4. Einsetzung einer Parlamentarischen Untersuchungskommission, Datensicherheitsvorfall

Antrag der Parlamentarischen Untersuchungskommission Datensicherheit vom 21. November 2025
KR-Nr. 172a/2023

Ratspräsident Beat Habegger: Ich begrüsse zu diesem Geschäft und natürlich auch zu den vorhergehenden Geschäften die Mitglieder des Regierungsrates heute bei uns im Kantonsrat, herzlich willkommen. Wir haben zu diesem Geschäft freie Debatte beschlossen. Ich habe den Ablauf für dieses Geschäft wie folgt vorgesehen: Zuerst spricht der Kommissionspräsident *(Benno Scherrer)* der Parlamentarischen Untersuchungskommission *(PUK)*, dann der Regierungspräsident *(Martin Neukom)*, dann die Fraktionssprechenden und die Ratsmitglieder, und schliesslich gebe ich dem Regierungspräsidenten und den Mitgliedern des Regierungsrates das Wort für eine Replik, bevor der PUK-Präsident die Debatte abschliessen wird. Ich gehe davon aus, dass Sie mit diesem Vorgehen einverstanden sind.

Benno Scherrer (GLP, Uster), Präsident der Parlamentarischen Untersuchungskommission (PUK) Datensicherheit: Es freut mich, Ihnen heute im Namen der PUK Datensicherheit unseren Schlussbericht zu präsentieren und die Auflösung unserer Kommission zu beantragen.
Zu welchem Schluss kommt die PUK? Der Regierungsrat hat die Daten- und Informationssicherheit vernachlässigt. Die Parlamentarische Untersuchungskommission Datensicherheit kritisiert die Organisation der kantonalen Verwaltung bei der Daten- und Informationssicherheit. Sie lässt den Direktionen und der Staatskanzlei in der Umsetzung viel Spielraum. Das Silo-Denken, das den untersuchten Datensicherheitsvorfall in der Direktion der Justiz und des Inneren erst ermöglichte, muss aus Sicht der PUK Datensicherheit endlich überwunden werden.
Wir haben unseren Bericht am 12. Dezember 2025 den Medien und damit der Öffentlichkeit präsentiert, und Sie, liebe Kolleginnen und Kollegen, haben diesen am Montag darauf auf Ihrem Pulten gefunden und hatten nun Zeit, ihn zu lesen und in den Fraktionen zu diskutieren. Und auch der Regierungsrat – der Regierungspräsident wird nach mir sprechen – hat sich mit dem Bericht auseinandergesetzt und wird Stellung dazu beziehen. Ich werde dann in einem zweiten Votum auf das Gesagte eingehen. Ich möchte, nachdem uns die schriftliche Stellungnahme erst gestern Abend um 18 Uhr zugestellt wurde, erst auf die mündlichen Reaktionen oder Ausführungen des Regierungspräsidenten reagieren.
Die PUK Datensicherheit hat ihren Auftrag in der Kantonsratssitzung vom 3. Juli 2023 bekommen. Wir haben als parteiübergreifende Kommission rein der Untersuchung verpflichtet agiert. Als PUK verfügten wir über die Informationen und die Ressourcen, die für unsere Arbeit notwendig waren. Die Arbeit der PUK und die Diskussionen waren intensiv und sehr, sehr sachlich. Wir haben unter höchster Diskretion gearbeitet und unabhängig, das heisst auch ohne Rücksprache mit den

Fraktionen und ohne deren Information getagt. Es gab auch keine Indiskretionen, welche unsere Arbeit behindert hätten. Nach der Wahl der Mitglieder im Herbst 2023 hat die PUK Datensicherheit zuerst die organisatorischen Grundlagen für ihre Arbeit gelegt. Nach einer Informationsbeschaffungsphase haben wir uns den umfangreichen Unterlagen der JI *(Direktion der Justiz und des Innern)*, Regierungsratsbeschlüssen, Strategieprogrammen zur ICT und so weiter befasst. Ebenso standen wir im Austausch mit der Staatsanwaltschaft und konnten für spezifische Fragestellungen Einsicht in die Akten nehmen und diese beiziehen. Die Staatsanwaltschaft hatte den Teilaspekt der Datenentsorgung einer vertieften strafrechtlichen Prüfung unterzogen. Die PUK Datensicherheit anerkennt und verdankt die grossen Anstrengungen, welche die Staatsanwaltschaften unternommen haben, um diese Fragen zu klären. Diese Arbeiten waren eine äusserst wertvolle Grundlage für die Arbeit der PUK Datensicherheit. Dafür danke ich im Namen der Kommission ausdrücklich.
Die Hauptarbeit der PUK lag in der Sachverhaltsermittlungs- und Beweiserhebungsphase, in der wir die meisten Befragungen durchführten. Schliesslich erarbeiteten wir den provisorischen Schlussbericht. Die Personen, die Gegenstand des Verfahrens der PUK bildeten, bekamen darauf Gelegenheit, sich zu den Teilen des Berichtsentwurfs, die sie betreffen, zu äussern. Danach beriet die Kommission die Stellungnahmen und bereinigte den Schlussbericht. Am 21. November 2025 hat die PUK Datensicherheit nach 50 Sitzungen den vorliegenden Bericht einstimmig verabschiedet. Für die professionelle Arbeit und engagierte Zusammenarbeit danke ich allen Kommissionsmitgliedern sehr, sehr herzlich. Ein besonderer Dank geht an unseren Kommissionssekretär, Heiri Gander, und an die Rechtskonsulentin der PUK, Noëlle Glaus, sowie die Protokollführerinnen, insbesondere Franziska Gasser. Diese Mitarbeitenden der Parlamentsdienste waren es, die diese Untersuchung erst möglich gemacht haben.
Die PUK Datensicherheit hat vom Kantonsrat den Auftrag bekommen, die Geschehnisse um den mit einer Anfrage *(KR-Nr. 456/2022)* und einer Interpellation, «Verantwortlichkeiten bei der Justizdirektion verlangen Aufklärung» *(KR-Nr. 462/2022)*, öffentlich bekannt gemachten Datensicherheitsvorfall bei der JI und allfälligen weiteren kantonalen Stellen abzuklären und politisch aufzuarbeiten. Die Arbeit einer PUK soll unter anderem dazu beitragen, das Vertrauen in Regierung und Verwaltung zu erhalten und zu stärken. Mit der sorgfältigen Aufarbeitung und der ausgewogenen Bewertung der Sachverhalte schafft eine Untersuchungskommission Transparenz. Damit dies gelingt, braucht es die Offenheit der Regierung und der Verwaltung, an dieser Arbeit mitzuwirken. Es ist ein besonderes Signal, gerade in einer Zeit, in der es um das Vertrauen in die öffentlichen Institutionen weniger gut bestellt ist, dass die PUK Datensicherheit auf diese Bereitschaft zum konstruktiven Austausch zählen konnte. Ebenso möchte ich jetzt schon die allgemein positive Aufnahme des Berichts durch den Regierungsrat würdigen.
Wir haben uns bei unserer Arbeit eng am Auftrag des Kantonsrates, den die GPK *(Geschäftsprüfungskommission)* vorbereitet hat, orientiert. Wir stellen unsere Erkenntnisse auf den ersten Seiten des umfassenden Berichts zusammen. Auf etwa

200 weiteren Seiten zeigen wir auf, welche rechtlichen und organisatorischen Grundlagen galten und gelten und wie politisch darum gerungen wurde. Wir haben herausgearbeitet, wie der Datensicherheitsvorfall möglich wurde, welche Umstände ihn begünstigt haben und wie die vom Vorfall betroffene Direktion, die JI, und der Regierungsrat, als Gesamtgremium, damit umgingen.
Mit diesem Bericht und den Empfehlungen betont die PUK Datensicherheit die Wichtigkeit von Zusammenarbeit, von direktionsübergreifenden Regelungen, von klaren Standards. Die PUK Datensicherheit attestiert aber auch, dass in den letzten Jahren diesbezüglich weichenstellende Entscheidungen getroffen wurden. Die PUK konnte feststellen, dass die Informationssicherheit der kantonalen Verwaltung durch gesetzliche Grundlagen bereits früh angemessen geregelt war. Der Regierungsrat hat der Informationssicherheit als gesamtkantonaler Gemeinschaftsaufgabe über die Direktionen hinaus über Jahre aber schlicht zu wenig Beachtung geschenkt. Er hat die Thematik Informationssicherheit mit zu wenig Nachdruck vorangetrieben und ungenügend begleitet. Und die Perspektive als Direktionsvorstehende hat gegenüber jener als Regierungsmitglied überwogen. Die Regierungsmitglieder sahen keinen Handlungsbedarf, solange die IT im operativen Tagesgeschäft passabel funktionierte, und hatten meist kein Interesse an einer Zentralisierung der Informatik. Erst mit der IKT-Strategie 2018 hat der Regierungsrat eine wichtige Weichenstellung vorgenommen und mit der Zentralisierung der Grundversorgung den Kanton weitergebracht.
2015 schon hatte der Regierungsrat die Funktion des kantonalen Informationssicherheitsbeauftragten geschaffen. Er erliess 2019 die allgemeine Informationssicherheitsrichtlinie. Die kantonalen Aktivitäten haben sich aber erst ab 2022 durch den Erlass der Informationssicherheitsstrategie, früher Cybersicherheitsstrategie, merklich verstärkt. Das Bewusstsein für die Notwendigkeit einer stärkeren kantonalen Herangehensweise an die Informationssicherheit und einer einheitlichen Umsetzung der Vorgaben fehlte jedoch weiterhin. Ausserdem sind die konkreten Bestimmungen zur Informationssicherheit im Gegensatz zu früher nicht mehr auf Verordnungsstufe geregelt. Der zweistufige Ansatz mit einer gemeinsamen kantonalen Basis und individuellen Umsetzungen lässt den Direktionen und der Staatskanzlei aus Sicht der PUK Datensicherheit weiterhin zu viel Autonomie. Die PUK Datensicherheit attestiert dem Regierungsrat aber, dass er die Entwicklung der neuen IKT-Strategie 2018 eng begleitet hat.
Nun ein paar Ausführungen zum Datensicherheitsvorfall in der JI und später zum Umgang der JI nach dem Bekanntwerden des Vorfalls: Der Zeitraum dieses Vorfalls lässt sich auf die Jahre 2002 bis 2014 eingrenzen. Das sind die Jahre, in denen ein externer Dienstleister, über den Datenträger der JI weggekommen sind, für die JI-Informatik tätig gewesen ist. Die PUK Datensicherheit fand dazu keinen schriftlichen Vertrag, und es fehlt auch an Belegen, dass die korrekte Löschung von Daten schriftlich bestätigt wurde. Es bestehen aber keine Anzeichen, dass im Rahmen einer Aufräumaktion 2019, anders als ursprünglich kolportiert, diesbezüglich relevante Unterlagen abhandengekommen sein sollen. Festgestellt werden muss: Die Aufsicht, die Abläufe, die internen Kontrollen sowie die Dokumenta-

tionen waren in der JI-Informatik in jener Zeit ungenügend. Ein kausales Fehlverhalten des Regierungsrates oder dessen Direktionsvorsteherinnen und Direktionsvorsteher beim eigentlichen Datensicherheitsvorfall in der JI kann die PUK Datensicherheit hingegen nicht feststellen.
Hier im Parlament wurde auch die Information der Direktionsvorsteherin der JI nach dem Bekanntwerden des Datensicherheitsvorfalls kritisch hinterfragt. Als die aktuelle Direktionsvorsteherin *(Regierungsrätin Jacqueline Fehr)* im November 2020 vom Datensicherheitsvorfall erfuhr, hat sie eine Administrativuntersuchung angeordnet und den kantonalen Informationssicherheitsbeauftragten sowie die Datenschutzbeauftragte *(Dominika Blonski)* informiert. Die Kommunikation der JI gegenüber den Behörden war jedoch ungenügend. Die Finanzkontrolle wurde nicht informiert. Die GPK hat zwar im Rahmen eines Referentengesprächs im März 2021 vom Vorfall Kenntnis bekommen. Es reicht aus der Sicht der PUK Datensicherheit aber nicht aus, eine Information dieser Tragweite ausschliesslich in einem solchen Rahmen zu platzieren. Zudem ist die Zustellung des Schlussberichts der Administrativuntersuchung an die GPK ausgeblieben. Regierungsrätin Jacqueline Fehr räumte diese Fehler aber rasch selbst ein. Kritisiert wird von der PUK Datensicherheit die Kommunikation der Direktionsvorsteherin gegenüber dem Regierungsrat. Bei der ersten mündlichen Information an der Regierungsratssitzung vom 18. Dezember 2020 wurde der Vorfall so beiläufig erwähnt, dass sich später kaum jemand daran erinnern konnte. Erst an der Sitzung vom 21. Dezember 2022, nachdem die Öffentlichkeit bereits davon Kenntnis hatte, wurde der Regierungsrat grundlegend informiert. Schliesslich hat die JI mit einem externen Bericht, dem sogenannten KPMG-Bericht *(Wirtschaftsprüfungsunternehmen)*, Transparenz über die Situation im Bereich der Informationssicherheit und des Datenschutzes geschaffen und ihre Bemühungen in diesem Bereich wesentlich intensiviert. Das begrüsst die PUK Datensicherheit. Sie hat aber wenig Verständnis dafür, dass die Regierungsmitglieder sich kaum für Vorgänge in anderen Direktionen interessierten. Sowohl der Schlussbericht der Administrativuntersuchung als auch der KPMG-Bericht beinhalten aus Sicht der PUK Datensicherheit Schlussfolgerungen, die für den gesamten Kanton, alle Direktionen und die Staatskanzlei von Interesse sein müssten.
In Umgang mit diesen Feststellungen zeigt sich für die PUK Datensicherheit die fehlende direktionsübergreifende, die fehlende gesamtkantonale Perspektive. Für die PUK Datensicherheit ist es unerklärlich, dass jede Direktion und die Staatskanzlei für sich ihre eigenen Schlüsse daraus gezogen haben. Hier sieht die PUK Datensicherheit klar den Regierungsrat als Kollegialbehörde in der Pflicht, die Umsetzung der Empfehlungen auf der kantonalen Ebene einheitlich anzugehen.
Die PUK Datensicherheit legt aufgrund ihres Berichts 50 Empfehlungen vor, die drei Bereiche adressieren. Themenkomplex 1, gemeinsame Verantwortung, Koordination und Zusammenarbeit: Die PUK Datensicherheit fordert mit Nachdruck eine intensivere Zusammenarbeit und gemeinsame Verantwortung. Sie fordert eine Anpassung der Verordnung über die Organisation des Regierungsrates. Die Zuständigkeit für die Regeln zur Umsetzung des IDG *(Gesetz über die Information und den Datenschutz)* soll auf der kantonalen Ebene statt in den Direktionen

verortet sein. Die Herausforderungen der Digitalisierung sind gesamtheitlich zu betrachten, die Grundlagen zu vereinheitlichen und gesamtkantonal zu steuern.
Zweitens, kantonal verbindliche Vorgaben und Weisungsrechte: Regelungen zur Informationssicherheit sind auf Verordnungsstufe zu regeln. Gerade die Allgemeine Informationssicherheitsrichtlinie, die AISR, ist als Verordnung zu erlassen. Der kantonale Informationssicherheitsbeauftragte, der ISIK, ist mit einem Weisungsrecht auszustatten und seine Unabhängigkeit ist zu gewährleisten. Und schliesslich: Der Gesamtregierungsrat muss sich gegenseitig und auch die Aufsichtskommissionen informieren.
Die externe Aufsicht über die Informationssicherheit ist wesentlich zu stärken. Dazu nennt die PUK drei Möglichkeiten, die geprüft werden sollen: die Verstärkung der Kontrolle durch die Datenschutzbehörde mit einer neu gestalteten Berichterstattung gegenüber den Aufsichtskommissionen oder die Stärkung der Ressourcen und Möglichkeiten der Finanzkontrolle oder schliesslich mit der Schaffung einer neuen, unabhängigen Instanz der Informationssicherheitskontrolle, welche die externe Aufsicht in diesem Bereich wahrnimmt. Und schliesslich hat der Kantonsrat eine wirksame Oberaufsicht durch seine bisherigen Strukturen oder gegebenenfalls durch eine neu zu schaffende Aufsichtskommission für IT-Projekte und Informationssicherheit sicherzustellen.
Und jetzt bin ich gespannt auf die Ausführungen der Regierung und die Diskussion. Danke.

Regierungspräsident Martin Neukom: Zuerst möchte ich im Namen der Regierung ganz herzlich danken, und zwar der Parlamentarischen Untersuchungskommission Datensicherheit für ihre Arbeit und für ihre Auseinandersetzung mit den massgeblichen Themen im Bereich Datenschutz und Datensicherheit. Speziell danken möchte ich dem Kommissionspräsidenten Benno Scherrer für seine geleistete Arbeit. Der Bericht ist aus unserer Sicht eine sehr gute Grundlage für die gemeinsame Weiterentwicklung der kantonalen Informationssicherheit in der Verwaltung.
Der Regierungsrat stellt fest, dass sich das zu Beginn befürchtete Ausmass eines Datenverlustes nicht bestätigt hat. Es gibt keine Hinweise dafür, dass es Zugriffe auf verschlüsselte Datenträger oder auf sensible Daten der Justizbehörden gab. Die öffentlich gewordenen persönlichen Daten von gewissen Mitarbeitenden der Staatsanwaltschaft sind durch anderweitige, öffentlich verfügbare Quellen bekannt geworden. Der Bericht grenzt die Vorfälle auch klar auf den Zeitraum von 2002 bis 2014 ein.
Erlauben Sie mir zuerst noch eine persönliche Bemerkung zum Thema Datensicherheit und Informationssicherheit: Die Bedrohungslage im Bereich Informationssicherheit hat sich seit den Nullerjahren substanziell geändert. Wir sind heute, unsere Gesellschaft ist deutlich digitaler, auch der Staat ist deutlich digitaler, und daher ist es auch sehr viel wichtiger, dass diese digitale Infrastruktur funktioniert, zuverlässig funktioniert und verlässlich ist. Leider haben sich Cyberkriminelle in den letzten 20 Jahren ebenfalls massiv verbessert und Cyberkriminelle sind heute leider viel professioneller, als sie das vor 20 Jahren waren. Ob sie einen Staat

