BASEL LANDSCHAFT
REGIERUNGSRAT

Vorlage an den Landrat

Beantwortung der Interpellation 2025/575 von Fredy Dinkel: «Sicherheit digitaler Daten»
2025/575

vom 24. März 2026

1. Text der Interpellation

Am 10. Dezember 2025 reichte Fredy Dinkel die Interpellation 2025/575 «Sicherheit der digitalen Daten» ein. Sie hat folgenden Wortlaut:

Im Jahresbericht 2024 steht auf Seite 26: «Nach sorgfältiger Abwägung von Chancen und Risiken hat der Regierungsrat Ende 2023 der Nutzung von Microsoft Cloud Services für die Verwaltung BL zugestimmt. Vorderhand mit Auflagen betreffend Umfang und Datenklassierung (öffentliche und interne Daten).» Wie auch Nachfragen bei der zentralen Informatik (ZI) ergeben haben, ist sich diese der Risiken durch die Auslagerung von Daten auf Servern von Anbieter in Ländern mit tieferen Sicherheitsstandards bewusst. Im Besonderen ist die Nutzung bis auf weiteres auf Daten der Informationssicherheitsklassen „öffentlich und „intern" beschränkt. Die Nutzung für Daten der Klassen „vertraulich" oder „streng vertraulich" ist nur auf Grundlage weiterer Schutzmassnahmen, Restrisikoeinschätzungen und Beschluss des Regierungsrats zulässig. Auch der Bund hat die zugenommene Unsicherheit bezüglich der Entwicklung der geopolitischen Sicherheitslage erkannt und arbeitet am Aufbau einer Swiss-Governance Cloud (SGC). Dieser Aufbau soll zwischen 2025 und 2032 stattfinden und auch den Kantonen zur Nutzung angeboten werden. Obwohl es zu bestimmten Lösungssegmenten alternative Technologieanbieter und Dienstleister gibt, ist gemäss Aussagen der ZI eine kurz- und mittelfristige Umstellung auf schweizerische oder europäische Anbieter nicht möglich, da die entsprechenden Kapazitäten fehlen.

Vor diesem Hintergrund stellen sich verschiedene Fragen und ich bitte den Regierungsrat diese zu beantworten:

1. *Die Verwendung von Cloudlösungen haben viele Vorteile, sind aber auch mit Risiken verbunden, somit stellen sich folgende Fragen:*
   a Was wird für die Sensibilisierung der Mitarbeitenden unternommen?
   b. Finden regelmässige Schulungen, z.B. Online-Kurse, statt?
   c. Welche Mitarbeitenden müssen an solchen Schulungen teilnehmen?

2. *Die Klassierung der Daten ist mit Bewusstsein und entsprechendem Aufwand verbunden. Zudem gibt es einen Ermessensspielraum zwischen internen, vertraulichen und streng vertraulichen Daten.*
   a. Sind die verantwortlichen Mitarbeitenden entsprechend ausgebildet?
   b. Haben sie das dafür notwendige Zeitbudget?
   c. Gibt es dazu eine QS oder Kontrollen?

d. Wie hoch sind die Risiken bei einer falschen Klassierung?

3. *Jährlichen Kosten der Cloud-Lösungen, inkl. der dazu notwendigen Software as a Service (SaaS) Dienstleitungen. Eine gute Schätzung reicht, es geht mir um die Grössenordnung.*
   a. Total der Kosten
   b. Welcher Anteil der Kosten wird direkt von der ZI erbracht, von Anbietern in der CH, im EU-Raum, in anderen Weltregionen?

4. *Standort der Server*
   a. Werden alle vertraulichen und streng vertraulichen Daten bei der Behörde selbst gespeichert?
   b. Welcher Anteil der internen Daten wird bei externen Anbietern in der CH und ausserhalb der CH gespeichert? Eine Schätzung reicht aus.

2. Einleitende Bemerkungen

Cloud-Dienste sind im privaten Umfeld seit längerer Zeit ein fester Bestandteil des Alltags. Auch Unternehmen und Softwarehersteller bieten ihre Leistungen zunehmend online und als Cloud-Lösungen an. Verschiedene Anbieter verfolgen dabei die Strategie, ihre Produkte künftig ausschliesslich als Cloud-Dienste bereitzustellen. Diese Entwicklung führt dazu, dass sich auch öffentliche Verwaltungen verstärkt mit dem Einsatz von Cloud-Diensten auseinandersetzen und geeignete Rahmenbedingungen für deren sicheren Einsatz schaffen müssen.

Vor der Nutzung einer Cloud-basierten Applikation wird daher jeweils eine Risikoanalyse durchgeführt. Dabei werden verschiedene Aspekte geprüft und bewertet. Zu den relevanten Kriterien gehören unter anderem der Speicherort der Daten, der Ort ihrer Bearbeitung sowie allfällige extraterritorial anwendbare Rechtsordnungen. Dazu zählt beispielsweise der CLOUD Act (Clarifying Lawful Overseas Use of Data Act), ein US-Bundesgesetz aus dem Jahr 2018. Diese Faktoren werden bei der Beurteilung und Auswahl von Cloud-Diensten entsprechend berücksichtigt.

Mitarbeitende erhalten vor ihrem Stellenantritt mit den Vertragsunterlagen relevante Richtlinien und Weisungen zugestellt. Mit dem Eintritt in die öffentliche Verwaltung, besonderen Behörden und Gerichte unterstehen sie der Geheimhaltungspflicht. Zudem werden sie auf die einschlägigen Weisungen und Reglemente hingewiesen, insbesondere auf die Verordnung über die Informatik (Informatikverordnung; SGS 140.51) sowie auf das Benutzungsreglement Informatikmittel; SGS 140.551, welches unterzeichnet an die zuständigen direktionalen Personalstellen retourniert werden muss.

Zu den Fragen der Interpellation betreffend die Sicherheit digitaler Daten besteht keine zentrale Datensammlung. Die Antworten wurden deshalb mittels einer Umfrage bei den betroffenen Fachstellen, den IT-Verantwortlichen sowie den zuständigen Controlling-Instanzen erhoben.

3. Beantwortung der Fragen

1. *Die Verwendung von Cloudlösungen haben viele Vorteile, sind aber auch mit Risiken verbunden, somit stellen sich folgende Fragen:*
   Als Grundsatz ist festzuhalten, dass gemäss § 20 der Verordnung über die Informationssicherheit (VIS; SGS 162.51) alle Mitarbeitenden für die Sicherstellung der Informationssicherheit eigenverantwortlich sind.

   a Was wird für die Sensibilisierung der Mitarbeitenden unternommen?
   Die Sensibilisierung der Mitarbeitenden erfolgt mehrstufig, fachspezifisch in den einzelnen Behörden. Die Direktionen, besonderen Behörden und Gerichte stellen im Rahmen ihrer Fachverantwortung die notwendigen Schulungen zu den jeweiligen direktionsspezifischen IT-Systemen sicher; die Direktionssicherheitsbeauftragten (DIT-SIBE) werden bedarfsorientiert beigezogen.

Organisationsübergreifend werden über die Plattform «SensiBL» regelmässig obligatorische Sensibilisierungsaktionen zu Themen der Informationssicherheit und Risiken – insbesondere im Zusammenhang mit digitalen Anwendungen – durchgeführt. Eine obligatorische Initialschulung für neue Mitarbeitende und Externe wird ebenfalls nach dem Eintritt angestossen. Die Inhalte und Schwerpunkte der Sensibilisierungsmassnahmen werden risikobasiert durch die Fachgruppe Informationssicherheit (FIS) koordiniert.

b Finden regelmässige Schulungen, z.B. Online-Kurse, statt?
Regelmässige Schulungen finden statt. Bereits vor der Einführung neuer IT-Systeme werden Sicherheits-, Schulungs- und Supportkonzepte festgelegt sowie entsprechende Dokumentations- und Schulungsunterlagen erstellt, die den Mitarbeitenden anschliessend auch online dauerhaft zur Verfügung stehen. Die Durchführung der anwendungsspezifischen Schulungen liegt bei den zuständigen Dienststellen und Ämtern der Direktionen, der besonderen Behörden und der Gerichte; bei Bedarf werden zusätzliche themenspezifische Schulungen unter Einbezug der Direktionalen Informationstechnologie-Sicherheitsverantwortlichen (DIT-SIBE) und/oder des Kantonalen Informationstechnologie-Sicherheitsverantwortlichen (KIT-SIBE) organisiert. Offene Fragen können jederzeit über den Helpdesk an die zuständigen Stellen gerichtet werden.

c Welche Mitarbeitenden müssen an solchen Schulungen teilnehmen?
Grundsätzlich werden alle Mitarbeitenden entsprechend ihrer Tätigkeit in der Nutzung der von ihnen benötigten IT-Systeme und Fachanwendungen geschult. Die Verantwortung für diese anwendungsspezifischen Schulungen liegt bei den jeweiligen Dienststellen und Ämtern der Direktionen, der besonderen Behörden und der Gerichte.

