KANTON solothurn

KR.Nr.

Gesetz über die Auslagerung von Informatikdienstleistungen (Auslagerungsgesetz, AusG)

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

Zuständiges Departement

Finanzdepartement

Vorberatende Kommissionen

Finanzkommission

Inhaltsverzeichnis

Beilagen

Beschlussesentwurf

Kurzfassung

In den letzten Jahren hat sich die Informationstechnologie stark weiterentwickelt. Der Einsatz von Informationstechnologie ist oft mit umfangreichen Auslagerungen an Dritte verbunden. Vermehrt werden Informatikdienstleistungen über Cloud-Lösungen bezogen. Solche Auslagerungen sind mit Risiken und Herausforderungen verbunden. Gegenwärtig fehlen im Kanton Solothurn die erforderlichen Rechtsgrundlagen für besonders bedeutsame, umfangreiche oder risikobehaftete Auslagerungen von Informatikdienstleistungen. Mit dieser Vorlage wird die gesetzliche Grundlage geschaffen, welche die Voraussetzungen, Zuständigkeiten und Verantwortlichkeiten bei der Auslagerung von Informatikdienstleistungen durch die kantonale Verwaltung regelt.

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen nachfolgend Botschaft und Entwurf des Gesetzes über die Auslagerung von Informatikdienstleistungen.

1. Ausgangslage

Angesichts der sich stetig und immer schneller ändernden Informationstechnologien nehmen cloudbasierte technische Lösungen eine immer zentraler werdende Rolle ein. Die Anforderungen in diversen Bereichen der kantonalen Verwaltung tendieren immer häufiger in Richtung plattformunabhängige Zugangsmöglichkeiten und die Erwartungen an «mobile Arbeit jederzeit und überall» steigen stetig. Die Erfahrungen zeigen weiter, dass viele Anbieter von IT-Lösungen von Systemen abrücken, welche in den lokalen Rechenzentren der Kundinnen und Kunden selbst betrieben werden können (sogenannte «On-Premises» Lösungen) und nur noch cloudbasierte Lösungen anbieten. Die Tendenz geht klar in Richtung Cloud-Technologien und es gibt immer weniger Alternativen zu Cloud-Lösungen. Aus diesen Gründen sehen sowohl die Digitalisierungsstrategie des Kantons Solothurn[1] wie auch das «Impulsprogramm SO! Digital 2023-2025»[2] den Einsatz von Cloud-Technologien vor. Die kantonale Verwaltung möchte insbesondere die Einführung von Microsoft 365 als neue Office Version (mit Public-Cloud-Anbindung) als Ersatz zu den bestehenden lokal betriebenen Office-Anwendungen prüfen.

Mit dem Einsatz von Cloud-Technologien ist zwangsläufig eine Auslagerung von Informatikdienstleistungen verbunden. Der Betrieb der ausgelagerten Informatikdienstleistungen findet ausserhalb der Rechenzentren der kantonalen Verwaltung statt, woraus sich neue und veränderte Herausforderungen für die Informationssicherheit, den Datenschutz und die Archivierung ergeben. Werden Personendaten in eine Cloud ausgelagert, liegt eine Datenbearbeitung im Sinne von § 6 Abs. 5 des Informations- und Datenschutzgesetzes vom 21. Februar 2001 (InfoDG, BGS 114.1) vor. Das InfoDG erlaubt in § 17 Abs. 1 zwar unter gewissen Voraussetzungen das Bearbeiten von Personendaten durch Dritte; die vorgenommene Rechtsgrundlagenanalyse hat allerdings ergeben, dass für besonders bedeutsame, umfangreiche oder risikobehaftete Auslagerungen die bestehenden rechtlichen Grundlagen ungenügend sind. Ebenso ist die Auslagerung von Sachdaten (d.h. Daten ohne Personenbezug) auf gesetzlicher Ebene ungenügend geregelt. Mit dieser Vorlage wird für die kantonale Verwaltung die Rechtsgrundlage geschaffen, welche den Rahmen für die Auslagerung von Informatikdienstleistungen und damit auch für die Auslagerung in Clouds definiert. Sie hält insbesondere fest, unter welchen Voraussetzungen eine Auslagerung zulässig ist, wer einen entsprechenden Entscheid zu fällen und wer die Verantwortung für die Auslagerung zu tragen hat.

2. Cloud-Lösungen und deren Einsatzfelder

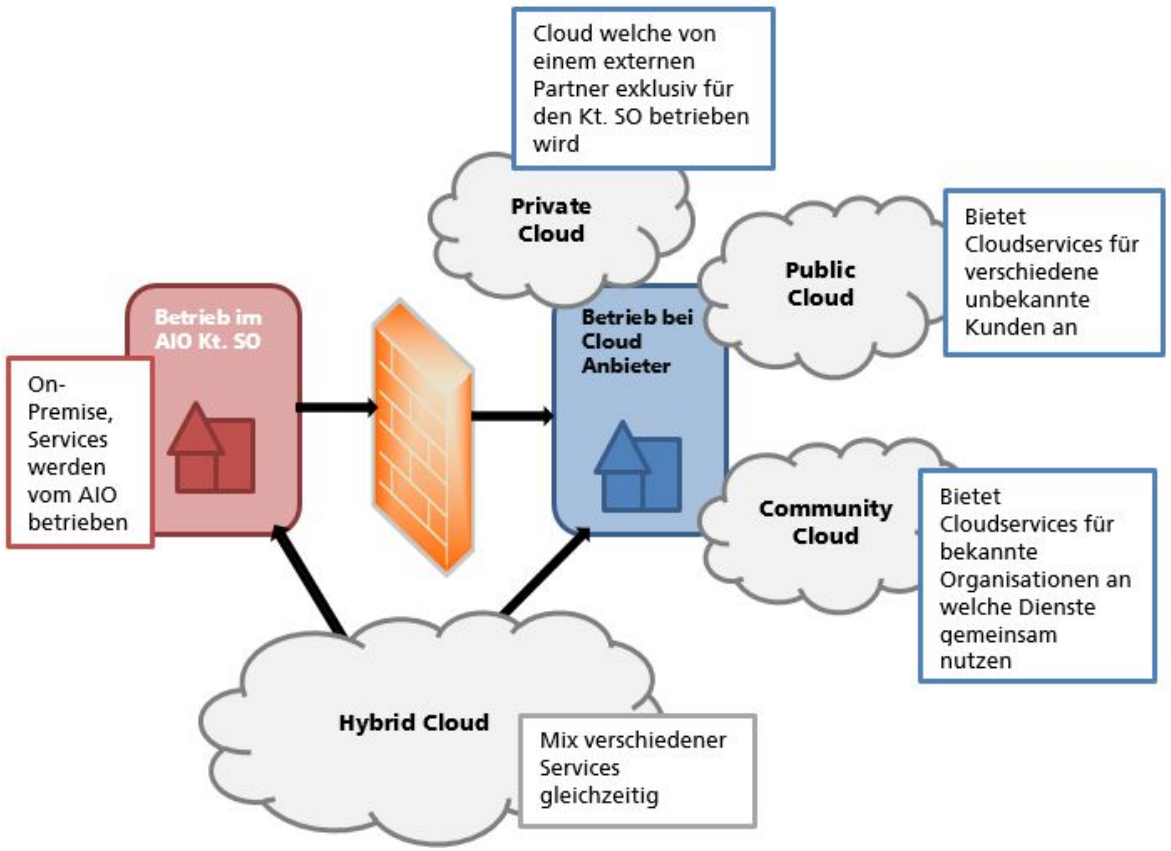
2.1 Begriff und Ausprägungen

«Cloud Computing» ist ein Modell, das es ermöglicht, grundsätzlich jederzeit und von jedem Ort über das Internet und unabhängig vom Gerät auf einen geteilten Pool von konfigurierbaren Computerressourcen zuzugreifen. Diese Ressourcen können in Form von Netzwerken, Servern, Speichersystemen, Anwendungen oder Diensten schnell und mit geringem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden.[3] Häufig wird anstatt des Begriffs «Cloud Computing» die Abkürzung «Cloud» gebraucht.

