. 1 lit. b IDG) erfordert die vertragliche Vereinbarung von Kontrollrechten (z.B. durch Audit- und Einsichtsrechte). Die Nachweispflicht (§ 6 Abs. 3 IDG) verlangt vom öffentlichen Organ, die Ausübung dieser Kontrolle zu dokumentieren. Zudem erstrecken sich die gesetzlichen Kontrollbefugnisse der Datenschutzbeauftragten auch auf Auftragsbearbeiter (§ 45 IDG).

- **Transparenz über Datenbearbeitungen:** Die Nachweispflicht verlangt eine detaillierte Dokumentation der Bearbeitungsprozesse (§ 6 Abs. 3 IDG i.V.m. § 1d IDV). Bei Hochrisikoprojekten muss die DSFA eine genaue Beschreibung der geplanten Vorgänge enthalten (§ 12a Abs. 3 IDG). Das öffentliche Verzeichnis der Bearbeitungstätigkeiten schafft zudem eine Grundtransparenz für die Öffentlichkeit (§ 24 IDG).

- **Transparenz über Serverstandorte und Sicherheitsmassnahmen:** Die Regeln zur grenzüberschreitenden Bekanntgabe erzwingen Transparenz über den Datenstandort (§ 23 IDG). Die ISV und die Dokumentationspflicht nach IDV verlangen eine systematische Erfassung der Risiken sowie die Definition und Dokumentation der technischen und organisatorischen Massnahmen (TOMs, § 8 IDG; § 1d lit. c IDV). Die «Weisung Schutzmassnahmen Informationssicherheit» konkretisiert diese Pflichten und fordert eine Dokumentation der Verantwortlichkeiten und Schutzmassnahmen für Public Cloud-Lösungen.

- **Vertragsgestaltungsspielraum bei Standardanwendungen:** Bei Auslagerung von Informatikdienstleistungen muss ein Auftragsdatenbearbeitungsvertrag (ADV) abgeschlossen werden, der die Pflichten des öffentlichen Organs auf die oder den Auftragsdatenbearbeitenden überbindet. Entspricht der Standardvertrag eines Anbieters dieser Anforderung nicht, ist eine Voraussetzung von § 7 Abs. 1 IDG nicht erfüllt und die Auslagerung nicht zulässig.

- **Durchsetzung von Rechtsansprüchen (z. B. Datenrückgabe/Exit):** Da die Gesamtverantwortung beim Kanton verbleibt (§ 6 Abs. 1 IDG), muss er bei Vertragsabschluss sicherstellen, dass eine geordnete Datenrückgabe und eine Exit-Strategie jederzeit möglich sind. Dies ist eine grundlegende Anforderung, die sich aus § 7 Abs. 1 lit. b IDG ergibt und im Auftragsdatenbearbeitungsvertrag (ADV) geregelt werden muss. Die «Weisung Schutzmassnahmen Informationssicherheit» präzisiert dies für Cloud-Dienste.

- **Risiko des Datenzugriffs durch ausländische Behörden:** Im Rahmen der DSFA wird dieses Risiko bewertet und durch geeignete Massnahmen adressiert (§ 12a IDG). Die «Weisung Schutzmassnahmen Informationssicherheit» sieht hierfür beispielsweise Verschlüsselung vor. Eine Vorabkonsultation der oder des Datenschutzbeauftragten ist notwendig (§ 13 IDG).

- **Abhängigkeit von einzelnen Anbietern:** Das strategische Risiko eines «Lock-in» ist ein Governance-Thema, das im Rahmen der umfassenden Risikoanalyse einer DSFA zu bewerten ist (§ 12a IDG). Die Gesamtverantwortung des öffentlichen Organs (§ 6 IDG) umfasst auch die Pflicht, die langfristige staatliche Handlungsfähigkeit zu sichern. Hier sieht die «Weisung Schutzmassnahmen Informationssicherheit» technische Anforderungen zur Gewährleistung der Datenportabilität vor.

- **Zweckentfremdung und Data Mining:** Dies wird durch die Kombination zweier zentraler Grundsätze des IDG rechtlich unterbunden. Erstens darf der Auftragnehmer die Daten nur so bearbeiten, wie es das öffentliche Organ selbst dürfte (§ 7 Abs. 1 lit. b IDG). Zweitens verbietet der Grundsatz der Zweckbindung (§ 12 IDG) jede Bearbeitung für andere als die ursprünglich festgelegten Zwecke. Eine Nutzung der Daten für eigene Zwecke des Anbieters (z.B. für Werbeprofile) ist somit ein Verstoss gegen ADV und IDG, der gemäss § 51 IDG strafrechtlich sanktioniert wird.

6.2 Auslagerungsgesetz würde Sonderfall Basel-Stadt schaffen

Sollte der Grosse Rat dennoch die Schaffung einer neuen, spezifischen Rechtsgrundlage als unumgänglich erachten, müssten zentrale Fragen sorgfältig geprüft werden, um eine mit Bundes- und internationalem Recht kompatible Lösung zu gewährleisten und einen "Sonderfall Basel-Stadt" zu vermeiden. Das revidierte IDG setzte zwingende internationale Verpflichtungen direkt und sorgfältig um. Ein Sondergesetz würde diesen kohärenten Rechtsrahmen grundlegend ändern, was nicht nur gesetzgeberisch ineffizient wäre, sondern auch die Konformität mit dem europäischen Datenschutzrecht gefährden könnte.