repräsentieren, eine Gemeinde, eine Firma oder auch Private, alle können Ziel einer entsprechenden Cyberattacke sein. Deshalb hat heute die IT-Sicherheit, die Informationssicherheit einen viel höheren Stellenwert, als sie das vielleicht vor 20 Jahren hatte, nicht nur im Kanton Zürich, sondern international auf der ganzen Welt.
Die IT-Sicherheit im Kanton Zürich hat sich massiv verbessert. Es wurden sehr, sehr grosse Anstrengungen getätigt, um die IT-Sicherheit zu verbessern. Wichtig ist aber auch: Mit den allergrössten Anstrengungen gibt es, wie überall im Leben, keine 100-prozentige Sicherheit. So gibt es auch bei der IT-Sicherheit keine 100-prozentige Sicherheit. Also selbst bei einem professionellen Schutz kann es trotzdem zu erfolgreichen Angriffen kommen. Wie gesagt, die Datensicherheit im Kanton hat sich stark verbessert und der Regierungsrat ist klar der Ansicht, dass wir heute auf einem guten Stand sind. Wie gesagt, trotz den hohen Anstrengungen ist auch hier keine 100-prozentige Sicherheit, aber wir haben einen guten Stand. Wichtig ist auch zu sagen: Es ist nie ein Prozess, der irgendwann abgeschlossen ist, sondern die Weiterentwicklung der Informationssicherheit ist eine Daueraufgabe.
Bevor ich zu den Empfehlungen, zu den einzelnen Empfehlungen der PUK komme, möchte ich einen kurzen Überblick über die strategischen Grundlagen der IT-Sicherheit im Kanton Zürich geben: 2017 wurde das AFI, das Amt für Informatik, gegründet. 2018 wurde die kantonale IKT-Strategie beschlossen. Gleichzeitig wurde die Strategie digitale Verwaltung beschlossen. 2019 wurde die Verordnung über die Informationsverwaltung und -sicherheit entsprechend erlassen, gleichzeitig wurden die AISR beschlossen; AISR, das sind die Allgemeinen Informationssicherheitsrichtlinien. 2020 wurden Stellen für die Informationssicherheit und es wurden Stellen für die Informationssicherheitsbeauftragten in den Direktionen geschaffen. Weiter wurden die sogenannten BISR festgesetzt. BISR, das sind die Besonderen Informationssicherheitsrichtlinien. 2022 wurde dann die kantonale Cybersicherheitsstrategie durch den Regierungsrat beschlossen. Weiter wurden externe Prüfungen der Informationssicherheitsmanagementsysteme durchgeführt und auch die Lieferanten wurden geprüft. Also Sie sehen, die heutigen Strukturen und Prozesse im Bereich der Informationssicherheit unterscheiden sich ganz grundlegend von jenen zum Zeitpunkt des untersuchten Datensicherheitsvorfalls.
Dann kommen wir zu den Empfehlungen der PUK: Die PUK hat 50 Empfehlungen erarbeitet. Wir haben viele von diesen Empfehlungen bereits umgesetzt. Und die restlichen Empfehlungen, die wir noch nicht umgesetzt haben, sind wir gerne bereit, detailliert zu prüfen. Ich gehe jetzt aufgrund der zeitlichen Beschränkungen nicht auf alle 50 Empfehlungen ein, ich habe deshalb vier Themenbereiche herausgepickt, zu denen ich gerne noch detaillierter etwas sage. Das erste ist das Silo-Denken. Die Parlamentarische Untersuchungskommission kritisiert das Silo-Denken in den Direktionen, und wir in der Regierung sind klar der Ansicht: Ja, selbstverständlich, Silo-Denken ist nicht zielführend, die gute Zusammenarbeit zwischen den Regierungsräten und zwischen den Direktionen ist sehr wichtig. Es gilt

allerdings zu bedenken, dass die Direktionen extrem unterschiedliche Tätigkeitsbereiche haben, vom Justizvollzug über das Steuerwesen bis zur Lebensmittelkontrolle. Das sind ganz unterschiedliche Tätigkeiten mit unterschiedlichen Risiken und unterschiedlichen Risikoprofilen, deshalb: Unterschiedliche Risiken bedingen auch unterschiedliche Lösungen, Vereinheitlichung ist also nicht per se eine Patentlösung. Wir müssen dort vereinheitlichen, wo es Sinn ergibt und wo wir die Leistung durch eine Vereinheitlichung besser erfüllen können. Wichtig ist, dass alle am gleichen Strick ziehen. Die Zuordnung des Amtes für Informatik zur Finanzdirektion erachtet der Regierungsrat weiterhin als sachgerecht. Eine gemeinsame Zuständigkeit der gesamten Regierung für das Amt für Informatik würde vermutlich die Führungsverantwortung eher schwächen als stärken.
Zweiter Punkt, die Rechtsgrundlagen: Die PUK fordert stärkere rechtliche Verankerung der Datensicherheit. Das sehen wir ebenfalls als sinnvoll an. Der Regierungsrat plant daher, in diesem Jahr eine neue Verordnung zu erlassen, es ist die IKTV, die Verordnung über die Informations- und Kommunikationstechnologie in der kantonalen Verwaltung. Darin werden auch die Zuständigkeiten für die IKT-Sicherheit geregelt. Bereits umgesetzt sind die neuen AISR, also nochmals: die Allgemeinen Informationssicherheitsrichtlinien, und sie erhalten für die gesamte Verwaltung verbindliche Mindestanforderungen für die Informationssicherheit.
Punkt 3, Sicherheitsorganisation: Die PUK fordert ein Weisungsrecht für den ISIK. Der ISIK, das ist der Informationssicherheitsbeauftragte des Kantons Zürich. Wir werden das prüfen. Es ist allerdings zu klären, wie dann die Verantwortlichkeiten sind. Es stellt sich also die Frage, ob, wenn der ISIK ein Weisungsrecht hätte, die Verantwortung für die IT-Sicherheit dann auch an den ISIK übergeht oder ob es dann eine doppelte Verantwortung gibt. Das wird alles zu klären sein, der Regierungsrat wird dies detailliert prüfen. Weiter fordert die PUK, dass der ISID in der Nähe der Direktionsleitung oder des Generalsekretärs angesiedelt wird. Der ISID ist im Gegensatz zum ISIK – das ist derjenige für den ganzen Kanton – der Informationssicherheitsbeauftragte pro Direktion. Es macht aus unserer Sicht Sinn, den Informationssicherheitsbeauftragten der Direktion nahe am Direktionsvorsteher beziehungsweise an der Direktionsvorsteherin oder nahe am Generalsekretär oder an der Generalsekretärin anzusiedeln. Das heisst, der Regierungsrat geht einig mit dieser Empfehlung.
Punkt 4 sind Schulungen: Die PUK fordert verbindliche Schulungen für die Informationssicherheit, und der Regierungsrat teilt diese Haltung, dass Schulungen bezüglich Informationssicherheit wichtig sind. Einzelne Schulungen in der kantonalen Verwaltung sind bereits verbindlich, beispielsweise die sogenannte Hoxhunt-Plattform. Da erhält man in der Verwaltung regelmässig sogenannte Phishing-E-Mails, also E-Mails, wo man eben nicht draufklicken sollte. Das sind E-Mails mit einem Wettbewerb oder mit einer Aufforderung, man solle ein neues Passwort wählen oder irgendetwas. Da sind die Leute, die solche Phishing-Mails schreiben, sehr kreativ. Und es ist ein Test, man soll eben nicht draufklicken. Wenn man trotzdem draufklickt, dann kommt eine Meldung, die einem erklärt,

warum man hätte erkennen sollen, dass man da eben genau nicht hätte draufklicken sollen; aus meiner Sicht eine sehr sinnvolle Sache, das dient der Sensibilisierung. Solche Phishing-Attacken sind sehr, sehr verbreitet. Der Regierungsrat wird prüfen, inwiefern weitere Schulungen zum Thema Informationssicherheit künftig verpflichtend sein sollen.
Der Regierungsrat hat zum PUK-Bericht und zu den einzelnen Empfehlungen bereits schriftlich Stellung genommen. Dieser Regierungsratsbeschluss *(RRB)* wurde heute Morgen veröffentlicht. Es ist der RRB 41/2026, meine soeben gemachten Ausführungen basieren darauf. Die schriftliche Stellungnahme ist, kann man vermuten, etwas ausführlicher als meine mündlichen Stellungnahmen und enthält die detaillierten Stellungnahmen zu den einzelnen Forderungen der PUK. Aus zeitlichen Gründen habe ich davon jetzt nur vier Punkte erwähnt, Sie können das ja dann gerne noch nachlesen.
Erlauben Sie mir noch eine persönliche Bemerkung zum Schluss: Bitte seien Sie sich bewusst, meine Damen und Herren Kantonsräte, jede Forderung nach IT-Sicherheit hat letztendlich ein Preisschild. Bessere Informationssicherheit, das braucht Zeit innerhalb der Verwaltung und das verursacht auch Kosten. Deshalb ist es auch beim sehr wichtigen Thema Informationssicherheit wie immer, es braucht ein Abwägen: Wie viel Sicherheit wollen wir und zu welchen Kosten? Und bitte halten Sie das bis zum Dezember, bis zur nächsten Budgetdebatte präsent.
Zum Schluss möchte der Regierungsrat abschliessend festhalten, dass er gerne bereit ist, die von der PUK Datensicherheit gewonnenen Erkenntnisse zusammen mit dem Kantonsrat in gegenseitiger Offenheit und im Interesse der Sache zu nutzen. Ich danke der PUK Datensicherheit nochmals für ihre umfangreiche und wertvolle Arbeit. Danke.

Ratspräsident Beat Habegger: Besten Dank dem Regierungspräsidenten und dem PUK-Präsidenten. Wir kommen jetzt zu den Fraktionssprechenden, denen jeweils zehn Minuten Redezeit zur Verfügung steht, anschliessend dann die übrigen Mitglieder des Kantonsrats, die fünf Minuten sprechen dürfen.