---

[1] RRB Nr. 2021/716 vom 25. Mai 2021.
[2] RRB Nr. 2022/1575 vom 24. Oktober 2022.
[3] Definition in Anlehnung an PETER MELL/TIMOTHY GRANCE, The NIST Definition of Cloud Computing, National Institute of Standards and Technology (NIST), September 2011, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf (besucht am ...).

Die einzelnen Cloud-Lösungen unterscheiden sich und sind entsprechend vielfältig. Die nachfolgende Abbildung liefert eine Übersicht zu den unterschiedlichen Ausprägungen.



2.2 Einsatz der Public Cloud Anwendung Microsoft 365 in verschiedenen öffentlichen Verwaltungen

Der Einsatz von Microsoft 365 beschäftigt aktuell auch den Bund, immer mehr Kantone und Gemeinden. Der Stand der Arbeiten ist allerdings unterschiedlich weit fortgeschritten und verändert sich dynamisch. Zur Veranschaulichung soll im Folgenden beispielhaft der Einsatz von Microsoft 365, eine klassische Public Cloud-Anwendung, auf Bundesebene und im Kanton Zürich kurz aufgezeigt werden.

Auf Bundesebene dürfen Nutzer und Nutzerinnen in der Cloud von Microsoft keine besonders schützenswerten Daten und keine vertraulichen Dokumente speichern. Die E-Mails und Kalender der Mitarbeitenden der Bundesverwaltung werden weiter vom Bund selber und vor Ort in den Rechenzentren des Bundes verarbeitet und gespeichert.[1] Ab November 2023 führt auch die Armee Microsoft 365 als Kollaborationsplattform für die Truppe ein. Die Kommandanten von Abteilungen und Truppenkörpern der Armee setzen Microsoft 365 für die Planung der Wiederholungskurse sowie für ausserdienstliche Aufgaben ein.[2]

Im März 2022 hat der Zürcher Regierungsrat einen Grundsatzentscheid zugunsten von Cloud-Services von Microsoft gefällt und Rahmenbedingungen für diesen Einsatz definiert.[3] Seither hat

[1] Medienmitteilung des Bundesrats vom 15. Februar 2023, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-93076.html (besucht am ...).
[2] Medienmitteilung des Bundesrats vom 6. November 2023, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-98466.html (besucht am ...).
[3] Beschluss des Regierungsrates des Kantons Zürich, RRB 542/2022 vom 22. März 2022, https://www.zh.ch/bin/zhweb/publish/regierungsratsbeschluss-unterlagen./2022/542/RRB-2022-0542.pdf (besucht am ...).

die Finanzdirektion des Kantons Zürich Ausführungsbestimmungen erlassen, welche diverse Daten (z.B. besonders schützenswerte Personendaten) von der Auslagerung ausnehmen. Verschiedene Kantonsverwaltungen, etwa der Kanton Bern, verfolgen eine ähnliche Stossrichtung.

In den Kantonen St. Gallen und Schaffhausen sowie in den Städten Bern und Zürich laufen ebenfalls Projektarbeiten zum Einsatz von Microsoft 365.

3. Rechtsgrundlage zur Auslagerung

3.1 Ungenügende Rechtsgrundlage im Kanton Solothurn

Das Aufzeichnen, Aufbewahren, Verwenden und zugänglich Machen von Personendaten in einer Cloud stellt ein Bearbeiten von Personendaten im Sinn von § 6 Abs. 5 InfoDG dar. Das InfoDG erlaubt in § 17 Abs. 1 grundsätzlich das Bearbeiten von Personendaten durch Dritte. Die Behörde hat allerdings den Datenschutz durch Vereinbarungen, Auflagen oder in anderer Weise sicherzustellen. Die Verantwortung zum Schutz vor Missbrauch von Personendaten bleibt gemäss dem Wortlaut von § 17 Abs. 1 InfoDG bei der Behörde, welche die Datenbearbeitung auslagert. Die Behörde muss Dritte rechtlich wirksam zur Einhaltung des Datenschutzes verpflichten.[1]

Dort, wo Personendaten ohne besonderen Schutzbedarf von der Auslagerung betroffen sind, genügt die vorhandene Rechtsgrundlage. Auch dort, wo nur einzelne Dienststellen besonders schützenswerte Personendaten zur Bearbeitung auslagern und deren Schutz durch Vereinbarung, Auflagen oder in anderer Weise sicherstellt, genügt die vorhandene Rechtsgrundlage in § 17 Abs. 1 InfoDG. Der Kanton Solothurn verfügt somit über eine 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 vorzugehen ist. Bei der Redaktion von § 17 Abs. 1 InfoDG wurde noch nicht an die Einführung von umfassenden Cloud-Lösungen gedacht. Entsprechend findet sich in der Botschaft zum Informations- und Datenschutzgesetz folgende Erläuterung zu § 17 Abs. 1: «Die Frage, ob und wie weit Dritte mit der Datenbearbeitung beauftragt werden dürfen, wird nicht hier beantwortet.»[2]

Für besonders bedeutsame, umfangreiche oder risikobehaftete Auslagerungen von Informatikdienstleistungen (wie beispielsweise bei gewissen Cloud-Lösungen) benötigt die kantonale Verwaltung damit eine weitergehende Rechtsgrundlage, welche mit dieser Vorlage geschaffen wird.

3.2 Anforderungen an die neue Rechtsgrundlage

Das neue Gesetz soll die Voraussetzungen, die Zuständigkeiten, die Verantwortlichkeiten und das Risikomanagement bei der Auslagerung von Informatikdienstleistungen regeln. Ziel ist es, bei solchen Auslagerungen sowohl den verschiedenen öffentlichen Interessen als auch dem Grundrechtsschutz Rechnung zu tragen.

Eine Auslagerung von Informatikdienstleistungen beinhaltet eine Reihe von faktischen und rechtlichen Risiken und Herausforderungen (vgl. Erwägungen in Ziffer 5.1). Zunächst umfassen solche Auslagerungen sehr oft die Übertragung von Personendaten[3] an Auftragnehmende.

---

[1] Botschaft zum Informations- und Datenschutzgesetz vom 22. August 2000, RRB Nr. 1653, Erläuterungen zu § 17 Abs. 1, S. 20.
[2] Botschaft zum Informations- und Datenschutzgesetz vom 22. August 2000, RRB Nr. 1653, Erläuterungen zu § 17 Abs. 1, S. 20.
[3] Zur Definition von Personendaten siehe § 6 Abs. 2 InfoDG.