6.3 Kompetenzverschiebung könnte zu Effizienzverlusten führen

Auch eine allfällige Kompetenzverschiebung zwischen Regierungsrat und Grossem Rat und deren Folgen wären genau zu analysieren. Das Parlament setzt Recht und übt Oberaufsicht aus (§§ 80, 90 KV), die Exekutive führt die Verwaltung und erlässt Ausführungsbestimmungen (§ 101 KV; OG § 1, 2, 4, 5). Daher liegen operative Auslagerungsentscheide bei der Exekutive. Eine Verlagerung von Detailkompetenzen ins Parlament würde das System schwerfälliger machen und könnte damit die Handlungsfähigkeit der Exekutive beeinträchtigen. Die Reaktions- und Funktionsfähigkeit der Verwaltung im dynamischen IT-Umfeld könnte eingeschränkt werden, wenn z.B. der Grosse Rat die Länderliste für Datenübermittlungen prüfen und aktualisieren müsste oder strategische Auslagerungen einer allfälligen Genehmigungspflicht durch den Grossen Rat unterliegen.

6.4 Auslagerungsgesetz weder notwendig noch angezeigt

Die vorangehende Auslegeordnung verdeutlicht, dass der Kanton Basel-Stadt unter den per 1. Januar 2025 revidierten Rechtsgrundlagen ein robustes und modernes System zur Steuerung der Auslagerung von Informatikdienstleistungen, insbesondere Cloud-basierten Vorhaben etabliert hat. Mit den bestehenden Rechtsgrundlagen werden die mit der Auslagerung von Informatikdienstleistungen verbundenen, Risiken angemessen gesteuert. Das baselstädtische Recht erreicht damit bereits heute ein hohes Schutzniveau. Die Notwendigkeit für Gesetzesanpassungen besteht nicht.

Vor dem Hintergrund eines möglichen datenschutzrechtlichen Sonderfalls Basel-Stadt und potenzieller Einschränkungen der Agilität der Verwaltung in einem sehr dynamischen Umfeld, ist auch die Zweckmässigkeit von Gesetzesanpassungen zu hinterfragen.

Dem Solothurner Weg zu folgen und ein separates Auslagerungsgesetz zu schaffen, wie dies die Motion fordert, erachtet der Regierungsrat daher als weder notwendig noch angezeigt.

Zudem weist der Regierungsrat darauf hin, dass die in der Motion geforderte Frist von einem Jahr für die Vorlage einer solchen Rechtsgrundlage aus gesetzgeberischer Sicht unrealistisch ist.

7. Operative Folgen allfälliger Anpassungen des Rechtsrahmens

Im Kanton Basel-Stadt wird heute, basierend auf einer modernen und umfassenden gesetzlichen Grundlage, im Einzelfall entschieden, ob die Verwaltung einen Informatikdienst in Zusammenarbeit mit externen Partnern selbst betreibt oder diesen vollständig ausgelagert. Dabei werden die Vor-

und Nachteile unter Berücksichtigung von Sicherheit, Datenschutz, Verfügbarkeit, Effizienz und Wirtschaftlichkeit sorgfältig abgewogen.

Entsprechend liegen die kantonalen Daten schon heute sowohl in vom Kanton angemieteten Servern in verschiedenen Rechenzentren (on premise, z.B. Steuerdaten) wie auch in verschiedenen Betriebsmodellen von Drittanbietern, darunter auch Cloud-Lösungen (z.B. Mailserver).

Diese Form der Aufgabenerfüllung ist in der öffentlichen Verwaltung etabliert und bewährt. Sie ermöglicht es, den hohen Anforderungen an Informationssicherheit, Verfügbarkeit und Wirtschaftlichkeit in einem zunehmend komplexen Umfeld gerecht zu werden.

Beim Kanton werden etwa Arbeitsplatzservices, Netzwerk, Perimeter Infrastruktur, Datenbankservices sowie das Security Operations Center (SOC) im Rahmen von Servicebezügen durch Partner betrieben – viele davon im Zuge der jüngsten Initiative zur Erneuerung der Infrastruktur oder zur Stärkung der Informationssicherheit.

Falls ein Gesetzgebungsprozess angestossen werden sollte, rechnet der Regierungsrat mit Auswirkungen auf verschiedenen operativen Ebenen:

7.1 Obstruktion in der Übergangsphase

Während der Ausarbeitung und Inkraftsetzung neuer Regelungen bestünde das Risiko einer mehrjährigen Phase der Rechtsunsicherheit. Diese würde insbesondere anstehende und laufende Projekte betreffen.

Die Frage stellt sich, ob Grossprojekte für einen neuen Dienst im Leistungsbezug überhaupt gestartet werden könnten, solange unklar ist, ob das zugrunde liegende Betriebsmodell den zukünftigen Rechtsgrundlagen entspricht.