Karl Heinz Meyer (SVP, Neerach): Heute beraten wir den PUK-Bericht Datensicherheit. Als Erstes möchte ich mich bei allen PUK-Mitgliedern für die konstruktive Arbeit innerhalb der Kommission bedanken. Wider Erwarten wurde praktisch keine Parteipolitik betrieben. Der Präsident, Benno Scherrer, führte uns souverän durch sämtliche Sitzungen. Auch der Sekretär, Heiri Gander, sowie die juristische Konsulentin, Noëlle Glaus, leisteten äusserst wertvolle Arbeit für die PUK, besten Dank.
Nun, heute ist auch der Tag, den PUK-Bericht politisch zu würdigen. Es zeigt sich klar, dass während zwölf Jahren die Entsorgung von Endgeräten, Speichermedien et cetera mit sensiblen Inhalten durch eine zweifelhafte Firma ohne fachlichen Hintergrund in der JI beauftragt wurde. Es ist mehr als ärgerlich, dass keine Verträge oder Aufträge durch Personen mit Verantwortung in der JI gefunden werden konnten. Auch dieser Umstand lässt kein gutes Licht auf die Abläufe und das

Verantwortungsbewusstsein in der JI erscheinen. Dazu ein Bonmot aus den Befragungen, was den Chef einer Behörde betrifft: So war die JI mit den Chipkarten und der Verschlüsselungstechnologie der Daten relativ früh gut aufgestellt. Bei einem Kadertreffen wurde darauf hingewiesen, dass es mit dem Chipkarten-Handling relativ mühsam sei, was der Leiter dieser Behörde nicht nachvollziehen konnte. Nun, es stellte sich heraus, dass der Leiter dieser Behörde seine Chipkarte gar nie aus dem System entfernt hatte. Also das System ist halt nur so gut, wie es gelebt wird.
Dieses Bewusstsein scheint sich in der JI noch länger hingezogen zu haben. So haben Berichte der Finanzkontrolle, die Administrativuntersuchung und auch der BDO-Bericht *(Schweizer Wirtschaftsprüfungsunternehmen)* nicht zu tiefgreifenden Massnahmen geführt. Ebenso ist die Kommunikation der JI insbesondere nach der Administrativuntersuchung gegenüber dem Gesamtregierungsrat und der Datenschutzbeauftragten erst viel zu spät, zum Teil erst auf Nachfragen erfolgt. Auch in der Ressourcenplanung der JI wurden grosse Schwachpunkte aufgedeckt. So hat sich bei den Befragungen gezeigt, dass 2019 200 bis 300 neue Desktopgeräte verschleudert werden mussten, da diese nicht mehr gebraucht wurden. Doch auch der Gesamtregierungsrat hat sich über Jahre, was die Informationssicherheit betrifft, viel zu lange auf seine Abteilungen in den Direktionen verlassen. Als Regierungsrat kann man kein Experte in diesen Fragen sein – und muss es auch nicht sein –, aber der Chef muss wissen, dass alles dafür getan wird, damit die Sicherheit der Daten der Bürger und der Angestellten sicher ist. Und die Regierung muss alles tun, um die Sicherheit der Daten zu gewährleisten. Schauen Sie, am Ende des Tages ist es nun einmal der Chef, der die Verantwortung trägt, und Verantwortung ist nicht teilbar.
Damit komme ich zu den Empfehlungen. Aus unserer Sicht möchte ich nur auf die vier wichtigsten Empfehlungen eingehen. Erstens: Der Umgang mit Microsoft 365 muss kritisch hinterfragt werden und es müssen Alternativen aufgezeigt werden. Es ist nun einmal so, dass mit dem US CLOUD Act alle Daten, die bei US-Firmen sind, auch wenn diese auf Schweizer Servern gespeichert werden, vom US-Staat eingefordert werden können. Zweitens: Die Informationssicherheit muss auf kantonaler Stufe geregelt werden, damit garantiert ist, dass der Standard in allen Direktionen und der Staatskanzlei gewährleistet ist. Drittens: Der ISIK – er wurde schon erwähnt –, also der kantonale Sicherheitsbeauftragte muss mit einem Weisungsrecht ausgestattet werden. Damit können die nötigen Vorgaben rasch umgesetzt werden. Viertens: Der Kantonsrat muss seine Aufsicht über die Digitalisierung und IT in der Verwaltung bedeutend griffiger gestalten. Heute wird diese Aufsicht mit GPK, FIKO *(Finanzkommission)*, STGK *(Kommission für Staat und Gemeinden)* geteilt. Ausserdem gibt es noch die Subkommission IKT. Die heutige Situation ist nicht effizient.
Ich erlaube mir noch einen Ausblick auf aktuelle Geschehnisse. Mit RRB 766/2025 vom 9. Juli 2025 werden bei der JI 92 Millionen Franken für ein Geschäfts- und Verwaltungssystem bei den Justizbehörden als gebundene Ausgabe bewilligt, notabene zu den bereits bewilligten 25 Millionen Franken aus dem Jahr 2024, siehe RRB 815/2024. Nun, dass die Veröffentlichung dieses RRB 766/2025

schön in die Sommerferien gefallen ist, war natürlich Zufall; ein Schelm, wer eine Absicht dahinter sieht. Dieser ausführlich begründete RRB fällt nicht nur durch den hohen Betrag auf, sondern auch durch das Dialogverfahren. Dieses Verfahren scheint man dann auszuwählen, wenn man noch keine Ahnung hat, was eigentlich bestellt werden soll. Diese Befürchtung wurde mir auch persönlich im Austausch mit Gerichten bestätigt. So sollen ihre Bedürfnisse, also die Bedürfnisse der Gerichte, erst jetzt eruiert und der JI mitgeteilt werden. Ich frage mich, wie man den Betrag von 92 Millionen Franken überhaupt plausibel nennen kann, wenn man die Bedürfnisse dieser Institutionen noch gar nicht kennt. Ein seriöses Projektmanagement setzt doch erst das Erstellen der Bedürfnisse voraus. Und erst dann kann ich plausibel die Kosten veranschlagen. Entweder wurden die Kosten extrem hoch angesetzt oder es erwartet uns ein weiteres Digitalisierungs-Waterloo in der JI. Aber da die Justizdirektorin 2027 nicht wieder zur Wahl antritt, darf dies dann jemand anderes ausbaden. Ich darf der Justizdirektorin noch zu ihrer bestandenen Ausbildung als Mediatorin herzlich gratulieren. Allerdings ist es stossend, dass diese Ausbildung auf Kosten der Steuerzahler erfolgte, denn bei einem Lohn von 330'000 Franken darf die Bevölkerung erwarten, dass man sich zu 100 Prozent seiner Arbeitszeit für sie einsetzt. Diese Ausbildung hätte nach dem Ausscheiden… *(Der Ratspräsident unterbricht den Votanten.)*

Ratspräsident Beat Habegger: Bitte äussern Sie sich zum PUK-Bericht und nicht zu anderen Themen, die Sie beschäftigen. Vielen Dank.

Karl Heinz Meyer fährt fort: Ich möchte noch würdigen: Es scheint, dass der PUK-Bericht bereits Einfluss auf den Regierungsrat ausgeübt hat. Allerdings ist die Kommunikation kritisch zu würdigen. Der Regierungsrat hat der Geschäftsleitung des Kantonsrates am 22. Januar 2026 einen Brief zukommen lassen, dass das Parlament am Sonntag, 25. Januar 2026, also gestern, den RRB 21/2026 erhalten würde. Gestern, 17.51 Uhr, wurde dieser neunseitige RRB uns Parlamentariern per Mail zur Kenntnis gebracht. Da stellt sich mir schon die Frage, welche Absicht des Regierungspräsidenten dahintersteckt, dass der RRB so spät zugestellt wurde. Das kann ja auch kein Zufall sein. Oder wollten Sie uns Parlamentariern einfach noch etwas Sonntagsarbeit bescheren? Dieses Vorgehen ist für eine vertrauensvolle Zusammenarbeit unwürdig. Vor allem steht ja auch nichts Bahnbrechendes in diesem RRB. Die meisten Empfehlungen will der Regierungsrat ja umsetzen oder zumindest prüfen. Besten Dank.

Davide Loss (SP, Thalwil): Der Kantonsrat hat beschlossen, eine PUK zur umfassenden Aufarbeitung eines Datensicherheitsvorfalls in der Direktion der Justiz und des Innern einzusetzen. Die SP-Fraktion hatte sich damals gegen die Einsetzung des schärfsten Mittels der parlamentarischen Oberaufsicht ausgesprochen, hat den Entscheid des Kantonsrates jedoch akzeptiert und aktiv in der Parlamentarischen Untersuchungskommission mitgearbeitet. Die SVP-Fraktion – und allen voran Altkantonsrat Valentin Landmann – erhofften sich eine «PUK Jacqueline

Fehr», doch daraus wurde nichts. Es ist wie so oft bei Parlamentarischen Untersuchungskommissionen: Es kommt am Schluss etwas anderes heraus, als man ursprünglich vermutet hat. Statt eines Pamphlets mit langem Sündenregister der in den Augen der SVP-Fraktion unliebsamen Regierungsrätin wurde es ein solides Grundlagenwerk zur Daten- und Informationssicherheit in der kantonalen Verwaltung. Für diejenigen, die sich etwas anderes erhofften, muss das ein echter Rohrkrepierer sein. Die politische Verantwortung für diesen Datensicherheitsvorfall trägt nicht etwa Regierungsrätin Jacqueline Fehr, sondern der Gesamtregierungsrat.

Anlass für die Einsetzung der PUK war ein Datensicherheitsvorfall in der Direktion der Justiz und des Innern. Bis im Jahr 2014 wurden Hardware-Elemente unsachgemäss entsorgt. So gelangten sensible Daten in die Hände eines notorisch kriminellen Mitbürgers. Dieser drohte den Justizbehörden mit der Veröffentlichung der entsprechenden Daten. Dieser Datenvorfall, bei dem über Jahre hinweg unsachgemäss entsorgte Datenträger mit teils sensiblen Informationen in den Umlauf geraten sind, ist ein eklatanter Vertrauensbruch in die Fähigkeit der kantonalen Verwaltung, fundamentale Standards der Datensicherheit einzuhalten. Diese Daten, teils hochsensibel, gelangten in Kreise, in die sie nie hätten gelangen dürfen.