Die organisationsübergreifenden Sensibilisierungsmassnahmen zur Informationssicherheit «SensiBL» sind für alle Anwender von IT-Systeme der kantonalen Verwaltung, der besonderen Behörden und der Gerichte – einschliesslich externer Mitarbeitenden – obligatorisch. Die Koordination erfolgt durch die kantonale FIS. Die Vorgesetzten stellen die Teilnahme sicher. Die Ergebnisse werden anonymisiert ausgewertet und den zuständigen Stellen zur Kenntnis gebracht. Eine Auswertung auf Ebene einzelner Personen erfolgt nicht.

2. *Die Klassierung der Daten ist mit Bewusstsein und entsprechendem Aufwand verbunden. Zudem gibt es einen Ermessensspielraum zwischen internen, vertraulichen und streng vertraulichen Daten.*
a Sind die verantwortlichen Mitarbeitenden entsprechend ausgebildet?
Eine verwaltungsübergreifende Grundsensibilisierung in der Thematik «Klassifizierung» wird in einer kommenden SensiBL-Schulung aufgenommen. Die generelle Zuständigkeit für die Klassierung von Dokumenten liegt bei den Dossiers führenden Stellen der einzelnen Dienststellen, Behörden und Ämtern gemäss § 7 der Verordnung über die Aktenführung und die Geschäftsverwaltung (GEVER-Verordnung, SGS 140.13). Gemäss § 6 und § 8 Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG, SGS 162) obliegt es diesen Instanzen, angemessene Massnahmen zur Sicherstellung des Informationsschutz sicherzustellen. Diese Massnahmen können sich fallweise und in Abhängigkeit der bearbeiteten Dokumenten-/Datensammlungen stark unterscheiden. Sinnvoll ist die Bereitstellung von generellen verwaltungsübergreifenden Vorgaben und Hilfsmitteln – wie zum Beispiel grundsätzliche Klassierungsstrukturen zu Ordnungssystemen.

Ein typisches Vorgehen kann aufgrund der Einführung der GEVER-Fachapplikation «Fabasoft» aufgezeigt werden. Im Rahmen des Rollouts werden nach dem «Train-the-Trainer»-Konzept zielgerichtete Schulungen direkt in den jeweiligen Dienststellen der Direktionen und besonderen Behörden durchgeführt. Die Fachapplikation bietet umfassende Möglichkeiten zur Datenklassifizierung sowie zur Einrichtung differenzierter Zugriffsrechte. Die

Dienststellen werden dabei vom Kompetenzteam GEVER (KT GEVER) fachlich beraten und unterstützt.

b Haben sie das dafür notwendige Zeitbudget?
Der Ressourcenbedarf, insbesondere hinsichtlich des erforderlichen Zeitbudgets für Aus- und Weiterbildungen in den jeweiligen Aufgaben- und Zuständigkeitsbereichen, ist von den Dienststellen und Ämtern der Direktionen, der besonderen Behörden und der Gerichte zu bestimmen und sicherzustellen. Die Generalsekretärenkonferenz (GSK) hat für den obligatorischen ICT-Schulungsbereich ein jährliches Zeitbudget pro Mitarbeitende definiert, das die Teilnahme an den «SensiBL»-Sicherheitskampagnen gewährleistet.
Bei den jeweiligen Fachapplikationen liegt die diesbezügliche Verantwortung beim Fachapplikationsowner.

c Gibt es dazu eine QS oder Kontrollen?
Gestützt auf § 2 Abs. 4 Verordnung zum Gesetz über die Information und den Datenschutz (Informations- und Datenschutzverordnung, IDV; SGS 162.11) muss dies durch die verantwortlichen Dienststellen und Ämtern der Direktionen, der besonderen Behörden und der Gerichte periodisch vorgenommen und beurteilt werden.