Solche Unsicherheiten führen dazu, dass Projekte sistiert oder verschoben werden müssten, mit unmittelbaren Auswirkungen auf Zeitpläne, Budget und strategische Abhängigkeiten.

7.2 Technische und organisatorische Handlungsfähigkeit

Die kantonale Verwaltung ist darauf angewiesen, rasch und flexibel auf technologische Entwicklungen, Sicherheitsanforderungen und Marktveränderungen reagieren zu können.

Schon heute können die erforderlichen Abklärungen, insbesondere betreffend die Bearbeitung und den Schutz von Personendaten, mehrere Monate oder Jahre in Anspruch nehmen.

Ein Gesetzgebungsprozess und, je nach dessen Ausgang, neue Verfahrensschritte, würden die Umsetzung von IT-Projekten verzögern und damit den eigenen Ansprüchen des Kantons in Bezug auf Kundenorientierung, Digitalisierung und IT-Sicherheit entgegenstehen.

7.3 Betriebskontinuität, Stabilität und Kostenfolgen

Ein grosser Teil der heutigen IT-Services wird in partnerschaftlichen Betriebsmodellen geführt. Dazu gehören etwa das Security Operations Center (SOC), Netzwerk- und Datenbankservices sowie die Workplace- und Kollaborationsinfrastruktur. Diese Modelle gewährleisten eine hohe Stabilität, Skalierbarkeit und Sicherheitsabdeckung.

Mit dem anstehenden Ende verschiedener Servicelebenszyklen wird derzeit geprüft, welcher Grad an Auslagerung bzw. Fremdbezug jeweils optimal für die Zukunft ist. Dabei wird die Strategie verfolgt, strategisch wichtiges Wissen gezielt intern zu halten oder wieder aufzubauen. Allfällige Neuregelungen der Rechtsgrundlagen könnten dazu führen, dass Dienstleistungen, die nicht mehr

vereinbar wären, potenziell vor Ende ihres Lebenszyklus in aufwändigen Projekten neu definiert und für den internen Betrieb aufgestellt werden. Es muss von substanziellen Projektkosten und einer deutlichen Erhöhung des Personalbedarfs als unmittelbare Folge ausgegangen werden.

Am Beispiel des Mailservice können mögliche Folgen aufgezeigt werden:
Dessen Betrieb ist seit über zehn Jahren ausgelagert. Mit der Einführung von Microsoft 365 wird künftig die dem Mailservice zugrundeliegende Infrastruktur und Software an Microsoft übertragen, während die operative Betreuung weiterhin durch kantonale Mitarbeitende erfolgt.

Je nach Ausgang eines allfälligen Gesetzgebungsprozesses, könnte der Betrieb des bestehenden wie auch des künftigen Mailservices in diesen Formen in Frage gestellt sein.

Andererseits würde ein vollständiger Eigenbetrieb beträchtliche Investitionen in Infrastruktur, Personal und Betriebssicherheit erfordern. Ob dabei ein vergleichbares Sicherheits- und Servicelevel erreicht werden könnte, ist fraglich. Die Erkenntnisse aus anderen Verwaltungen lassen eher das Gegenteil befürchten.

8. Fazit

Der Regierungsrat nimmt das Kernanliegen der Motion, den Schutz von Daten bzw. die Informationssicherheit, sehr ernst. Die Auseinandersetzung mit den geltenden Rechtsgrundlagen wie auch den möglichen operativen Konsequenzen, zeigen auf, dass die Umsetzung der Motion weder notwendig noch angezeigt ist.

- Der bestehende Rechtsrahmen (IDG, IDV, ISV) ist modern, umfassend und deckt alle von der Motion aufgeworfenen Fragen ab.
- Im Kanton Basel-Stadt besteht aufgrund seiner aktuellen Rechtsgrundlagen kein Bedarf für separates «Auslagerungsgesetz» wie im Kanton Solothurn. Die geltenden Rechtsgrundlagen bieten ein robustes und transparentes System zur Steuerung der Auslagerung von Informatikdienstleistungen, insbesondere Cloud-basierten Vorhaben, das auf die heutigen Risiken ausgerichtet ist.
- Eine Verschiebung der Zuständigkeiten bzw. eine Verlagerung von Detailkompetenzen ins Parlament würden das System schwerfälliger machen und damit die Handlungsfähigkeit der Verwaltung im dynamischen IT-Umfeld beeinträchtigen.
- Die Beeinträchtigungen der Funktionalität der IT-Dienstleistungen und die damit verbundenen finanziellen Folgen auf Grund eines allfälligen Gesetzgebungsprozesses könnten unter Umständen schwerwiegend ausfallen.

9. Antrag

Auf Grund dieser Stellungnahme beantragen wir, die Motion Anina Ineichen und Konsorten betreffend „Schaffung einer gesetzlichen Grundlage für die Auslagerung von Informatikdienstleistungen“ dem Regierungsrat nicht zu überweisen.

Im Namen des Regierungsrates des Kantons Basel-Stadt

Dr. Conradin Cramer
Regierungspräsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin