Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 14. Januar 2026

41. Bericht der Parlamentarischen Untersuchungskommission Datensicherheit (Stellungnahme)

Der Kantonsrat setzte am 3. Juli 2023 eine Parlamentarische Untersuchungskommission ein (im Folgenden PUK Datensicherheit). Gegenstand der Untersuchung waren die Vorkommnisse rund um den mit der Anfrage KR-Nr. 456/2022 und der dringlichen Interpellation KR-Nr. 462/2022 öffentlich bekannt gewordenen Datensicherheitsvorfall bei der Direktion der Justiz und des Innern und allfälligen weiteren kantonalen Stellen. Der Kantonsrat erteilte der PUK Datensicherheit unter anderem den Auftrag, aufgrund der Untersuchungsergebnisse organisatorische und strukturelle Verbesserungsvorschläge aufzuzeigen, wie solche Vorkommnisse durch die zuständigen Behörden frühzeitig erkannt und verhindert werden können und die Informations- und Datensicherheit des Kantons Zürich bestmöglich gewährleistet werden kann (KR-Nr. 172/2023).

Die PUK Datensicherheit stellte ihren Bericht vom 21. November 2025 am 12. Dezember 2025 der Öffentlichkeit vor.

Da der Bericht der PUK Datensicherheit in erster Linie den Regierungsrat und die kantonale Verwaltung betrifft, nimmt der Regierungsrat dazu gegenüber dem Kantonsrat schriftlich Stellung. Der Regierungspräsident ist zu beauftragen, die Stellungnahme im Rahmen der Beratung des Berichts im Kantonsrat, die derzeit für den 26. Januar 2026 vorgesehen ist, mündlich zu vertreten.

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Schreiben an die Mitglieder des Kantonsrates (Versand per E-Mail am Vortag der mündlichen Stellungnahme des Regierungspräsidenten zum Bericht der PUK Datensicherheit im Kantonsrat):

I. Vorbemerkungen

Der Regierungsrat dankt der PUK Datensicherheit für die eingehende Auseinandersetzung mit den massgeblichen Fragen des Datenschutzes und der Informationssicherheit und die daraus abgeleiteten Handlungsempfehlungen. Der vorgelegte Bericht bildet aus seiner Sicht eine gute Grundlage für die gemeinsame Weiterentwicklung der Informationssicherheit in der kantonalen Verwaltung.

Der Regierungsrat stellt fest, dass sich das zu Beginn der Untersuchung befürchtete Ausmass eines Datenverlusts nicht bestätigt hat. Insbesondere gibt es keine Hinweise dafür, dass Zugriffe auf verschlüsselte Datenträger und damit auf sensitive Daten und Systeme der Zürcher Justizbehörden erfolgten. Die tatsächlich öffentlich gewordenen persönlichen Daten von Mitarbeitenden der Staatsanwaltschaft sind vielmehr über anderweitige öffentlich verfügbare Quellen bekannt geworden.

Der Bericht grenzt die Vorfälle klar ein für die Zeit zwischen 2002 und 2014. Obwohl auch der Kanton Zürich immer wieder Angriffen von Cyberkriminellen ausgesetzt ist, ist es seither soweit ersichtlich zu keinem vergleichbaren Datenvorfall gekommen. Die Datensicherheit in der kantonalen Verwaltung hat sich seit den Vorfällen stark verbessert und ist heute auf einem guten Stand. Entscheidend ist neben den technischen Vorkehrungen auch das Bewusstsein der Mitarbeitenden in der kantonalen Verwaltung für den Umgang mit sensiblen Daten. Naturgemäss kann allerdings trotz grossen Anstrengungen keine hundertprozentige Sicherheit gewährleistet werden. Bei der Erhaltung und Weiterentwicklung der Informationssicherheit handelt es sich um eine Daueraufgabe.

Der Regierungsrat möchte bei dieser Gelegenheit hervorheben, dass ein erheblicher Teil der Empfehlungen der PUK Datensicherheit bereits umgesetzt worden ist oder sich in Umsetzung befindet und dass er gewillt ist, die übrigen Empfehlungen mit dem Kantonsrat und seinen Organen in gegenseitiger Offenheit zu prüfen. Zu diesem Zweck legt der Regierungsrat dem Kantonsrat – soweit in der kurzen Frist möglich – seine eigene Sichtweise und seine Anliegen dar.

Zur Vereinheitlichung der Anwendung der Informations- und Kommunikationstechnologie (IKT) sowie zur Weiterentwicklung der Informationssicherheit in der kantonalen Verwaltung hat der Regierungsrat bereits grosse Anstrengungen unternommen. Insbesondere beschloss er 2017 die Gründung des Amtes für Informatik (AFI; RRB Nr. 267/2017) und die Grundlagen der neuen kantonalen IKT (RRB Nr. 780/2017). Gestützt darauf setzte er 2018 die kantonale IKT-Strategie fest, mit der er das sogenannte Dreischichtenmodell mit der zentralen und standardisierten IKT-Grundversorgung sowie den Kantons- und Fachapplikationen einführte (RRB Nr. 383/2018). Gleichzeitig setzte er die Strategie Digitale Verwaltung 2018–2023 fest (RRB Nr. 390/2018). Auf der Grundlage dieser beiden Beschlüsse entstanden die Gremien «Steuerung Digitale Verwaltung und IKT» (SDI) und «Operative Informatiksteuerung» (OIS). 2019 erliess er die Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019 (IVSV; LS 170.8; RRB Nr. 794/2019) sowie die (erste) Allgemeine Informationssicherheitsrichtlinie (AISR; RRB Nr. 795/2019). Damit wurden unter anderem die oder der IKT-Sicherheitsbeauftragte des Kantons Zürich (ISIK; heute Informationssicherheitsbeauftragter des Kantons Zürich) sowie die Fachgruppe In-

formatiksicherheit (FAGIS; heute Fachgruppe Informationssicherheit) in einem Regelwerk verankert. 2019 setzte der Regierungsrat zudem die Strategie Digitaler Wandel an den Schulen der Sekundarstufe II fest (RRB Nr. 259/2019). 2020 bewilligte er insgesamt 7,0 Stellen für die Informationssicherheitsbeauftragten der Direktionen und der Staatskanzlei (ISID) sowie eine gebundene Ausgabe von Fr. 3 211 200 für die Umsetzung der (die AISR ausführenden) Besonderen Informationssicherheitsrichtlinien (BISR) in den Direktionen und der Staatskanzlei (RRB Nr. 1193/2020). 2022 setzte er die kantonale Cybersicherheitsstrategie fest (RRB Nr. 676/2022). 2023 unterbreitete er dem Kantonsrat die Vorlage für ein neues Gesetz über die Information und den Datenschutz (IDG; RRB Nr. 878/2023; Vorlage 5923), 2024 die Vorlage für ein Gesetz über elektronische Basisdienste (RRB Nr. 963/2024; Vorlage 5985). 2025 folgten die Strategie Digitale Verwaltung 2025+ (RRB Nr. 45/2025) und die (zweite) Allgemeine Informationssicherheitsrichtlinie (AISR; RRB Nr. 438/2025). Für 2026 beabsichtigt der Regierungsrat den Erlass einer Verordnung über die Informations- und Kommunikationstechnologie in der kantonalen Verwaltung (IKTV) samt einer Ergänzung der IVSV im Bereich der Informationssicherheit sowie den Erlass einer Verordnung über das Gremium «Steuerung Digitale Verwaltung und IKT». Neben diesen Massnahmen wurde in der kantonalen Verwaltung der digitale Arbeitsplatz eingeführt. Ausserdem wurden externe Prüfungen der Informationssicherheits-Managementsysteme in den Direktionen und der Staatskanzlei sowie Lieferantenprüfungen durchgeführt. Die heutigen Strukturen und Prozesse im Bereich der kantonalen IKT und der Informationssicherheit unterscheiden sich dadurch grundlegend von denjenigen im Zeitpunkt des untersuchten Datensicherheitsvorfalls.

Vor diesem Hintergrund nimmt der Regierungsrat Stellung zu den Empfehlungen der PUK Datensicherheit. Er orientiert sich dabei am Aufbau von Kapitel 18 des Berichts, in dem die 50 Empfehlungen in acht Themenbereiche gegliedert sind.

II. Stellungnahme zu den Empfehlungen

1. Koordination und Zusammenarbeit innerhalb des Regierungsrates

Der Regierungsrat teilt die Haltung der PUK Datensicherheit, dass ein Silodenken bei der Informationssicherheit nicht zielführend ist, sondern es einer grundsätzlichen Offenheit für direktionsübergreifende Lösungen bedarf. Gleichzeitig ist zu bedenken, dass in der kantonalen Verwaltung eine ausserordentliche Vielzahl von Aufgaben erfüllt wird, die sich grundlegend voneinander unterscheiden – vom Justizvollzug über das Steuerwesen und die Lebensmittelkontrolle bis hin zum Was-

serbau, um nur einige zufällig ausgewählte Beispiele zu nennen. Unterschiedliche Problemstellungen und Risiken erfordern indessen unterschiedliche Lösungen und Massnahmen. Der Regierungsrat strebt deshalb nicht eine Vereinheitlichung um ihrer selbst willen an, sondern ein Vorgehen nach dem Leitsatz «gemeinsam digital unterwegs» (RRB Nr. 1362/2021), bei dem alle Einheiten «am gleichen Strick ziehen», dabei aber jeweils die ihnen eigenen Stärken zur Geltung bringen können.

Zu berücksichtigen ist ferner, dass die tägliche Umsetzung der Rechtsordnung (einschliesslich des von der PUK Datensicherheit angesprochenen IDG) zwangsläufig auf Direktionsebene erfolgen muss.

In diesem Sinne hat der Regierungsrat, wie einleitend ausgeführt, bereits entscheidende Massnahmen für eine gezielte Normierung und Vereinheitlichung getroffen. Diesen Weg wird er auch mit der vorgesehenen IKTV weiterverfolgen. Danach soll beispielsweise das AFI im Bereich der IKT-Grundversorgung Vorgaben für die Direktionen und die Staatskanzlei zur Informationssicherheit, zu den Basiskonfigurationen sowie zur Applikations-, Daten- und Technologiearchitektur erlassen können. Zudem sollen mit einer sogenannten Nebenänderung die AISR, die oder der ISIK sowie die FAGIS in der IVSV verankert werden.

Diese Bestrebungen sind eingebettet in das von der Sicherheitsdirektion im Auftrag des Regierungsrates geführte Integrale Risikomanagement (vgl. dazu § 14 Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung vom 18. Juli 2007 [VOG RR; LS 172.11] und RRB Nr. 878/2023). Nach der neuen AISR (Ziff. 8) haben die Direktionen und die Staatskanzlei zu gewährleisten, dass ihr jeweiliges Risikomanagementsystem Informationssicherheitsrisiken in angemessener Weise berücksichtigt. Bei der Erarbeitung und dem Erlass von Anforderungen an Informationssicherheitsrisiken müssen die oder der ISIK sowie das SDI sicherstellen, dass dies unter Berücksichtigung des Integralen Risikomanagements erfolgt.

Zum gezielten Einbezug des Regierungsrates in die Steuerung der Informationssicherheit sieht die neue AISR insbesondere jährliche Steuerungsmeetings (Ziff. 6.4) sowie eine jährliche Berichterstattung der oder des ISIK (Ziff. 6.5) vor.

Die Zuordnung des AFI zur Finanzdirektion erachtet der Regierungsrat nach wie vor als sachgerecht, zumal mit der Finanzverwaltung, dem Personalamt und der Kantonalen Drucksachen- und Materialzentrale auch andere Verwaltungseinheiten, die Querschnittdienstleistungen für die kantonale Verwaltung erbringen, der Finanzdirektion zugeordnet sind. Die Zuordnung zu einer anderen Direktion hätte aus seiner Sicht keinen Mehrwert zur Folge, sondern nur einen erheblichen Umsetzungsaufwand. Die Einführung einer gemeinsamen Zuständigkeit für das AFI wäre sodann eine Massnahme, welche die Führungsverantwortung eher schwächen als stärken würde.

Prüfenswert erscheinen dem Regierungsrat hingegen vertiefte Überlegungen dazu, wie die Koordination, die Zusammenarbeit und die Steuerung ganzheitlicher erfolgen könnten.

2. Strategische Grundlagen, strategische Steuerung und Begleitung durch den Regierungsrat

Die PUK Datensicherheit empfiehlt im Bereich der strategischen Steuerung eine «gesamtkantonale Steuerung». Es ist nicht abschliessend klar, was damit gemeint ist bzw. was genau wie gesteuert werden soll. Die Vielzahl und Verschiedenheit der Aufgaben sowie die dezentrale Struktur der kantonalen Verwaltung (vgl. dazu Ziff. 1 vorne) bringen es mit sich, dass nicht alles gesamtkantonal gesteuert werden kann. Dies würde dem Anspruch auf eine wirksame und wirkungsvolle Leistungserbringung nicht gerecht werden oder teilweise sogar entgegenwirken. Der Regierungsrat ist aber klar der Ansicht, dass eine Gesamtsteuerung dort unabdingbar ist, wo sie gesetzlich vorgesehen ist oder sie die Qualität, Effizienz und Effektivität gewährleistet oder steigert.

Das gegenwärtige Strategiegefüge ist organisch gewachsen und setzt sich aus einer Vielzahl von Teilstrategien zusammen. Nach der Absicht des Regierungsrates soll dieses Gefüge in einem nächsten Schritt vereinfacht und harmonisiert werden. Die entsprechenden Arbeiten sind bereits im Gang.

Mit der kantonalen Cybersicherheitsstrategie (RRB Nr. 676/2022) hat der Regierungsrat bereits eine Fachstrategie für den Bereich der Informationssicherheit festgesetzt. Diese Strategie ist derzeit in Überarbeitung und soll als kantonale Informationssicherheitsstrategie neu festgesetzt werden. Dabei sollen auch die Empfehlungen der PUK Datensicherheit berücksichtigt werden.

Mit der neuen, am 1. Januar 2026 in Kraft getretenen AISR hat der Regierungsrat einen Schwerpunkt auf den Informationsaustausch zwischen den Direktionen und der Staatskanzlei und ihren Verwaltungseinheiten sowie dem Regierungsrat und dem Gremium SDI gelegt. Zudem hat er die Rollen der oder des ISIK sowie der ISID gestärkt und formelle Massnahmen wie die bereits erwähnten jährlichen Steuerungsmeetings und Berichte vorgesehen (vgl. dazu Ziff. 1 vorne).

3. Rechtliche Grundlagen

3.1 Regelungen zur Informationssicherheit

Der Regierungsrat beabsichtigt, 2026 eine Verordnung über die Informations- und Kommunikationstechnologie in der kantonalen Verwaltung (IKTV) zu erlassen. Darin sollen unter anderem die Zuständigkeiten für die IKT-Sicherheit geregelt werden. Das AFI soll im Bereich der IKT-Grundversorgung bestimmte Vorgaben für die Direktionen und die Staatskanzlei, unter anderem zur Informationssicherheit, er-

lassen können. Gleichzeitig sollen mit einer Änderung der IVSV Grundlagen auf Verordnungsstufe für die AISR, die oder den ISIK sowie die FAGIS geschaffen werden. Damit wird die Übersichtlichkeit der rechtlichen Grundlagen massgeblich verbessert.

Beim Erlass von Regelungen wird der Regierungsrat stets auf deren Stufengerechtigkeit achten. Dabei wird er Vorgaben für die kantonale Verwaltung – soweit angemessen – auch weiterhin in Weisungen und Richtlinien erlassen, zumal eine Verankerung solcher Vorgaben auf Verordnungs- oder gar Gesetzesstufe oft nichts zu deren Rechtswirkung und Wahrnehmbarkeit beiträgt, sondern eher zu einer Schwerfälligkeit und Starrheit, die gerade im wandelbaren IKT-Bereich nicht von Vorteil ist. Inwieweit eine Regelung zur Kenntnis genommen wird, hängt nicht in erster Linie von der Regelungsstufe ab, sondern von den Kommunikations- und Schulungsmassnahmen.

3.2 Allgemeine Informationssicherheitsrichtlinie (AISR)

Mit der neuen AISR hat der Regierungsrat für die gesamte kantonale Verwaltung einheitliche und verbindliche Mindestanforderungen festgelegt, die eine in sich stimmige Umsetzung des Schutzes von Informationen ermöglichen. Er hat damit auch den Informationsaustausch gestärkt und den Einbezug des Regierungsrates und des Gremiums SDI formalisiert (vgl. Ziff. 1 und 2 vorne). Gleichzeitig hat der Regierungsrat bewusst Raum für ergänzende Regelungen der Direktionen und der Staatskanzlei gelassen, da unterschiedliche Problemstellungen und Risiken unterschiedliche Lösungen und Massnahmen erfordern, gerade in der kantonalen Verwaltung mit ihrer ausgesprochenen Vielfalt an Aufgaben (vgl. Ziff. 1 vorne). Nur so können die einzelnen Einheiten ihre Stärken ausspielen, handlungsfähig bleiben und ihrer gesetzlichen Verantwortung nachkommen. Aus Gründen der Stufengerechtigkeit (vgl. Ziff. 3.1 vorne) hat der Regierungsrat die AISR sodann bewusst als Weisung erlassen, wobei er bestimmte Punkte mit der vorgesehenen IKTV und der damit verbundenen Änderung der IVSV neu auf Verordnungsstufe verankern möchte und offen für weitere Regelungen auf Verordnungsstufe ist, soweit damit ein klarer Mehrwert verbunden ist. Der Regierungsrat ist überzeugt, dass die Informationssicherheit mit diesem differenzierten und flexiblen Ansatz hinsichtlich des Regelungsumfangs und der Regelungsstufe nicht geschwächt, sondern gestärkt wird.

Die oder der ISIK wird weiterhin laufend prüfen, ob und gegebenenfalls inwieweit die AISR angepasst werden sollte, auch vor dem Hintergrund des Berichts der PUK Datensicherheit, und die dafür nötigen Schritte veranlassen.

3.3 Revision des Archivgesetzes

Der Regierungsrat ist der Ansicht, dass die Vorgaben zur Aktenführung, zur Anbietungspflicht sowie zur Vernichtung oder Löschung hinreichend klar aus § 5 IDG und aus der IVSV hervorgehen. Allfällige unbefriedigende Vorkommnisse wären deshalb nicht auf eine unzulängliche Regelung zurückzuführen, sondern auf eine unzulängliche Rechtsanwendung. Jedenfalls geht der Regierungsrat mit der Empfehlung der PUK Datensicherheit einig, dass bei Aktenaufräumaktionen die zuständige Person des Staatsarchivs zu informieren und allenfalls zu beteiligen ist.

3.4 Regelung der Amtsübergaben

Der Regierungsrat wird die Anregung der PUK Datensicherheit, die Amtsübergaben besser zu regeln, prüfen. Die Finanzdirektion wird das Personalamt beauftragen, die Ausarbeitung entsprechender Regelungen für kantonale Angestellte zu prüfen und mit der Staatskanzlei abzustimmen, inwieweit solche Regelungen auch auf Amtsübergaben durch Mitglieder des Regierungsrates angewendet werden können.

4. Sicherheitsorganisation

Der Regierungsrat teilt die Auffassung der PUK Datensicherheit, dass zentrale Vorgaben im Bereich der Informationssicherheit wesentlich sind, wobei allfälligen unterschiedlichen Problemstellungen und Risiken Rechnung zu tragen ist (vgl. Ziff. 1 vorne). Demgemäss hat er mit der AISR selbst solche Vorgaben erlassen. Weiter beabsichtigt er, das AFI in der IKTV zum Erlass von ergänzenden Vorgaben zur Informationssicherheit in der IKT-Grundversorgung zu ermächtigen (vgl. Ziff. 3.1 vorne).

Der Regierungsrat wird darüber hinaus prüfen (sei dies schon im Zuge des Erlasses der IKTV oder mit einer nachfolgenden Verordnungsänderung), ob die oder der ISIK allenfalls organisatorisch an anderer Stelle angegliedert werden sollte und mit einem eigenen Weisungsrecht ausgestattet werden kann. Vor dem Hintergrund, dass die Mitglieder des Regierungsrates vom Volk gewählt und nach dem Direktorialsystem der Kantonsverfassung (vgl. Art. 65 Abs. 3 KV) für ihre Direktion verantwortlich sind, bedarf der Entscheid über die Gewährung und gegebenenfalls Ausgestaltung eines solchen Weisungsrechts indessen einer sorgfältigen Abwägung, bei der auch die Überlegungen der PUK Datensicherheit sowie das Ziel einer Verbesserung der Steuerbarkeit der Informationssicherheit einzubeziehen sind.

Der Regierungsrat geht grundsätzlich einig mit der Empfehlung der PUK Datensicherheit, dass die ISID in der Nähe der Direktionsleitung oder der Generalsekretärinnen oder Generalsekretäre anzusiedeln sind. Sofern Besonderheiten in einer Direktion oder der Staatskanzlei dies

gebieten, sollte aber weiterhin eine Zuordnung zum Bereich Digitalisierung oder IT möglich sein. Der nötige Informationsfluss zu den Direktionsleitungen ist dabei in jedem Fall zu gewährleisten.

5. Koordinierte Weiterentwicklung der Informationssicherheit in den Direktionen und der Staatskanzlei

5.1 Konkretisierung der Besonderen Informationssicherheitsrichtlinien (BISR)

Mit der neuen AISR hat der Regierungsrat die notwendigen Grundlagen geschaffen, um besondere Anforderungen im Bereich der Informationssicherheit gezielt in BISR zu umschreiben und mit Wirkung für die gesamte kantonale Verwaltung umzusetzen. Die AISR stellt die notwendige Koordination unter den Direktionen und der Staatskanzlei dadurch sicher, dass die BISR auf Antrag der FAGIS durch das SDI erlassen werden, wobei in diesen beiden Gremien alle Direktionen und die Staatskanzlei vertreten sind. Es ist geplant, dass die überarbeiteten BISR im Laufe des Jahres 2026 erlassen werden.

In der vorgesehenen IKTV sollen die Direktionen und die Staatskanzlei ausdrücklich zum Bezug der IKT-Grundversorgung vom AFI verpflichtet werden, und das AFI soll zum Erlass von Vorgaben zur Informationssicherheit im Bereich der IKT-Grundversorgung ermächtigt werden. Die IKTV soll auch bestimmte Regelungen zur Datenbearbeitung bei der Erbringung von IKT-Leistungen durch das AFI und andere Verwaltungseinheiten enthalten.

Hinsichtlich der Lieferantenprüfungen hat das Gremium SDI einen Vorstoss zur Ausarbeitung eines Prozesses gutgeheissen und der ISIK einen ersten konzeptionellen Entwurf erstellt. Bei der weiteren Ausarbeitung dieses Prozesses sollen die Empfehlungen der PUK Datensicherheit berücksichtigt werden. Der Prozess soll noch im Jahr 2026 eingeführt werden.

5.2 Entsorgung und Löschung

Der Regierungsrat geht mit der Empfehlung der PUK Datensicherheit einig, dass die Entsorgung und Löschung von Datenträgern nach den gesetzlichen Vorgaben und nach anerkannten Standards zu erfolgen hat. Demgemäss erbringen das AFI und das Immobilienamt schon heute entsprechende Dienstleistungen.

Die Finanzdirektion wird das AFI beauftragen, zu prüfen, ob und gegebenenfalls in welcher Form in der kantonalen Verwaltung ein einheitlicher Entsorgungsprozess eingeführt werden kann und soll. Dabei wird unter anderem der besonderen Stellung und den besonderen Bedürfnissen der Kantonspolizei Rechnung zu tragen sein (vgl. dazu auch Ziff. 6 hinten).

5.3 Lieferantenprüfungen

Hinsichtlich der Lieferantenprüfungen kann auf die Ausführungen zur Konkretisierung der BISR verwiesen werden (vgl. Ziff. 5.1 vorne).

5.4 Schulungen

Der Regierungsrat teilt die Haltung der PUK Datensicherheit, dass Schulungen eine wichtige Voraussetzung für eine hohe Informationssicherheit sind. Demgemäss erbringt das AFI schon heute verschiedene Leistungen im Bereich der Sensibilisierung sowie Angebote in der Form von Grund-, Fach- und Einzelschulungen. Deren Nutzung ist grundsätzlich freiwillig; einzelne Schulungsmassnahmen wie beispielsweise die Phishing-Sensibilisierungs-Plattform «Hoxhunt» sind jedoch standardmässig für alle Mitarbeitenden der kantonalen Verwaltung eingeführt und insofern verbindlich. Die Finanzdirektion wird das Personalamt und das AFI beauftragen, zu prüfen, inwieweit die Schulungen zur Informationssicherheit künftig verpflichtend ausgestaltet werden sollen, wie dies in der kantonalen Verwaltung teilweise schon der Fall ist.