Wir stehen heute an einem Punkt, an dem wir aus einem ernsten Vorfall in der kantonalen Verwaltung nicht nur Lehren ziehen, sondern entschlossen handeln müssen, damit solche Vorkommnisse in Zukunft verhindert werden. Der Schlussbericht der PUK ist ein umfangreiches, nach intensiver Arbeit verfasstes Grundlagenwerk, das uns nicht nur den konkreten Fall, sondern auch strukturelle Defizite aufzeigt. Es ist wichtig festzuhalten: Diese mangelhafte Praxis war nicht die Folge eines Einzelfehlers, sondern von struktureller Vernachlässigung der Informationssicherheit, über Jahre hinweg und über die gesamte kantonale Verwaltung. Die PUK hat klar herausgearbeitet, dass es an einer kohärenten, gesamtkantonalen Steuerung und Strategie zur Informationssicherheit gefehlt hat. Die gesetzlichen Grundlagen der 90er-Jahre wurden zwar im Grundsatz geschaffen, aber ihre Umsetzung und Weiterentwicklung blieben unkoordiniert. Die kantonale Informationssicherheitsorganisation wurde zu wenig entwickelt. Und wenn sie entwickelt wurde, blieb sie in der Praxis oft wirkungslos. Für die SP-Fraktion ist klar: Ein moderner Staat braucht eine starke, zentrale und koordinierte Strategie für Informationssicherheit, die nicht in Silos einzelner Direktionen verpuffen darf.

Es ist zu begrüssen, dass die PUK klar zum Schluss kommt, dass der eigentliche Datensicherheitsvorfall nicht allein der amtierenden Justizdirektorin politisch angelastet werden kann, weil er sich über einen sehr langen Zeitraum erstreckte, ja, in einem Zeitraum, als die Justizdirektorin gar noch nicht im Amt war. Gleichzeitig ist es unbestritten, dass der Regierungsrat insgesamt seiner Verantwortung zu lange nicht gerecht wurde, indem er fehlende koordinierte Vorgaben und eine ganzheitliche Steuerung nicht rasch angegangen hat. Regierungsrätin Jacqueline Fehr hat nach Bekanntwerden des Datensicherheitsvorfalls gegenüber dem Regierungsrat, der Datensicherheitsbeauftragten und der GPK mangelhaft kommuniziert. So hat sie es unter anderem unterlassen, der GPK den Schlussbericht der

administrativen Untersuchung zuzustellen. Dies hat sie jedoch von Beginn weg eingestanden und sich dafür entschuldigt. Doch Hand aufs Herz, wenn das grösste Versäumnis eines Regierungsmitglieds das Nichtzustellen eines Berichts an eine Aufsichtskommission ist, dann leben wir sozusagen im perfekten Staat.
Die PUK kommt auch zum Schluss, dass in der Direktion der Justiz und des Innern ein hoher Sicherheitsstandard im Bereich Daten- und Informationssicherheit geherrscht hat. Damit ist klar, der Datensicherheitsvorfall hätte auch in jeder anderen Direktion geschehen können. Die Vernichtung der Akten in der Abteilung DigiSol *(Digital Solutions)* im Jahr 2019 hatte keinen Zusammenhang mit dem Datenvorfall. Auch das ist wenig überraschend, da der Vorfall ja erst im Jahr 2020 bekannt wurde.
Der PUK-Bericht hält fest, dass es im Nachhinein richtig war, auf die Einsetzung eines ausserkantonalen Staatsanwalts beziehungsweise einer ausserkantonalen Staatsanwältin zu verzichten. Auch hier eine Klammerbemerkung: Sie mögen sich noch an die Vehemenz erinnern, mit der das gefordert wurde. Nun zeigt sich, mit welcher Akribie Kantonspolizei und Staatsanwaltschaft die Untersuchungen komplett unabhängig geführt haben, ein starkes Zeichen für unseren Rechtsstaat. Die strafrechtliche Untersuchung stellt fest, dass es keine strafrechtlich verfolgbaren Handlungen gab. Mit den missbräuchlich erworbenen Daten wurde offenbar keine Straftat begangen, und damit ist zum Glück bis heute niemand nachweislich zu Schaden gekommen. Gleichzeitig macht die Strafuntersuchung wichtige Hinweise zur Dimension des Vorfalls. Die Systeme der Justiz waren schon damals stark geschützt. So gelang es nicht, ins Rechtsinformationssystem oder andere Fachapplikationen einzudringen; dies die wichtigsten Befunde zum Datensicherheitsvorfall an sich.
Für die SP-Fraktion ist klar: Wir fordern eine klare politische Verantwortung des Regierungsrates für die gesamtkantonale Informationssicherheit, die nicht auf einzelne Direktionen abgewälzt werden darf. Die Zeit des Silo-Denkens ist endgültig vorbei. Die PUK empfiehlt in diesem Sinn richtigerweise, dass der Regierungsrat seine Rolle als strategische Steuerungsinstanz stärker wahrnehmen muss, mit einer kohärenten IT- und Datensicherheitsstrategie, die verbindlich ist und nicht nur Empfehlung bleiben darf. Doch – und das müssen wir uns vor Augen führen – das wird etwas kosten. Es wird sich zeigen, ob die Bürgerlichen bereit sind, diesbezüglich die Verantwortung wahrzunehmen und die entsprechenden Ressourcen zur Verfügung zu stellen.
Der Regierungsrat hat seine Stellungnahme zum Schlussbericht der PUK veröffentlicht. Dass diese Stellungnahme erst am Vorabend der heutigen Debatte zugestellt wurde, lässt doch einige Zweifel an der Seriosität aufkommen, mit der der Regierungsrat diese Empfehlungen der PUK umsetzen muss. Immerhin sieht der Regierungsrat einen gewissen Handlungsbedarf – doch mit angezogener Handbremse. Für die Sozialdemokratische Fraktion ist klar: Wir brauchen keine kosmetischen Änderungen, sondern einen Kulturwandel in der Verwaltung. Datensicherheit darf nicht als rein technisches, administratives Thema verstanden werden, sondern muss Teil eines modernen demokratischen Dienstleistungsstaats

sein. Dazu gehören einheitliche, verbindliche Vorgaben zur Informationssicherheit für alle Direktionen und staatsnahen Betriebe, mit klaren Sanktionen und Kontrollmechanismen. Es braucht eine Stärkung der Aufsichtsinstanzen, nicht zur Kontrolle der Kontrolle willen, sondern um Risiken frühzeitig zu erkennen und auszuschalten und das Vertrauen der Bevölkerung in das Funktionieren der kantonalen Verwaltung sicherzustellen. Es braucht transparente Audit- und Berichtspflichten gegenüber den parlamentarischen Aufsichtsgremien, damit wir als Volksvertretung nicht erst über gravierende Vorfälle informiert werden, wenn sie bereits öffentlich geworden sind. Es braucht auch Investitionen in Fachkompetenz und Weiterbildung, denn gute Datensicherheit lebt von qualifiziertem Personal. Diese Punkte sind nicht optional, sie sind die Grundlage für ein digitales Fundament unseres Gemeinwesens, das demokratischen, rechtlichen und sozialen Standards entspricht.
Zum Schluss möchte ich meinen Kolleginnen und Kollegen der PUK für die äusserst vertrauensvolle und engagierte Zusammenarbeit danken. Mein Dank geht auch an die Mitarbeitenden der Parlamentsdienste. Ohne sie wäre es nicht möglich gewesen, ein derart solides Grundlagenwerk zu schaffen. Wir danken auch dem Regierungsrat, dass er sich den Herausforderungen gestellt hat und die notwendigen Lehren, so hoffe ich, daraus zieht. Unsere Lehre muss klar sein: Vertrauen ist kein Zustand, sondern ein fortlaufender Prozess, und dieser Prozess braucht Regeln, Ressourcen und politische Entschlossenheit. Ich zähle auf Sie. Ich danke Ihnen.

Claudio Zihlmann (FDP, Zürich): Vorab möchte ich Folgendes betonen, das ist mir sehr wichtig: Heute geht es nicht darum, Bashing gegenüber dem Regierungsrat, der Verwaltung oder sonst jemandem zu betreiben. Es geht darum, aus den vergangenen Fehlern die richtigen Schlüsse für die Zukunft zu ziehen, die richtigen Schlüsse für eine Zukunft, welche das Risiko für die Wiederholung eines solchen Falles minimiert. Und es geht nicht weniger darum, jetzt die Weichen zu stellen, damit der Kanton in Sachen Datensicherheit und IKT für die Zukunft richtig aufgestellt ist. Deswegen hoffe ich doch, dass diese Debatte heute dazu beitragen kann, nun die richtigen Schlussfolgerungen aus dem vorliegenden PUK-Bericht zu ziehen und möglichst rasch gemeinsam die richtigen Prioritäten zu setzen. Denn einen solchen Fall möchten wir nicht noch einmal erleben und deswegen gilt es nun eben gemeinsam anzupacken. Nichtsdestotrotz ist es entscheidend, die begangenen Fehler, Schwachstellen, aber auch die involvierten Direktionen und demzufolge auch Personen klar zu benennen. Denn nur durch glasklare Transparenz über das Geschehene können wir die Schlussfolgerungen für die Zukunft ziehen.
Der Präsident der PUK hat es bereits erwähnt, er hat die Hintergründe und die Stossrichtungen des 219 Seiten starken Berichts eingehend erläutert. Die FDP-Fraktion teilt die Erkenntnisse der PUK. Der Regierungsrat hatte der Informationssicherheit als gesamtkantonaler Gemeinschaftsaufgabe über die Direktionen hinweg lange zu wenig Beachtung geschenkt. Er hat die Thematik Informationssicherheit mit zu wenig Nachdruck vorangetrieben und auch nicht genügend gut

begleitet. Besonders schwerwiegend erscheint uns, dass der Regierungsrat den mahnenden Worten des früheren Datenschutzbeauftragten *(Bruno Baeriswyl)*, der Geschäftsprüfungskommission, der Finanzkommission sowie der Finanzkontrolle deutlich zu wenig Aufmerksamkeit geschenkt hatte. Für die FDP-Fraktion ist es nicht nachvollziehbar, dass der Regierungsrat diese Empfehlungen nicht mit Nachdruck verfolgte und lange kantonalen Lösungen äusserst zurückhaltend gegenüberstand. Für die FDP war insbesondere auch das Gärtchen-Denken der einzelnen Direktionen – es wurde bereits erwähnt – die eigentliche Voraussetzung, welche den Datensicherheitsvorfall damals in der Direktion der Justiz und des Innern überhaupt erst ermöglichte.
Nun kommen wir zum eigentlichen Datensicherheitsvorfall, welcher schlussendlich zum Einsetzen dieser PUK geführt hatte. Gemäss dem PUK-Bericht kann ein kausales Fehlverhalten des Regierungsrates oder der Direktionsvorsteherinnen und -vorsteher für den eigentlichen Datensicherheitsvorfall in der JI nicht festgestellt werden. Trotzdem möchte die FDP festhalten: Die Kommunikation – das wurde auch schon erwähnt – der JI gegenüber den Behörden war schlichtweg ungenügend. Gemäss dem PUK-Bericht wurde die Finanzkontrolle schon gar nicht informiert. Die Datenschutzbeauftragte erhielt den Schlussbericht erst auf wiederholte Nachfrage. Die GPK des Kantonsrates erfuhr zwar im Rahmen eines Referentengesprächs im März 2021 vom Datensicherheitsvorfall, eine Zustellung des Schlussberichts blieb aber aus. Dieses Vorgehen ist schlicht inakzeptabel. Weiter war die direkte Kommunikation der Justizdirektorin Jacqueline Fehr an den Gesamtregierungsrat ebenfalls ungenügend. Gemäss der PUK erwähnte Jacqueline Fehr bei der ersten mündlichen Information an der Regierungsratssitzung vom 18. November 2020 den Vorfall so beiläufig, dass sich später kaum jemand an diese Information erinnern konnte. Auch dieses Vorgehen ist für die FDP-Fraktion inakzeptabel. Zu jenem Zeitpunkt dürfte die Tragweite des Datensicherheitsvorfalls in der JI auch der Vorsteherin bekannt gewesen sein. Eine umfassende Kommunikation an den Gesamtregierungsrat wäre dringend notwendig gewesen. Den Schlussbericht zur administrativen Untersuchung erhielt der Regierungsrat zudem erst im Vorfeld des Point de Presse vom 6. Dezember 2022 und erst am 21. Dezember 2022 wurde der Regierungsrat über den Datensicherheitsvorfall grundlegend informiert. Es muss hier in aller Deutlichkeit gesagt werden, diese Kommunikation war ungenügend.
Nun, was der PUK-Bericht auch deutlich zeigt: Die Daten- und Informationssicherheit im Kanton Zürich scheint auch heute noch nicht abschliessend gewährleistet. Deswegen ist es nun dringend notwendig, die Empfehlungen der PUK ernst zu nehmen. Was sind nun die nächsten Schritte? Der umfangreiche Bericht enthält 50 Empfehlungen. Nicht jede dieser Empfehlungen verlangt unmittelbares Handeln durch den Kantonsrat. Aus unserer Sicht liegt es nun insbesondere auch an der GPK, die Empfehlungen zu sichten, zu priorisieren, auf eine Zeitachse zu legen und den Umsetzungsstand der Empfehlungen zu monitoren, denn die Umsetzung der Empfehlungen braucht Zeit und braucht die Zusammenarbeit mit der Verwaltung, weiteren Kommissionen sowie dem Kantonsrat als Institution, denn

nur so können wir vorwärtsmachen. Die FDP erwartet jedoch, dass dieser umfangreiche Bericht zu effektiven Änderungen, Optimierungen und Anpassungen beim Thema Datensicherheit führt. Im Zentrum steht dabei eines der höchsten Güter, das wir überhaupt haben, es geht um die sensiblen Daten der Bürgerinnen und Bürger unseres Kantons. Es muss alles unternommen werden, dass diese für die Zukunft besser geschützt werden. Wir erwarten, dass die Regierung als ein Gremium die Verbesserungen anpackt und ihre Zusammenarbeit intensiviert. Gemäss dem gestern Abend erhaltenen RRB 41/2026 ist der Regierungsrat – wir haben es vom Regierungspräsidenten bereits gehört – gewillt, die Empfehlungen der PUK mit dem Kantonsrat und seinen Organen in gegenseitiger Offenheit zu prüfen; dies ist begrüssenswert. Und gerne weise ich noch einmal darauf hin: Der PUK-Bericht wurde einstimmig genehmigt, von allen Fraktionen, weil jede Fraktion ja mit einem Mitglied in dieser PUK vertreten war. Dies bedeutet für uns, dass eben wohl auch alle Fraktionen Veränderungen zustimmen werden und müssen. Und so hoffe ich doch, dass diese Einstimmigkeit auch die Basis für das weitere einstimmige und zielgerichtete Handeln legt.
Eine wichtige Empfehlung der PUK ist bereits auf dem Weg zur Umsetzung, nämlich die Stärkung der externen IKT-Aufsicht. Die PI der FDP *(KR-Nr. 342/2025)* sowie auch die wohl kommende Kommissionsmotion werden den Anstoss geben, eine IKT-Aufsicht ins Leben zu rufen. Glauben Sie mir, als FDP-Kantonsrat widerstrebt es mir, die Miliz zusätzlich zu belasten oder zusätzliche Ressourcen für die Verwaltung zu fordern. Jedoch haben der PUK-Bericht und auch die Diskussion gezeigt: In diesem Fall erscheint es uns, als wäre eine neue Kommission, ausgestattet mit den entsprechenden Mitteln als Aufsichts- oder Sachkommission, gerechtfertigt. Wir sehen, es gilt also noch einiges zu tun. Packen wir es an – gemeinsam. Herzlichen Dank für die Aufmerksamkeit.

Gabriel Mäder (GLP, Adliswil): Die PUK Datensicherheit hat ihre Arbeit unter ausserordentlich schwierigen Umständen aufgenommen. Die mediale Inszenierung der sichergestellten Datenträger, ausgerechnet hier im Kantonsrat, die dringliche Anfrage wie auch die laufenden Beratungen und Budgetdiskussionen, die immer wieder auf die Arbeit der PUK referenzierten – alles Zutaten für ein grosses Drama. Aber die Kommission hat dem Druck widerstanden. Und nicht nur das, die Kommission hat den Fokus nicht auf Schuldzuweisungen gelegt, sondern das grosse Ganze im Blick behalten. Wo notwendig, hat sie weitere Auskunftspersonen beigezogen und sich die Zeit genommen, in die Tiefe der Materie einzutauchen. Auch ich hätte es lieber gehabt, wenn der Bericht früher fertig gewesen wäre oder wenn man wenigstens zwischendurch etwas vernommen hätte. Aber die Kommission hat ihren Auftrag mit der äussersten Geheimhaltung ausgeführt und so ihre Arbeit geschützt. Und der vorliegende Bericht entschädigt für die Wartezeit, er ist sachlich, gründlich, differenziert und frei von Polemik. Die Kommission hat nicht skandaliert, sondern strukturell analysiert, das verdient grosse Anerkennung.
Der Auslöser der Untersuchung ist bekannt: die unsachgemässe Entsorgung von Datenträgern mit sensiblen Informationen. Dieser konkrete Vorfall ist ernst zu

nehmen. Gleichzeitig macht der Bericht sehr klar: Er ist nicht das eigentliche Problem, er ist ein Symptom. Die entscheidende Frage lautet nicht, wie ein einzelner Datenträger entsorgt wurde, sondern warum ein solcher Vorfall in einem modernen Kanton überhaupt möglich ist und weshalb Warnsignale über Jahre hinweg keine ausreichende Wirkung entfaltet haben. Dass uns der Regierungsrat heute versichert, ein solcher Vorfall sei unter den heutigen Rahmenbedingungen nicht mehr möglich, ist zur Kenntnis zu nehmen, er ist jedoch kein Grund zur Beruhigung. Entscheidend ist nicht, ob sich ein konkreter Fehler zukünftig verhindern lässt, sondern ob das System insgesamt in der Lage ist, künftige Risiken frühzeitig zu erkennen und mögliche Schadensfälle zu minimieren.
Der Bericht zeigt deutlich: Datensicherheit ist im Kanton Zürich über lange Zeit nicht als strategische Führungsaufgabe behandelt worden. Risiken waren bekannt, Regelwerke existierten, Gremien wurden geschaffen, und dennoch fehlte es an Verbindlichkeit, an Durchsetzungskraft und an klarer politischer Verantwortung. Besonders aufschlussreich ist auch der Umgang mit der Administrativuntersuchung von 2021. Sie führte nicht zu einem unmittelbaren politischen Handlungsimpuls, sie wurde als nicht dringlich eingeschätzt, nicht systematisch im Gesamtregierungsrat behandelt und politisch nicht verarbeitet. Das ist kein individuelles Versäumnis, sondern ein strukturelles Problem im Umgang mit querschnittlichen Risiken.
Aus Sicht der GLP ist klar: Digitale Risiken sind Governance-Risiken, sie gehören auf die Ebene der politischen Führung. Wer den PUK-Bericht liest, trifft auf viele Befunde, die für dieses Parlament nicht neu sein dürften. Bereits der GPK-Spezialbericht zur IT aus dem Jahr 2017 hat gravierende Mängel bei Führung, Steuerung und Koordination der kantonalen Informatik festgestellt. Damals wurde festgehalten, dass eine klare strategische Führung fehlt, direktionsbezogene Interessen gesamtkantonale Lösungen blockieren und die politische Steuerung der IT unzureichend ist; es kommt uns bekannt vor. Diese Feststellungen wurden mit Empfehlungen verbunden. Der heutige PUK-Bericht zeigt aber leider, wie viele dieser strukturellen Probleme immer noch bestehen. Wir müssen damit feststellen: Der Datensicherheitsvorfall ist damit kein Bruch, sondern eine Fortsetzung bekannter Muster.
Ich möchte drei Cluster von Empfehlungen aus Kapitel 18 des Berichts hervorheben, die exemplarisch zeigen, wo die strukturellen Probleme liegen. Erstens, die Empfehlungen 1 bis 3: Die PUK stellt fest, dass der Regierungsrat als Kollegialbehörde stark auf die einzelnen Direktionen fokussiert ist, und fordert eine intensivere Zusammenarbeit und gemeinsame Verantwortung. Besonders deutlich wird es in Empfehlung 3, welche eine Anpassung der Organisationsverordnung verlangt, weil zentrale Zuständigkeiten zur Umsetzung des IDG heute auf Direktionsebene statt auf gesamtkantonaler Ebene verortet sind. Das ist ein zentraler Befund. Solange jede Direktion primär für sich handelt, entsteht keine durchgängige Sicherheitsarchitektur.
Zweitens, Empfehlungen 45 und 46: Die PUK fordert eine regelmässige, strukturierte Berichterstattung zu Informationssicherheitsrisiken, analog zu den Berichten der Finanzkontrolle zu IT-Schlüsselprojekten. In Empfehlung 46 wird explizit

verlangt, dass auch Audit-Berichte und Berichte der Datenschutzbeauftragten den Aufsichtskommissionen zur Kenntnis gebracht werden sollen. Das zeigt sehr klar: Die Oberaufsicht konnte ihre Rolle nicht wahrnehmen, weil sie zu wenig systematische Informationen erhielt.
Drittens, Empfehlungen 48 bis 50: Hier wird die Problematik der Aufsicht am deutlichsten. Die PUK fordert in Empfehlung 48 ausdrücklich eine wesentliche Stärkung der externen Aufsicht und schliesst die Schaffung einer neuen unabhängigen Aufsichtsinstanz nicht aus. In Empfehlung 50 erinnert sie den Kantonsrat ausdrücklich daran, die Umsetzung der Informationssicherheit im Rahmen der begleiteten Oberaufsicht engmaschig zu verfolgen und dafür gegebenenfalls neue Strukturen zu schaffen. Und wie von Kollege Zihlmann erwähnt, sind wir da bereits dran. Das ist bemerkenswert klar und deutlich und ein direkter Auftrag an dieses Parlament.
Noch ein Wort zur Verschachtelung der Gremien: Der Bericht zeigt auch sehr anschaulich, wie die Verantwortung in der Praxis verläuft: operative Verantwortung in den Direktionen, fachliche Koordinationen über den ISIK und Fachgremien oder durch externe Stellen oder die Finanzkontrolle, Datenaufsicht mit beratender und prüfender Rolle, politische Verantwortung beim Regierungsrat, Oberaufsicht bei den Aufsichtskommissionen. Das Problem ist nicht, dass wir zu wenig Gremien haben, das Problem ist, dass niemand durchgehend die Gesamtverantwortung trägt und Informationen nicht systematisch zusammengeführt werden. Digitalisierung wurde über Jahre als Abfolge einzelner Projekte verstanden, eine Fachanwendung hier, ein Pilotprojekt dort, unterschiedliche Standards je Direktion. Gesamtkantonale Lösungen waren zwar vorgesehen, aber oft freiwillig und damit zu schwach. Aus Sicht der GLP reicht dieses Verständnis zu kurz. Digitalisierung und zunehmend auch künstliche Intelligenz sind keine Projektfrage, sondern eine Infrastrukturfrage. Kein Amt baut seine eigenen Strassen, kein Schulhaus plant sein eigenes Autobahnnetz. Die Infrastruktur wird gemeinsam strategisch und politisch verantwortet und gebaut. Auf ihr können dann unterschiedliche Anwendungen genutzt werden, mit unterschiedlichen Bedürfnissen, aber auf einer gemeinsamen Grundlage. Liebe Ratsmitglieder, geschätzter Regierungsrat, Digitalisierung und KI sind Infrastruktur und diese gilt es ganzheitlich anzugehen. Darum freue ich mich, dass ich vom Regierungsratspräsidenten das Wort «Infrastruktur» in Bezug zur Digitalisierung heute zum ersten Mal im Rat gehört habe. Der PUK-Bericht zeigt, was passiert, wenn diese Sicht fehlt: Fragmentierung, unklare Zuständigkeit und Sicherheitslücken. Der Bericht legt auch die Grenzen der bisherigen Aufsicht offen. Die parlamentarische Aufsicht war vielfach auf fragmentierte, punktuelle oder verspätete Informationen angewiesen. Prüfungen fanden statt, erreichten das Parlament häufig aber erst, wenn Probleme bereits eskaliert waren. Das ist kein Vorwurf an den Kantonsrat, es ist ein strukturelles Defizit.
Aus Sicht der GLP braucht es darum eine Stärkung der Oberaufsicht nicht im Sinne von mehr Micromanagement, sondern im Sinne von besserer Steuerungsfähigkeit. Es braucht regelmässige, unabhängige Prüfungen, klare, vergleichbare Berichterstattung und transparente Eskalationsmechanismen. Gute Aufsicht ist

kein Misstrauen gegenüber der Verwaltung einer Regierung, sie ist Voraussetzung für Vertrauen, Akzeptanz und Innovationsfähigkeit.
Besonders wichtig ist für die GLP der Blick nach vorne. Die im PUK beschriebenen Muster sind nicht abgeschlossen, beim Einsatz von künstlicher Intelligenz drohen sich dieselben Fehler zu wiederholen. Viele Analysen, viele Leitlinien, aber weiterhin offene Fragen zur Verantwortung, Kontrolle und politischen Steuerung. KI ist kein IT-Tool und kein Pilotprojekt, KI ist ein Governance-Thema mit Grundrechts- und Vertrauensrelevanz. Wer aus der Datensicherheit nicht lernt, wird diese Lektion bei der KI erneut bezahlen.
Die GLP will weder Technologie bremsen noch Risiken verdrängen, sie steht für Innovationen mit klaren Leitplanken, für einen Staat, der digitale Risiken nicht vermeidet, sondern beherrscht. Aus dem PUK-Bericht zieht die Grünliberale Fraktion deshalb drei zentrale Konsequenzen: Erstens, es braucht klare politische Gesamtverantwortung für digitale Infrastruktur, Informationssicherheit und KI. Zweitens, es braucht unabhängige regelmässige Prüfungen statt punktueller Selbstkontrolle. Und drittens, es braucht eine gestärkte parlamentarische Oberaufsicht, die systematisch informiert wird und frühzeitig eingreifen kann. Nicht mehr Technik oder mehr Gesetze, sondern bessere Governance ist der Schlüssel. Besten Dank.

Urs Dietschi (Grüne, Lindau): Liebe Kolleginnen und Kollegen PUK-Mitglieder, Sekretär, rechtliche Beratung, Noëlle Glaus, herzlichen Dank für die super Zusammenarbeit. Für mich war das in meiner Kantonsratszeit ein Highlight. Es wird mir in Erinnerung bleiben als *das* Ereignis durch die ganze Zeit, die nächste Woche endet *(der Votant hat seinen Rücktritt aus dem Kantonsrat angekündigt)*.
Zur Datensicherheit und Entsorgung: Gestern erhielten wir den regierungsrätlichen Bericht, die Antwort auf den PUK-Bericht. Ich war entsetzt – gleiches Weitergehen mit dem Gärtli-Denken. Es ist nicht nachvollziehbar, dass man das heute noch so zelebrieren will, dass eine solche Firma, wie der Kanton eine ist, sich nachlässig in den eigenen Wänden wohlfühlt. Das Problem aus alter Zeit wird weiter produziert. Die Fortschritte, die gemacht wurden, sind sichtbar, aber es muss aufhören, dass jede Direktion für sich denkt und versucht, die Sicherheit richtig zu machen. Es fehlt ein gesamtheitlicher Ansatz, und das funktioniert nur, wenn alle zusammenarbeiten und sich nicht, wie in der Vergangenheit, auf den Schuhen stehen, was dann schlussendlich eben auch mit mangelnder Kontrolle zu dem Datensicherheitsvorfall führte. Die nicht kontrollierte Entsorgung hätte aber gerade so gut in anderen Direktionen passieren können, deswegen ist es fehl am Platz, die Anschuldigungen nur auf die JI zu richten. Es ist richtig, dass die Justizdirektorin schlecht kommuniziert hat, aber daraus eine Rücktrittsforderung zu machen, ist total falsch und daneben. Die Zusammenarbeit in den Direktionen manifestiert sich in einer Äusserung eines Mitglieds, das monierte, warum auch bei ihm untersucht werde. Es hat seinen Grund, weil überall etwas zu sehen war und, wie der PUK-Bericht leider feststellen musste, an vielen Ecken die Kurven nicht richtig gekriegt wurden, es zu lasch genommen wurde. Es gibt keine Direktion mit weniger wichtigen Daten, es haben alle denselben Standard einzuhalten,