Durch die Auslagerung von Personendaten ist der Schutzbereich des Grundrechts der informationellen Selbstbestimmung (Art. 13 Abs. 2 BV; Art. 8 Abs. 2 KV) berührt. Dieser umfasst das Recht jedes Menschen, selber entscheiden zu können, wann, von wem und unter welchen Umständen Daten über ihn bearbeitet werden.[1] Damit Grundrechtseingriffe zulässig sind, müssen sie sich auf eine genügende gesetzliche Grundlage abstützen können, von einem öffentlichen Interesse getragen und verhältnismässig sein sowie den Kerngehalt wahren (Art. 36 BV).[2] Mit dem neuen Gesetz gilt es, die Anforderungen für die Auslagerung von Personendatenbearbeitungen zu konkretisieren und den besonderen Risiken, namentlich bei besonders bedeutsamen oder umfangreichen Auslagerungen, Rechnung zu tragen.

Auch wenn bei einer Auslagerung reine Sachdaten ohne Personenbezug bearbeitet werden und vordergründig kein Grundrechtseingriff erfolgt, können wichtige öffentliche Interessen tangiert sein. Dies ist insbesondere dann der Fall, wenn die Natur der Sachdaten eine gewisse Sensibilität aufweist. Aus diesem Grund beschränkt das vorliegende Gesetz seinen Anwendungsbereich nicht auf Personendaten, sondern umfasst auch reine Sachdaten.

Zweck dieses Gesetzes ist es schliesslich nicht, jede Form von Auslagerung von Informatikdienstleistungen zu legitimieren, sondern rechtliche Anforderungen und Rahmenbedingungen (insbesondere Zuständigkeiten und Verantwortung) für solche Auslagerungen zu definieren. Die Rechtmässigkeit, einschliesslich der Verhältnismässigkeit, jeder konkreten Auslagerung muss im Einzelfall durch eine Gesamtwürdigung der Umstände beurteilt werden.

4. Geltungsbereich

Das Gesetz gilt für alle Behörden der kantonalen Verwaltung und richtet sich am Geltungsbereich der IKT-Strategie 2021-2026 Kanton Solothurn[3] aus. Erfasst sind demnach alle Behörden der kantonalen Verwaltung, inklusive der Gerichte. Vom Geltungsbereich dieses Gesetzes nicht erfasst sind die Solothurner Spitäler AG, die Fachhochschule Nordwestschweiz, die selbständigen öffentlich-rechtlichen Anstalten des Kantons sowie die kantonalen Schulen bezüglich der Informatikdienstleistungen für Unterrichtszwecke. Unter Informatikdienstleistungen für Unterrichtszwecke sind Anwendungen zu verstehen, die in unmittelbarem Zusammenhang mit dem Unterricht, d. h. der Wissensvermittlung durch die Lehrpersonen an die Schüler und Schülerinnen, stehen. Erfasst vom vorliegenden Gesetz ist die Auslagerung von Informatikdienstleistungen an kantonalen Schulen zu anderen Zwecken, etwa zu Verwaltungszwecken (z. B. Personalführung, Kommunikation mit und zwischen Lehrpersonen oder Eltern, Erstellung von Stundenplänen, Raumbewirtschaftung, Stromversorgung, Videoüberwachung etc.).

Ebenfalls nicht erfasst vom Gesetz sind die Gemeinden. Der Regierungsrat plant in einem zweiten Schritt die Auslagerung von Informatikdienstleistungen für alle Behörden gemäss dem Behördenbegriff von § 3 InfoDG zu regeln. Die zeitliche Staffelung ist der Dringlichkeit dieser Vorlage geschuldet.

5. Risiken bei Auslagerungen und Risikominimierung

5.1 Risiken

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. Zusätzlich zum

---

[1] Vgl. ASTRID EPINEY/PETRU EMANUEL ZLATESCU, in: Adrian Bieri/Julian Powell (Hrsg.), Kommentar zum Datenschutzgesetz (DSG), Zürich 2023, Art. 1 N 24.
[2] Vgl. statt vieler REGINA KIENER, Grundrechtsschranken, in: Oliver Diggelmann/Maya Hertig Randall/Benjamin Schindler (Hrsg.), Verfassungsrecht der Schweiz, Bd. II, Zürich 2020, N 27 ff.
[3] RRB-Nr. 2020/1660 vom 24. November 2020.

allgemeinen Risiko, dass die Behörden jegliche Anliegen nicht unmittelbar selbst, sondern nur noch vertragsrechtlich über den jeweiligen Dienstleister umsetzen können, ergeben sich unter anderem folgende Risiken:

- Transparenzdefizite hinsichtlich dem Standort von Servern und Datenbearbeitungen, den vom Anbieter angewandten Datensicherheitsmassnahmen sowie den neben dem Anbieter allenfalls beteiligten Personen (bspw. Unterauftragnehmer);
- Eingeschränkte Kontrollrechte und -möglichkeiten;
- Beschränkter Gestaltungsspielraum insbesondere in Bezug auf den Leistungsumfang und der Vertragsgestaltung bei Standardanwendungen;
- Beschränkte Durchsetzbarkeit von Rechtsansprüchen (z. B. im Zusammenhang mit Datenrückübertragungen);
- Gewährleistung der Vertraulichkeit der von der Auslagerung betroffenen Daten;
- Zugriff auf Daten durch ausländische Behörden (bspw. durch US-amerikanische Strafbehörden gestützt auf den CLOUD Act[1]);
- Gewährleistung der Verfügbarkeit der ausgelagerten Dienstleistungen;
- Zunehmende Abhängigkeit von bestimmten Anbietern;
- Zweckentfremdung der von der Auslagerung betroffenen Daten (insbesondere, wenn Dritte die Daten zu eigenen Zwecken nutzen);
- Data Mining bezüglich der Metadaten von Nutzer und Nutzerinnen;
- Einhalten von Aufbewahrungsfristen und Sicherstellen von Ablieferungen an das Staatsarchiv.

5.2 Mögliche Massnahmen zur Risikominimierung

Die Risiken im Rahmen einer Auslagerung sind durch passende Massnahmen angemessen zu minimieren. Beispiele möglicher Massnahmen:

- Definition von Kontrollrechten;
- Überbindung von Geheimhaltungspflichten;
- Festlegung von Datensicherheitsmassnahmen;
- Regelung von Unterauftragsverhältnissen;
- Regelung der Datenvernichtung und -rückübertragung;
- Festlegung von Unterstützungspflichten vom externen Dienstleister gegenüber der Behörde;
- Definition des Ortes der Datenbearbeitung;

[1] Clarifying Lawful Overseas Use of Data Act, https://www.congress.gov/bill/115th-congress/house-bill/4943 (besucht am ...).

- Festlegung des anwendbaren Rechts und Gerichtsstands;
- Beschränkung der Art der von der Auslagerung betroffenen Daten (z.B. Ausschluss von besonders schützenswerten Personendaten);
- Anonymisierung oder Pseudonymisierung von Daten;
- Verschlüsselungen;
- Ausschluss von zweckfremden Datenbearbeitungen;
- Datenmonitoring im Rahmen des Records Managements.

5.3 Vorhandene Instrumente zur Definition von Risiken und Massnahmen

Es liegt in der Pflicht der Behörde für sichere IT-Lösungen zu sorgen und Massnahmen vorzukehren, welche den Risiken Rechnung tragen. Grundlage dafür ist, die Risiken zu erkennen, diese möglichst zu beseitigen oder aber mit geeigneten Massnahmen auf ein zulässiges und tragbares Mass zu reduzieren. Die kantonale Verwaltung verfügt bei der Durchführung von IT-Projekten über geeignete Instrumente zur Definition von Risiken und Massnahmen. Dies sind Schutzbedarfsanalyse, Risikoanalyse, Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) und entsprechende Bearbeitungsreglemente.

Mit der Schutzbedarfsanalyse wird ermittelt, wie hoch der Schutzbedarf in Bezug auf Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Daten ist.

Wird kein erhöhter Schutzbedarf festgestellt, sind keine besonderen Massnahmen nötig und der Grundschutz der Informatiksysteme zur Gewährleistung der Anforderungen genügt. Wird allerdings ein erhöhter Schutzbedarf festgestellt, wird mittels definierter Vorlage eine Risikoanalyse durchgeführt, um festzustellen, welche Risiken in welchen Bereichen vorhanden sind. Darauf basierend werden Anforderungen an die Sicherheit bestimmt, um den Umgang und die entsprechenden Massnahmen für diese Risiken zu definieren.

Die entsprechenden Massnahmen werden in einem ISDS-Konzept weiter spezifiziert. In der Folge kann beispielsweise ein Bearbeitungsreglement erarbeitet werden.

6. Verantwortung

Grundsätzlich trägt jede Behörde die rechtliche Verantwortung für die eigene Aufgabenerfüllung. Delegiert eine Behörde gewisse Aufgaben an Dritte oder zieht sie Hilfspersonen zur Aufgabenerfüllung bei, geht damit keine Verantwortungsübertragung einher, sondern die Behörde bleibt im vollen Umfang verantwortlich.[1] Ferner entscheidet jede Behörde – unter Beachtung der verfassungsrechtlichen und gesetzlichen Schranken – selbständig, inwiefern sie Dritte zur Aufgabenerfüllung beizieht.

Bei der Auslagerung von Informatikdienstleistungen drängt sich allerdings eine differenzierte Betrachtung auf. So können Auslagerungen einen Entscheid auf höchster Führungsebene erfordern. Dies ist der Fall, wenn die Auslagerung von übergeordnetem oder strategischem Interesse ist, wenn sie für eine oder mehrere Organisationseinheiten zwingend vorgeschrieben werden soll, oder wenn sie ein hohes Risiko für die Grundrechte der betroffenen Personen mit sich bringt (vgl. § 5 und die dazugehörenden Erläuterungen). In all diesen Konstellationen erscheint

[1] DOMINIKA BLONSKI, Cloud – alles Risiko?, SJZ 119/2023, 992.

es sachgerecht, einen Beschluss des Regierungsrates für die kantonale Verwaltung, bzw. der Gerichtsverwaltungskommission für die Gerichte, vorauszusetzen.

Wie einleitend erwähnt, bleibt die auslagernde Behörde, d.h. diejenige Behörde deren Informatikdienstleitungen an Dritte ausgelagert werden, für die rechtmässige Aufgabenerfüllung verantwortlich. Allerdings muss die Verantwortung für die neuen, aufgrund der Auslagerung entstandenen Risiken durch die Behörde getragen werden, welche die Auslagerung gemäss § 5 beschlossen hat. Diese Zusatzverantwortung geht dementsprechend auf den Regierungsrat oder die Gerichtsverwaltungskommission über (vgl. Erläuterungen zu § 7).

7. Vernehmlassungsverfahren

Text

8. Verhältnis zur Planung

Dieses Gesetz hat einen konkreten Bezug zum aktuellen Legislaturplan 2021–2025 (SGB 0206/2021). Das Auslagerungsgesetz wurde aufgrund der Digitalisierungsoffensive des Impulsprogramms in Angriff genommen. Die Gesetzgebungsarbeiten sind Teil der Bemühungen dem im Legislaturplan unter Punkt B.1.2 aufgeführten strategischen Ziel «Digitale Transformation der öffentlichen Verwaltung vorantreiben» nachzukommen und das unter Punkt B.1.2.1 erwähnte Handlungsziel «Umsetzungsprogramm der Digitalisierungsstrategie realisieren» zu erreichen.

9. Auswirkungen

9.1 Personelle und finanzielle Konsequenzen

Allein durch den Erlass des Gesetzes über die Auslagerung von Informatikdienstleitungen ist nicht mit personellen oder finanziellen Konsequenzen zu rechnen. Dieses Gesetz ist aber Grundlage für weitergehende Entscheidungen in Bezug auf Projekte, welche die Auslagerung von Informatikdienstleistungen zur Folge haben, insbesondere Projekte mit Cloud-Fokus. Die Realisierung dieser Projekte kann durchaus personelle und finanzielle Folgen haben (vgl. Erwägungen zu Ziffer 9.4). So müssen Lizenzen beschafft oder Massnahmen zur Risikominimierung ergriffen werden oder allenfalls auch organisatorische Anpassungen personeller Natur erfolgen. Beim Entscheid zur Realisierung dieser Projekte sind die üblichen politischen Wege einzuhalten und die finanziellen und personellen Konsequenzen auszuweisen.

9.2 Vollzugsmassnahmen

Die einzige gesetzliche Grundlage zur Auslagerung findet sich in der kantonalen Gesetzgebung bis anhin in § 17 Abs. 1 InfoDG. Diese Rechtsgrundlage ist allerdings ungenügend (vgl. Erwägungen zu Ziffer 3). Das Auslagerungsgesetz ist neu die Rechtsgrundlage, welche den Rahmen für die Auslagerung von Informatikdienstleistungen vorgibt. Weitere Ausführungsbestimmungen sind nicht vorgesehen, allfällige Vollzugsmassnahmen werden nach dem Erlass des Gesetzes geprüft.

9.3 Folgen für die Gemeinden

Das Gesetz selbst hat keine direkten oder unmittelbaren Folgen für die Gemeinden. Der Geltungsbereich ist auf die Behörden der kantonalen Verwaltung beschränkt (vgl. Erwägungen zu

Ziffer 4). Bei konkreten Projekten, in denen ebenfalls Gemeinden involviert sind, kann es allerdings in der Zusammenarbeit zu Schnittstellen kommen, die geregelt werden müssen.

9.4 Wirtschaftlichkeit

Durch die Auslagerung von Informatikdienstleistungen ergeben sich projektbezogen eine Reihe von Einsparungen, es ist aber auch mit zusätzlichen und neuen Kosten zu rechnen. So sinken oder entfallen Investitionen in eigene Hardware, Software und Infrastruktur, da diese Leistungen von Dritten erbracht werden, die mit der Erbringung der Informatikdienstleistung beauftragt werden. Weitere Aufwendungen, die abnehmen oder entfallen, weil sie von Dritten übernommen werden, sind Aufwendungen für Wartung und Aktualisierungen von Software und Rechenzentrumsinfrastruktur, für Backup- und Wiederherstellungsfunktionalitäten, für Strom- und Kühlungsversorgung sowie für die physische Zugriffskontrolle und die Verwaltung von Immobilien.

Andererseits ist durch die kontinuierliche Nutzung von Informatikdienstleistungen Dritter mit erhöhten Betriebsausgaben und mit weiteren Zusatzkosten zu rechnen. Bei Projekten mit Cloud-Fokus ist mit zusätzlichen Ausgaben für Risikomanagement, Sicherheitsmassnahmen, Notfallplanung und Compliance zu rechnen, ebenso mit Kosten für Datentransfer und Netzwerknutzung. Mit zusätzlichem (personellem) Aufwand verbunden ist die Verwaltung der Dienstleistungsverträge und die Überwachung der Service-Level-Agreements (SLAs). Eine Veränderung oder Umverteilung des Bedarfs an IT-Personal kann sich aus den veränderten Aufgabenbereichen (bzgl. Wartung, Updates, Infrastruktur, Immobilien etc.) ergeben.

10. Erläuterungen zu einzelnen Bestimmungen der Vorlage

§ 1
Es wird auf die Erwägungen in Ziffer 3.2 und Ziffer 4 verwiesen.

§ 2
Es wird auf die Erwägungen in Ziffer 4 verwiesen.

§ 3 Abs. 1
In dieser Bestimmung werden zur Gewährleistung der Rechtssicherheit und besseren Verständlichkeit des Gesetzes zentrale Begriffe definiert.

§ 3 Abs. 1 Bst. a
Auslagerungen gehen jeweils von einer Behörde aus und richten sich an einen Dritten (vgl. Erläuterungen zu § 3 Abs. 1 Bst. c). Mittels Auslagerung wird der Dritte von der Behörde beauftragt, eine Informatikdienstleistung (vgl. Erläuterungen zu § 3 Abs. 1 Bst. b) zu erbringen. Grundsätzlich handelt es sich bei den ausgelagerten Informatikdienstleistungen um neue Dienstleistungen oder um Dienstleistungen, die vormals von der auslagernden Behörde selbständig erbracht worden sind. Eine Auslagerung im Sinne dieses Gesetzes liegt erst vor, wenn sie ein minimales Ausmass (Umfang und Dauer) erreicht. Aus diesem Grund gelten spezifische, einmalige Datenzugriffe Dritter, beispielswiese bei Erbringung von technischem Support, grundsätzlich nicht als Auslagerungen.

Massgeblich mit dem Begriff der «Auslagerung» verknüpft ist der Begriff der «Informatikdienstleistung».

§ 3 Abs. 1 Bst. b
Der Begriff «Informatikdienstleistungen» wird als Oberbegriff für alle Formen der Erbringung von Leistungen in der Informations- und Kommunikationstechnik verwendet. Im Zentrum der Dienstleistung muss immer die elektronische Verarbeitung von Informationen stehen. Aus diesem Grund stellt der blosse Kauf einer Software oder anderer Informatikmittel noch keine Auslagerung von Informatikdienstleistungen im Sinne dieses Gesetzes dar. Ebenfalls nicht erfasst

sind Fälle, in denen verwaltungsexterne Personen den Behörden reine Beratungsdienstleistungen anbieten – unabhängig davon, ob sich die Beratung auf Informatikmittel bezieht.

Die Informatikdienstleistungen umfassen nicht nur die eigentlichen «Kernleistungen», also die Primärfunktionen, welche die Aufgabenerfüllung ermöglichen, miteinbezogen sind auch die notwendigen Umsysteme (z. B. Verzeichnisdienste) und die unterstützenden Systeme (z. B. Anti-Malware, Backup, Administrationsplattformen und -tools) sowie die Bearbeitung von Randdaten.

§ 3 Abs. 1 Bst. c
«Dritte» sind Auftragnehmende ausserhalb der kantonalen Verwaltung, an welche die Informatikdienstleistungen ausgelagert werden. Es wird sich dabei in aller Regel um juristische Personen des Privatrechts handeln, denkbar sind aber auch öffentliche Organe ausserhalb des Kantons Solothurn.

§ 3 Abs. 1 Bst. d
Die «auslagernde Behörde» ist jene Behörde, die zur Erfüllung ihrer öffentlichen Aufgaben Informatikdienstleistungen an einen Dritten auslagert. Die auslagernde Behörde ist somit von der für den Entscheid über die Auslagerung zuständigen Behörde abzugrenzen. Bei Auslagerungen nach § 5 Abs. 1 und 2 ist der Regierungsrat bzw. die Gerichtsverwaltungskommission für den Entscheid zur Auslagerung zuständig.

§ 3 Abs. 1 Bst. e
Die «zuständige Behörde» bestimmt sich nach Massgabe von § 5. Die auslagernde Behörde ist in den Konstellationen von § 5 Abs. 3 auch zuständig zum Beschluss über die Auslagerung. In den Fällen nach § 5 Abs. 1 und 2 ist der Regierungsrat bzw. die Gerichtsverwaltungskommission zuständig.

§ 4 Abs. 1
Jede Auslagerung von Informatikdienstleistungen ist mit besonderen Risiken verbunden (vgl. Erwägungen in Ziffer 5.1). Aus diesem Grund werden in § 4 Abs. 1 die notwendigen Voraussetzungen festgelegt, die erfüllt sein müssen, damit eine Auslagerung von Informatikdienstleistungen zulässig ist. Dass diese Voraussetzungen erfüllt werden, ist durch Gesetz oder schriftliche Vereinbarung sicherzustellen.

§ 4 Abs. 1 Bst. a
Für sämtliches Handeln der Verwaltung besteht die Bindung an das Gesetz. Jedes Verwaltungshandeln muss eine hinreichende gesetzliche Grundlage aufweisen, im öffentlichen Interesse liegen und verhältnismässig sein (Art. 5 BV sowie Art. 5 KV). Eine Behörde kann sich auch durch die Auslagerung von Informatikdienstleistungen nicht von der Bindung an diese Grundprinzipien des rechtsstaatlichen Handelns lösen. Aus diesem Grund darf der Dritte die Informatikdienstleistung nur so und im selben Umfang erbringen, wie die Behörde es selbst tun dürfte. Dementsprechend darf der Dritte die ihm übertragenen Daten nicht für eigene Zwecke nutzen.

§ 4 Abs. 1 Bst. b
Der Schutz der Amts- und Berufsgeheimnisse sowie der Schutz von Personendaten gemäss der kantonalen Datenschutzgesetzgebung dürfen durch die Auslagerung nicht unterlaufen werden. Das allgemeine Amtsgeheimnis ergibt sich aus § 38 des Gesetzes über das Staatspersonal vom 27. September 1992 (BGS 126.1) und ist ebenfalls im Strafgesetzbuch verankert (Art. 320 StGB). Besondere Amtsgeheimnisse sind etwa das Steuergeheimnis (§ 128 des Gesetzes über die Staats- und Gemeindesteuer vom 1. Dezember 1985, BGS 614.11) oder das Sozialhilfegeheimnis (§ 19 des Sozialgesetzes vom 31. Januar 2007, BGS 831.1). Berufsgeheimnisse regelt in erster Linie das Strafgesetzbuch in Art. 321bis, sind aber auch in einer Reihe von Spezialgesetzen (z.B. im Gesundheitsgesetz vom 19. Dezember 2018 [BGS 811.11] oder in der Notariatsverordnung vom 21. August 1959 [BGS 129.11]) enthalten. Schliesslich bestehen auch weitere Geheimhaltungspflichten,

etwa das Verbot des politischen Nachrichtendienstes nach Art. 272 StGB. Die im Einzelfall anwendbaren Geheimhaltungspflichten müssen dem Dritten durch Gesetz oder schriftliche Vereinbarung überbunden werden. Der beauftragte Dritte muss durch Gesetz oder schriftliche Vereinbarung ebenfalls dazu angehalten werden, seine Mitarbeitenden und Hilfspersonen gleichermassen zur Geheimhaltung zu verpflichten. Als Hilfsperson gilt dabei jede Person, die durch den Dritten als Erfüllungsgehilfe beigezogen wird. Die Definition ist angelehnt an die bundesrechtliche Bestimmung von Art. 101 OR. Seit dem 1. Januar 2023 sind neu auch Hilfspersonen vom Straftatbestand der Amtsgeheimnisverletzung erfasst (Art. 320 StGB).

§ 4 Abs. 1 Bst. c
Angemessene technische und organisatorische Massnahmen sollen die Datensicherheit gewährleisten. Die Bestimmung ist angelehnt an § 16 Abs. 1 Bst. c InfoDG. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte hat im August 2015 einen Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes herausgegeben[1]. Gemäss diesem Leitfaden lassen sich die Gefahren, welche mit Informationssystemen verbunden sind, mit technischen und organisatorischen Massnahmen verringern. Technische Massnahmen hängen dabei direkt mit dem Informationssystem zusammen. Organisatorische Massnahmen hingegen betreffen das Umfeld des Systems, insbesondere die Personen, die es nutzen.[2]

Für die erforderlichen Massnahmen sind die nachstehenden Schwerpunkte zu setzen:

- Zugang zu den Daten (insbesondere Sicherung der Arbeitsplätze und Sicherheit der Serverräume);
- Identifizierung und Authentifizierung von Nutzerinnen und Nutzern;
- Lebenszyklus von Daten;
- Pseudonymisierung und Anonymisierung von Datensätzen;
- Sicherheit von Datenträgern (insbesondere auch für die Datensicherung);
- Austausch von Daten (insbesondere Verschlüsselung und Schlüsselmanagement);
- Auskunftsrechte.

§ 4 Abs. 1 Bst. c steht in einem engen Verhältnis zu § 6. Beide Bestimmungen knüpfen an die gleichen Datensicherheitsmassnahmen an, wobei § 6 diese Massnahmen im weiteren Kontext des Risikomanagements abbildet (vgl. Erläuterungen zu § 6).

§ 4 Abs. 1 Bst. d
Um sicherzustellen, dass die Voraussetzungen gemäss diesem Absatz nicht durch die Beauftragung einer Subunternehmerin umgangen werden können, hat sich der Dritte zu verpflichten, seinerseits nur andere Dritte zu beauftragen, wenn die zuständige Behörde vorgängig schriftlich zugestimmt hat. Die zuständige Behörde kann den Beizug von Subunternehmerinnen auch allgemein ausschliessen oder im Einzelfall ablehnen. Der Nachweis einer schriftlichen Genehmigung obliegt dabei dem Dritten. Die Transparenz über (neue) Subunternehmerinnen ist wichtig, damit die Behörden die (zusätzlichen) Risiken beurteilen und allenfalls minimierende rechtliche, technische oder organisatorische Massnahmen ergreifen können.

§ 4 Abs. 1 Bst. e
Diese Bestimmung verlangt, dass der Dritte durch Gesetz oder schriftliche Vereinbarung haftbar

[1] Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, August 2015.
[2] Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, a.a.O., S. 5 ff..

gemacht wird für die sorgfältige Auswahl, Instruktion und Überwachung seiner Mitarbeitenden und Hilfspersonen. Der notwendige Sorgfaltsmassstab orientiert sich an Art. 398 OR. Für die Definition von Hilfspersonen wird auf die obenstehenden Ausführungen zu Bst. b verwiesen.

§ 4 Abs. 1 Bst. f
Die Archivgesetzgebung verlangt insbesondere, dass archivwürdige Unterlagen aufzubewahren und dem Staatsarchiv zur Langzeitarchivierung abzuliefern sind. Damit die auslagernde Behörde das kann, sind ihr im Fall der Auslagerung vom beauftragten Dritten archivwürdige Unterlagen in langzeitarchivfähigen Dateiformaten zur Verfügung zu stellen.

Dass die entsprechenden Bestimmungen der kantonalen Archivgesetzgebung eingehalten werden, ist deshalb durch entsprechende Vereinbarung oder Gesetz sicherzustellen.

§ 4 Abs. 1 Bst. g
§ 4 Abs. 1 regelt in den Buchstaben a – f verschiedene Voraussetzungen, die in Bezug auf den Dritten, seine Organisation sowie seine technische Infrastruktur erfüllt sein müssen, damit eine Auslagerung von Informatikdienstleistungen überhaupt zulässig ist. Diese Voraussetzungen können ihre Wirkung jedoch nur entfalten, wenn die zuständige und die auslagernde Behörde sowie die zuständigen Aufsichtsbehörden über ausreichende Kontroll- und Weisungsrechte gegenüber den beauftragten Dritten verfügen, um die Voraussetzungen gemäss § 4 Abs. 1 Bst. a – f überhaupt überprüfen und durchsetzen zu können. Als zuständige Aufsichtsbehörden sind in erster Linie die Finanzkontrolle sowie die Beauftragte für Information und Datenschutz gemeint. Darüber hinaus sind aber auch sämtliche anderen zuständigen Aufsichtsorgane (z.B. die Geschäftsprüfungskommission) erfasst. Die Kontroll- und Weisungsrechte sind angemessen sicherzustellen, d.h. entweder mittels Erlass oder vertraglicher Verpflichtung. Das Kontrollrecht umfasst insbesondere, das Recht auf Einsicht und Prüfung der mit der erbrachten Informatikdienstleistung zusammenhängenden Datenbearbeitungen, Unterlagen und Prozesse. Die Behörden können bei den beauftragten Dritten Audits selbständig durchführen oder durch eine andere geeignete Stelle vornehmen lassen. Zu diesem Zweck haben die beauftragten Dritten den Behörden und ihren Vertretungspersonen den erforderlichen Zugang zu ihren Räumlichkeiten, Systemen und Informationen zu gewähren und sie angemessen zu unterstützen.

§ 4 Abs. 2
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. Es können wesentliche Beeinträchtigungen vorliegen, wenn Informatikdienstleistungen dann nicht verfügbar sind, wenn sie gebraucht werden. Für diesen Fall hat die auslagernde Behörde geeignete Massnahmen vorzukehren und unter anderem eine sogenannte Exitstrategie zu entwickeln. 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. Im Rahmen dieser Exitstrategie ist insbesondere die Rückübertragung der ausgelagerten Informatikdienstleistungen aufzuzeigen. Diese Exitstrategie ist periodisch auf ihre Wirksamkeit zu überprüfen und gegebenenfalls an geänderte Verhältnisse anzupassen.

§ 5
Die zuständige Behörde prüft, ob die Voraussetzungen gemäss § 4 Abs. 1 mittels Gesetz oder schriftlicher Vereinbarung sichergestellt sind und beschliesst schliesslich die Auslagerung der Informatikdienstleistungen.

Nur bei bedeutsamen, umfangreichen oder risikobehafteten Auslagerungen soll der Regierungsrat, resp. die Gerichtsverwaltungskommission für den Auslagerungsentschied zuständig sein. Ist also die Auslagerung von übergeordnetem oder strategischem Interesse (bedeutsam), soll sie für

eine oder mehrere Organisationseinheiten zwingend vorgeschrieben werden (umfangreich) oder stellt die Auslagerung ein hohes Risiko für die Grundrechte der betroffenen Personen dar, wie dies bei einer umfangreichen Bearbeitung besonders schützenswerter Personendaten der Fall ist (risikobehaftet), so beschliesst der Regierungsrat für die kantonale Verwaltung, respektive die Gerichtsverwaltungskommission für die Gerichte (§ 5 Abs. 2) die Auslagerung. Dies ergibt sich aus der Verantwortung des Regierungsrates, beziehungsweise der Gerichtsverwaltungskommission, für eine qualitativ gute, wirkungsvolle und zuverlässige Verwaltungstätigkeit zu sorgen (§ 25 des Gesetzes über die wirkungsorientierte Verwaltungsführung vom 3. September 2003 [WOV-G, BGS 115.1]; § 12 Abs. 1 des Gesetzes über die Organisation des Regierungsrates und der Verwaltung vom 7. Februar 1999 [RVOG, BGS 122.111] und § 60^{quater} Abs. 1 des Gesetzes über die Gerichtsorganisation vom 13. März 1977 [GO, BGS 125.12]).

Die Voraussetzungen gemäss § 5 Abs. 1 Bst. a - c verstehen sich alternativ.

§ 5 Abs. 1 Bst. a
Die Begriffe «übergeordnete» und «strategische» Interessen sind unbestimmte Rechtsbegriffe. Mit der Bestimmung soll zum Ausdruck gebracht werden, dass die Bedeutung der geplanten Auslagerung für die Frage der Zuständigkeit entscheidend ist. Ein übergeordnetes oder strategisches Interesse liegt beispielsweise dann vor, wenn die Auslagerung erhebliche personelle oder finanzielle Konsequenzen verursacht, auf einen längeren Zeitraum ausgerichtet ist oder einen Paradigmenwechsel darstellt (z.B. Anwendungen von Microsoft 365 oder SAP für die ganze Verwaltung).

§ 5 Abs. 1 Bst. b
Es soll ermöglicht werden, eine Auslagerung für eine oder mehrere Organisationseinheiten, z.B. für mehrere Ämter, zwingend vorzuschreiben. Damit wird erneut deutlich, dass die auslagernde Behörde und die zuständige Behörde nicht immer identisch sein müssen.

Eine solche Auslagerung kann aufgrund ihrer Tragweite nur durch die oberste Führungsebene beschlossen werden. Dies ist für die Verwaltung der Regierungsrat und für die Gerichte die Gerichtsverwaltungskommission.

§ 5 Abs. 1 Bst. c
Die besondere Bedeutung der Auslagerung nach § 5 Abs. 1 Bst. c knüpft an die Schwere des einhergehenden Grundrechtseingriffs an. Es wird darauf abgestellt, ob die Auslagerung ein hohes Risiko für die Grundrechte der betroffenen Personen darstellt. Im Vordergrund steht das Grundrecht der informationellen Selbstbestimmung (Art. 13 Abs. 2 BV; Art. 8 Abs. 2 KV; vgl. Erwägungen in Ziffer 3.2). Das hohe Risiko kann sich aus der Art, dem Umfang, den Umständen und dem Zweck der Auslagerung ergeben. Als Legalbeispiel für das Vorliegen eines hohen Risikos wird im Gesetz ausdrücklich die Konstellation genannt, in der die Auslagerung eine umfangreiche Bearbeitung von besonders schützenswerten Personendaten beinhaltet. Der Begriff der besonders schützenswerten Personendaten richtet sich nach dem kantonalen Informations- und Datenschutzgesetz. Ein hohes Risiko kann je nach konkreter Ausgestaltung der Auslagerung aber auch schon bei einer weniger umfangreichen Auslagerung von besonders schützenswerten Personendaten vorliegen.

Ein hohes Risiko wird regelmässig dann gegeben sein, wenn die Auslagerung eine grosse Anzahl Datenkategorien umfasst oder aber eine grosse Anzahl Personen davon betroffen ist. Auch die Natur bzw. Sensibilität der Informatikdienstleistungen, die ausgelagert werden sollen, ist für die Risikobewertung ausschlaggebend. Ferner ist der durch die Auslagerung verursachte rechtliche und faktische Kontrollverlust seitens der auslagernden Behörde zu berücksichtigen (vgl. Erwägungen in Ziffer 5.1). Das Ausmass dieses Kontrollverlustes hängt unter anderem von der Ausgestaltung des Vertragsverhältnisses mit dem Auftragnehmer ab. Relevant sind insbesondere die vereinbarten und umgesetzten technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit. Ein erhöhtes Risiko ist indiziert, wenn der Auftragnehmer seinen Sitz

im Ausland hat, bzw. die übertragenen Daten im Ausland bearbeitet werden, insbesondere wenn eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet (vgl. § 21bis InfoDG). Das gleiche gilt, wenn ausländisches Recht oder ein ausländischer Gerichtsstand auf das Vertragsverhältnis zur Anwendung gelangen, da dies mitunter die Rechtsdurchsetzung erheblich erschweren kann.

Zu betonen bleibt, dass § 5 Abs. 1 Bst. c lediglich die Zuständigkeit mit Blick auf die Auslagerung von Informatikdienstleistungen, die ein hohes Risiko für die Grundrechte mit sich bringen, regelt. Die Rechtmässigkeit und insbesondere die Verhältnismässigkeit von solchen Auslagerungen muss weiterhin im Einzelfall geprüft und stets gewährleitstet werden. Sofern die Risiken für die Grundrechte als zu hoch erscheinen und nicht durch angemessene Massnahmen gemindert werden können, hat die Auslagerung grundsätzlich zu unterbleiben.

§ 5 Abs. 2
Die Gerichte sind Teil der kantonalen Verwaltung. Im Hinblick auf die institutionelle Unabhängigkeit der Gerichte entscheidet die Gerichtsverwaltungskommission über die Auslagerung, soweit es sich bei der auslagernden Behörde um ein Gericht handelt und die Auslagerung entweder

- von übergeordnetem oder strategischem Interesse ist,
- für eine oder mehrere Organisationseinheiten zwingend vorgeschrieben werden soll oder
- ein hohes Risiko für die Grundrechte der betroffenen Personen mit sich bringt.