5.5 Umgang mit Informationssicherheitsrisiken der Cloud-Lösungen

Der Regierungsrat nimmt die gegenwärtigen Entwicklungen und die damit verbundenen Risiken bei Cloud-Anwendungen sehr ernst, auch vor dem Hintergrund der politischen Diskussionen um die «digitale Souveränität». Er teilt die Einschätzung, dass diese Risiken laufend sorgfältig zu beurteilen sind und dass eine Ablösung von Cloud-Anwendungen bei Bedarf vertieft zu prüfen ist. Zu diesem Zweck wird zurzeit eine kantonale Cloud-Strategie erarbeitet, die 2026 festgesetzt werden soll. Damit sollen die strategischen Leitplanken für den Cloud-Einsatz weiter präzisiert werden.

Vor diesem Hintergrund bedauert es der Regierungsrat, dass die Kommission für Staat und Gemeinden dem Kantonsrat beantragt hat, auf die Vorlage für ein Gesetz über elektronische Basisdienste (Vorlage 5985) nicht einzutreten, da diese Vorlage in § 17 eine Regelung zur Nutzung von Cloud-Anwendungen bei digitalen Arbeitsplätzen vorsieht.

Zur Umsetzung einer sachgerechten Klassifizierung der Informationen wird der Regierungsrat auch weiterhin die erforderlichen Massnahmen ergreifen, wie er dies schon bisher getan hat, indem er beispielsweise in Beschluss Nr. 542/2022 den Erlass einer «Allgemeinen Nutzungsrichtlinie M365» und in der neuen AISR (Anhang) den Erlass einer BISR für die Informationsklassifikation und -kennzeichnung bestimmte.

Es ist für den Regierungsrat nachvollziehbar, dass die Aufsichtskommissionen des Kantonsrates den Umgang mit Cloud-Lösungen kritisch begleiten und ihre Bedenken und Anliegen dabei frühzeitig einbringen.

6. Informationssicherheit bei von der AISR nicht erfassten kantonalen Stellen

Die Planungen und die Tätigkeiten der Kantonspolizei sind schon nach dem geltenden Recht mit denjenigen des Regierungsrates, der anderen Direktionen und der Staatskanzlei zu koordinieren (vgl. § 41 Abs. 2 lit. c Gesetz über die Organisation des Regierungsrates und der kantonalen Verwaltung vom 6. Juni 2005 [LS 172.1]). Vor diesem Hintergrund hat sich die Sicherheitsdirektion dafür entschieden, bei ihren IT-Projekten das Gremium OIS einzubeziehen. Da sich dies bisher als unproblematisch erwiesen hat und es den Vorgehensspielraum der Kantonspolizei mit ihrer besonderen Stellung und ihren besonderen Bedürfnissen zu wahren gilt, sieht der Regierungsrat keinen Anlass für eine weitergehende Formalisierung. Demgemäss beabsichtigt er auch, die Kantonspolizei vom Geltungsbereich der IKT-Verordnung ausnehmen, wie sie – mit guten Gründen und in bewährter Weise – schon heute vom Geltungsbereich der IKT-Strategie ausgenommen ist.

Vom Geltungsbereich der AISR (gemäss deren Ziff. 2.1) ist die Kantonspolizei sodann – entgegen dem Eindruck, den die Überschrift von Kapitel 18.6 des Berichts erwecken könnte – nicht ausgenommen.

Gegenüber den selbstständigen öffentlich-rechtlichen Anstalten hat der Regierungsrat nach geltendem Recht kein Weisungsrecht im Bereich der Informationssicherheit, auch nicht im Rahmen der Eigentümerstrategien. Sollte der Kantonsrat ein solches Weisungsrecht befürworten, hätte er dafür die gesetzlichen Grundlagen zu schaffen.

7. Kommunikation

7.1 Information des gesamten Regierungsrates

Der Regierungsrat ist der Meinung, dass die Direktionen und die Staatskanzlei ihn über relevante Administrativuntersuchungen in geeigneter Form in Kenntnis zu setzen haben.