d Wie hoch sind die Risiken bei einer falschen Klassierung?
Abgeleitet von § 8 Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG; SGS 162) und § 2 Abs. 3 Verordnung zum Gesetz über die Information und den Datenschutz (Informations- und Datenschutzverordnung, IDV; SGS 162.11) müssen Dienststellen und Ämtern der Direktionen, der besonderen Behörden und der Gerichte eine entsprechende Schutzbedarfsanalyse zu Daten- und Dokumentenbeständen vornehmen. Fallweise sind unterschiedliche Massnahmen zu treffen. Je nachdem, ob identifizierte Risiken technisch verringert oder durch organisatorische Massnahmen reduziert werden, verändert sich die Wahrscheinlichkeit einer Fehlbeurteilung hinsichtlich des korrekten Ablageorts.

3. *Jährlichen Kosten der Cloud-Lösungen, inklusive der dazu notwendigen Software as a Service (SaaS) Dienstleistungen. Eine gute Schätzung reicht, es geht mir um die Grössenordnung.*
   a. Total der Kosten
   Die in den Direktionen, besonderen Behörden und Gerichte durchgeführte Datenerhebung hat ergeben, dass mindestens 19 Cloud-Anwendungen eingesetzt, und dabei jährliche Kosten in der Höhe von rund 800 000–900 000 Franken anfallen. Die genannten Kosten umfassen sowohl Dienstleistungen als auch die Nutzung der entsprechenden SaaS-Lösungen.

   b. Welcher Anteil der Kosten wird direkt von der ZI erbracht, von Anbietern in der CH, im EU-Raum, in anderen Weltregionen?
   Von den insgesamt rund 810 000 Franken, die die Verwaltung einschliesslich besonderer Behörden und Gerichte für Cloud-Services ausgibt, entfallen rund 370 000 Franken beziehungsweise etwa 46 % auf die ZI. Diese Daten werden nahezu vollständig bei Cloud-Anbietern mit Datenspeicherung in der Schweiz gespeichert.

   Dienststellen und Behörden ausserhalb der ZI weisen insgesamt rund 440 000 Franken an Kosten für in der Cloud gespeicherte Daten aus. Dies entspricht rund 54 % der Gesamtkosten. Etwa 70 % dieser Daten werden bei Cloud-Anbietern mit Standort in der Schweiz gespeichert, der Rest bei deutschen Anbietern.

4. *Standort der Server*
   a. Werden alle vertraulichen und streng vertraulichen Daten bei der Behörde selbst gespeichert?

Die vertraulichen und streng vertraulichen Daten werden grundsätzlich auf der durch die Zentrale Informatik (ZI) bereitgestellten kantonalen Serverinfrastruktur gespeichert. Die meisten Organisationseinheiten verfügen über keine eigene Speicherinfrastruktur.

In einzelnen, fachlich begründeten Ausnahmefällen betreiben spezialisierte Stellen eigene oder angemietete Infrastrukturen bzw. nutzen geprüfte Fachapplikationen externer Anbieter. Diese betreffen klar abgegrenzte Aufgabenbereiche und erfolgen unter Einhaltung der geltenden Informationssicherheits- und Datenschutzvorgaben.

Cloudbasierte Plattformen dienen heute überwiegend der Kommunikation, sowohl im Internet mit der Datenklassifizierung «öffentlich» als auch im Intranet mit den Datenklassifizierungen «intern» und «öffentlich».

b. Welcher Anteil der internen Daten wird bei externen Anbietern in der CH und ausserhalb der CH gespeichert? Eine Schätzung reicht aus.

Die Erhebungen in den Direktionen zeigen ein heterogenes Bild. Insgesamt wird der gross mehrheitliche Teil der kantonalen Daten weiterhin auf kantonaler Infrastruktur gespeichert. Bei einzelnen Aufgabenbereichen – insbesondere im schulischen Umfeld – werden jedoch bereits die Mehrheit der Daten auf Cloud-Diensten gespeichert.

Eine Speicherung ausserhalb der Schweiz erfolgt nur vereinzelt. In diesen Fällen beschränkt sie sich ausschliesslich auf Deutschland und betrifft lediglich einen sehr kleinen Anteil der ausgelagerten Daten.

Liestal, 24. März 2026

Im Namen des Regierungsrats

Der Präsident:

Dr. Anton Lauber

Die Landschreiberin:

Elisabeth Heer Dietrich