§ 5 Abs. 3
Wenn kein Fall von § 5 Abs. 1 oder 2 vorliegt, obliegt der Entscheid über die Auslagerung von Informatikdienstleistungen der auslagernden Behörde selbst.

§ 6
Mit der Auslagerung von Informatikdienstleistungen gehen verschiedene Risiken einher (vgl. Erwägungen in Ziffer 5.1). Daher ist ein wirksames Risikomanagement eine unabdingbare Voraussetzung für den rechtmässigen, zweckmässigen und wirtschaftlichen Bezug von Informatikdienstleistungen durch Auslagerung. Deshalb werden die zuständigen Behörden aufgefordert, sowohl in ihrem eigenen Zuständigkeitsbereich als auch im Rahmen der Zusammenarbeit mit Dritten, die Risiken der Auslagerungen angemessen zu minimieren.

§ 6 Abs. 1
Absatz 1 stellt klar, dass Risikomanagement ein dauernder Prozess ist. Die Risikobeurteilung hat zu Projektbeginn zu erfolgen, muss aber periodisch überprüft werden. Die sich aus der Auslagerung ergebenden Risiken können nämlich aufgrund veränderter Umstände ebenfalls variieren. Nehmen die Risiken zu, muss diesen mit risikominimierenden Massnahmen begegnet werden. Bei einem erheblichen Risikozuwachs und mangels tauglicher Massnahmen, muss die fragliche Auslagerung gegebenenfalls nachträglich eingestellt werden.

§ 6 Abs. 2
Anhand der initialen und der laufenden Beurteilung der Risiken i.S.v. Abs. 1 obliegt es der zuständigen Behörde, die erkannten Risiken durch Massnahmen angemessen zu minimieren. Bei der Wahl von geeigneten Massnahmen steht der entscheidenden Behörde dabei ein Ermessensspielraum zu, welcher alle geeigneten technischen, organisatorischen und regulatorischen Massnahmen umfasst, die wirtschaftlich tragbar sind. Es handelt sich um die gleichen Massnahmen, auf die in § 4 Abs. 1 Bst. c Bezug genommen wird.

§ 6 Abs. 3
Ziel des Risikomanagements ist es, die geeigneten Massnahmen zur Risikovermeidung oder -reduktion zu treffen. Risiken können vermieden werden, indem auf eine bestimmte, zu riskante Tätigkeit ganz verzichtet wird (z. B. wird auf eine Auslagerung von einer Informatikdienstleistung verzichtet, bei welcher die Umsetzung von risikogerechten Massnahmen wirtschaftlich nicht vertretbar ist). Risiken können aber – im Rahmen der verfassungsrechtlichen und gesetzlichen Schranken – auch in Kauf genommen oder getragen werden. Sie dürfen aber nicht ignoriert werden. Risiken, die nach der Umsetzung der vorgesehenen Sicherheitsmassnahmen bestehen bleiben (sogenannte Restrisiken), oder Risiken, die nicht vermindert werden können, sind klar auszuweisen. Die Entscheidungsträger sind für ihre diesbezügliche Güterabwägung in dokumentierter Form auf diese Restrisiken und die potenziellen Auswirkungen hinzuweisen. Die verbleibenden Restrisiken müssen durch die zuständigen Behörden nachweisbar akzeptiert und entsprechend getragen werden.

§ 7
Diese Bestimmung regelt die Verantwortlichkeiten bei einer Auslagerung von Informatikdienstleistungen. Haftung und Regress bestimmen sich 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).

§ 7 Abs. 1
Dieser Absatz stellt klar, dass auch bei der Auslagerung von Informatikdienstleistungen die auslagernde Behörde für ihre Aufgabenerfüllung verantwortlich bleibt. Dieser Grundsatz ist allgemein anerkannt und bleibt vom vorliegenden Gesetz unberührt.

§ 7 Abs. 2
Die Verantwortung für die sich aus der Auslagerung ergebenden Risiken hat diejenige Behörde zu tragen, welche für den Entscheid über die Auslagerung gemäss § 5 zuständig ist. Bei Auslagerungen nach § 5 Abs. 1 und 2 ist dies der Regierungsrat bzw. die Gerichtsverwaltungskommission, in den übrigen Fällen die auslagernde Behörde. Wird der Dritte, an den Informatikdienstleistungen ausgelagert werden, vertragsbrüchig, indem er z.B. vereinbarte Sicherheitsvorkehrungen unterlässt, ausgelagerte Daten für eigene Zwecke nutzt oder den Betrieb einstellt oder kommt es aufgrund der Auslagerung zu einem Datenzugriff durch eine ausländische Behörde, trägt die nach § 5 zuständige Behörde die Verantwortung für die sich daraus ergebenden Konsequenzen. Für Umstände, welche die Aufgabenerfüllung unabhängig von der Auslagerung betreffen, bleibt in jedem Fall die auslagernde Behörde gemäss § 7 Abs. 1 i.V.m. § 3 Abs. 1 Bst. d verantwortlich (vgl. Erwägungen in Ziffer 6).

§ 8
Werden bei der Auslagerung von Informatikdienstleistungen Personendaten bearbeitet, bleibt die kantonale Datenschutzgesetzgebung massgebend. Für die Auslagerung von Personendaten sind also neben den Voraussetzungen im Sinne von § 4 auch die Voraussetzungen der Datenschutzgesetzgebung einzuhalten. Die kantonale Datenschutzgesetzgebung umfasst das Informations- und Datenschutzgesetz, die Informations- und Datenschutzverordnung vom 10. Dezember 2001 (InfoDV, BGS 114.2) sowie weitere spezialgesetzliche Bestimmungen (z.B. im Steuergesetz oder im Gesundheitsgesetz).

Ebenfalls bleiben die finanz- und submissionsrechtlichen Bestimmungen sowie die Bestimmungen der kantonalen Archivgesetzgebung von diesem Erlass unberührt.

§ 9
Bereits heute werden gewisse Informatikdienstleistungen der kantonalen Verwaltung ausgelagert. Die zum Zeitpunkt des Inkrafttretens dieses Gesetzes bestehenden Verträge, welche die Auslagerung von Informatikdienstleistungen zum Gegenstand haben, sind innert 5 Jahren ab

Inkrafttreten dieses Erlasses auf ihre Übereinstimmung mit dem Auslagerungsgesetz zu überprüfen und wenn nötig anzupassen oder, falls dies nicht möglich ist, aufzukündigen.

11. Rechtliches

Beschliesst der Kantonsrat den vorliegenden Erlass mit weniger als zwei Drittel der anwesenden Mitglieder, unterliegt dieser dem obligatorischen Referendum, andernfalls dem fakultativen Referendum (Art. 35 Abs. 1 Bst. d und Art. 36 Abs. 1 Bst. b KV).

Das Gesetz tritt auf einen vom Regierungsrat festzusetzenden Zeitpunkt in Kraft.

12. Antrag

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

Im Namen des Regierungsrates

Peter Hodel	Andreas Eng
Landammann	Staatsschreiber

Verteiler KRB

Finanzdepartement
Departemente (5)
Staatskanzlei (2; Rechtsdienst)
Amtsblatt (Referendum)
Parlamentsdienste
GS, BGS