7.2 Kommunikation gegenüber den Aufsichtskommissionen

Nach der Wahrnehmung des Regierungsrates erfüllen die Aufsichtskommissionen des Kantonsrates, die oder der Datenschutzbeauftragte sowie die Finanzkontrolle ihre Aufgaben schon heute sehr sorgfältig und gewissenhaft, sodass sie über die wesentlichen Risiken im Bereich der Informationssicherheit und von deren Entwicklung gut informiert sind. Der Regierungsrat ist aber offen dafür, die Kommunikation mit diesen Stellen im Rahmen der bestehenden Berichterstattungs- und Austauschgefässe noch zu vertiefen.

8. Interne und externe Aufsicht und Oberaufsicht

8.1 Eigene Audittätigkeit der Direktionen und der Staatskanzlei

Der Regierungsrat hat in der neuen AISR (Ziff. 6.2) festgelegt, dass die Direktionen und die Staatskanzlei mindestens jährlich anhand eines risikobasierten Ansatzes und gemäss den Vorgaben der ISO/IEC-27001-Klausel 9.2 überprüfen, ob die festgelegten Anforderungen an die Informationssicherheit eingehalten und die Informationssicherheitsmassnahmen angemessen und wirksam umgesetzt wurden. Im Auftrag des SDI überprüft die oder der ISIK sodann jährlich nach einem festgelegten und nachvollziehbaren Verfahren mittels eines risikobasierten Ansatzes die durchgeführten Einhalteprüfungen hinsichtlich der Objektivität bzw. Genauigkeit der Prüfergebnisse.

Die dahingehende Empfehlung der PUK Datensicherheit ist damit aus der Sicht des Regierungsrates erfüllt.

8.2 Stärkung der externen Aufsicht

Es ist ganz im Sinne des Regierungsrates, auf der politischen und auf der fachlichen Ebene starke externe Ansprechstellen für den Austausch über die Weiterentwicklung der Informationssicherheit zu haben.

Der Regierungsrat kann die Empfehlung der PUK, wonach die Aufsichtskommissionen des Kantonsrates die Umsetzung der Informationssicherheit im Rahmen der Oberaufsicht engmaschig verfolgen sollen, nachvollziehen. Dies gilt auch für die Empfehlung zur Stärkung der externen Aufsicht auf der fachlichen Ebene. Er hat deshalb in der neuen AISR (Ziff. 6.3) festgelegt, dass die Umsetzung der Informationssicherheit ab 2027 alle vier Jahre durch eine unabhängige, qualifizierte Zertifizierungsstelle (ISO/IEC 27001) anhand eines risikobasierten Ansatzes auf Angemessenheit und Wirksamkeit geprüft wird. Identifizierte Abweichungen zu Vorgaben sind innert nützlicher Frist zu beheben, und die Behebung ist innert Jahresfrist durch eine Nachprüfung zu bestätigen. Inwiefern darüber hinaus auch die oder der Datenschutzbeauftragte und die Finanzkontrolle eine fachliche Aufsicht im Bereich der Informationssicherheit wahrnehmen sollen, muss der Regierungsrat diesen Stellen überlassen. Die Bedenken der Finanzkontrolle, die Prüfungen im Bereich der Informatik nicht als ihre Kernaufgabe sieht (vgl. Bericht der PUK Datensicherheit, S. 191), sind dabei jedoch ernst zu nehmen. Ausserdem sollte eine Verzettelung der Aufsicht auf verschiedene Stellen vermieden werden, da dies der Sache nicht dienlich wäre.

III. Schlussbemerkungen

Abschliessend möchte der Regierungsrat noch einmal festhalten, dass er bereit ist, die von der PUK Datensicherheit gewonnenen Erkenntnisse zusammen mit dem Kantonsrat und seinen Organen in gegenseitiger Offenheit im Interesse der Sache zu nutzen. Er dankt der PUK Datensicherheit deshalb nochmals für ihre umfangreiche und wertvolle Arbeit.

II. Dieser Beschluss ist bis zum Beginn der Debatte zum Bericht der Parlamentarischen Untersuchungskommission Datensicherheit im Kantonsrat nicht öffentlich.

III. Mitteilung an die Mitglieder des Regierungsrates und die Staatsschreiberin.

Vor dem Regierungsrat
Die Staatsschreiberin:

Kathrin Arioli