das heisst auf gut Deutsch: Der ISIK ist mit Weisungsrecht auszustatten. Er muss auch, ob es den Direktionsvorstehenden wehtut oder nicht und auch wenn es ihre Macht eventuell einschränkt, mit Weisungen ausgestattet sein und diese durchbringen können, und zwar ohne langes Diskutieren oder Hausieren, wie das heute der Fall ist, um dann vielleicht doch noch im Ziel anzukommen. Es hat, wie gesagt, Verbesserungen gegeben, aber da ist es sehr, sehr wichtig, dass dies geändert wird.
Ein weiterer Punkt ist, dass das AFI einer Direktion unterstellt ist. Das AFI müsste selbstständig sein und von allem verwaltet werden, damit die ganze Sache besser in Fluss kommt, was die Sicherheit anbelangt. So wie es heute läuft, wird es irgendwann wieder zu einem Vorfall kommen, weil ja die Direktionen für sich ihr Gärtchen pflegen und nicht gross über die Mauern oder über den Zaun schauen. Daher ist es eben wichtig, wie gesagt, dass die Strukturen so geändert werden, dass der ISIK selbstständig ist. Man muss sich dann vielleicht auch darüber unterhalten, wem er unterstellt ist. Es kann nicht sein, dass ihm ein Direktionsmitglied vorgesetzt ist. Man muss sich überlegen, ob man das ähnlich wie bei der Datenschutzbeauftragten handhabt, ob der Kantonsrat für die Wahl zuständig sein soll. Dann kommt die Selbstständigkeit des AFI dazu, das die Dienstleistung für alle Direktionen erbringt. Es macht keinen Sinn, wenn in den einzelnen Direktionen noch gerufen wird, «ja, das ist eine Spezialapplikation, die läuft nur bei uns!», denn technisch können alle am selben Ort laufen, ein Fachspezialist kann ja noch dort sein. Aber an und für sich muss die Sache einer modernen Struktur angepasst werden. Der Kanton ist eine grosse Firma. Schauen Sie sich bei einer Firma um, wie das Ganze strukturiert ist. Das Anhängen der Informatik an die Finanzabteilung ist ein sehr, sehr alter Zopf.
Was weiter noch bei der Zusammenarbeit fehlt, ist eben die letzte Transparenz. Das Weisungsrecht, wie gesagt, muss unbedingt eingehalten werden. Und es muss weiter in die Zukunft geschaut werden. Ich habe schon im September einmal den RRB 542/2022 bezüglich des Microsoft-Produkts angesprochen. Es zieht sich das gleiche Muster durch den ganzen Bericht, man verteidigt sich und steckt vielfach den Kopf in den Sand. Der RRB 542/2022 zeigt einzig, dass man nicht gewillt ist, der heutigen Weltlage Rechnung zu tragen. Der Kanton muss sich bemühen, von den Tech-Giganten aus den USA wegzukommen. Der US CLOUD Act kann jederzeit zuschlagen, das ist keine Wahrscheinlichkeitsrechnung, ob das dann vielleicht in so und so vielen Jahren passiert, das ist eine 50-Prozent-Chance. Und wie ein Beispiel zeigt: Einem französischen Richter am Gericht in Den Haag wurden alle amerikanischen Produkte, von der Kreditkarte bis zum Arbeitsplatz alles Microsoft-Produkte, blockiert. Das kann bei der heutigen politischen Lage auch passieren. Deswegen muss unbedingt eine Strategie entwickelt werden, um von diesen Produkten wegzukommen. Es gibt genügend andere, freie Produkte, bei denen die Abhängigkeit nicht da ist, wo man nicht das Risiko hat, von einem so repressiven Staat gegängelt zu werden oder eines Tages ins Büro zu kommen und es funktioniert nichts mehr. Es gibt Produkte auf dem europäischen Markt, in der Schweiz, und der Kanton soll sich dorthin bewegen. Es gibt Staaten, die von den gefährlichen amerikanischen Produkten weggehen. Beim Bund kommt langsam

ein Umdenken, es muss auch hier passieren. Es ist klar – der Regierungspräsident hat es ausgeführt –, es hat ein Preisschild. Aber was ist einfacher, einen Preis zu zahlen oder irgendeines Tages sagen zu müssen «Die Daten sind weg»? Man muss dahin kommen und die Informatik neu aufstellen.
Man braucht vielleicht nicht unbedingt eine Aufsichtskommission aus dem Rat. Bei der Datenschutzbeauftragten sind entsprechende Leute, man könnte sie engagieren. Sie rapportieren regelmässig bei der GPK, was sie gesehen haben, wo es noch Sachen zu tun gibt. Und punkto Schulung – es wurde erwähnt – ist man auf einem besseren Weg. Aber das müsste eigentlich sein wie bei Banken, dort gibt es jedes Jahr einen Fragebogen. Wer ihn nicht besteht, hat an eine Nachsitzung, an einen Kurs zu gehen, wo ihm die fehlenden Punkte beigebracht werden. Dann entwickeln wir uns in die richtige Richtung punkto Datensicherheit. Diesbezüglich hoffe ich auf die Aufmerksamkeit der Regierung, dass sie nicht in ihren Plattitüden «wir arbeiten gerne zusammen» et cetera hängenbleibt, sondern dass es an die Hand genommen wird und der Kantonsrat als Aufsicht darauf drückt, dass das in die richtigen Bahnen kommt. Danke.

Ratspräsident Beat Habegger: Ich begrüsse noch auf der Tribüne eine Klasse des Gymnasiums Unterstrass. Herzlich willkommen bei uns im Kantonsrat.

Marzena Kopp (Die Mitte, Meilen): Die Mitte hält fest, dass der Datensicherheitsvorfall in der Direktion der Justiz und des Inneren im Rahmen der parlamentarischen Untersuchung gründlich, sachlich und umfassend aufgearbeitet wurde. Der PUK-Bericht ist eine nüchterne Analyse der Vorkommnisse. Die Ursachen dieses Vorfalls sind vielschichtig, einfache Schuldzuweisungen sind kaum möglich. Der Datensicherheitsvorfall basiert zwar auf krimineller Energie, ist aber auch Ausdruck struktureller Schwächen in Governance, Führung und Zusammenarbeit. Es mangelte nicht an gesetzlichen Grundlagen oder formellen Weisungen, sondern an der konsequenten Umsetzung, an strategischer Begleitung und an einer gemeinsam wahrgenommenen Verantwortung auf der Ebene des Regierungsrates. Zwar waren rechtliche Grundlagen zur Informationssicherheit über Jahre hinweg grundsätzlich vorhanden, ihre Umsetzung und Verankerung wurden jedoch politisch zu wenig priorisiert. Insbesondere die mangelnde Management-Attention führte dazu, dass Risiken nicht frühzeitig erkannt und systematisch adressiert wurden. Der PUK-Bericht zeigt nachvollziehbar auf, dass wiederholte Warnungen zwar zur Kenntnis genommen wurden, jedoch ohne die notwendigen strukturellen und politischen Konsequenzen blieben. Diese Zurückhaltung ist aus heutiger Sicht klar zu kritisieren.
Der Bericht macht zudem deutlich, dass ein ausgeprägtes direktionsbezogenes Denken – alternative Bezeichnungen: Silo-Denken, Königreiche, Gärtli-Denken – innerhalb des Regierungsrates die Entwicklung einer wirksamen gesamtkantonalen Informationssicherheit erheblich erschwert hat. Der starke Fokus auf den jeweiligen Zuständigkeitsbereich mag aus Sicht der einzelnen Person nachvollziehbar sein, ist politisch jedoch problematisch. Informationssicherheit, Daten-

schutz und Informatik allgemein sind Querschnittsaufgaben und müssen gesamtheitlich gedacht, gesteuert und verantwortet werden. Dem ist organisatorisch Rechnung zu tragen.
Kritisch zu würdigen ist, dass die Informationssicherheit wiederholt in den Hintergrund rückte. Dass zentrale Regelungen zur Informationssicherheit von der Verordnungs- auf die Richtlinienebene verschoben wurden, sehen wir ebenfalls kritisch. Gleichzeitig anerkennt die Mitte ausdrücklich, dass in den letzten Jahren wichtige Schritte zur Stärkung der Informationssicherheit eingeleitet wurden. Der Aufbau von Informationssicherheitsstrukturen, die Einführung kantonaler Schulungen sowie die Verabschiedung einer Informationssicherheitsstrategie sind richtige und notwendige Massnahmen. Wie nachhaltig ihre Wirkung sein wird, hängt jedoch entscheidend davon ab, ob sie verbindlich ausgestaltet, kohärent umgesetzt und dauerhaft politisch begleitet werden. Besonders zentral sind dabei klare Zuständigkeiten, eine stärkere rechtliche Verankerung, vereinfachte Governance-Strukturen sowie eine wirksame interne und externe Aufsicht.
Die Mitte nimmt wohlwollend zur Kenntnis, dass der Regierungsrat die im PUK-Bericht formulierten Empfehlungen teilweise bereits angegangen hat beziehungsweise dies beabsichtigt. Die Stärkung der Rolle des Amtes für Informatik, AFI, im Bereich der IKT-Grundversorgung, die Verankerung der AISR und des ISIK in der IVSV *(Verordnung über die Informationsverwaltung und -sicherheit)* werden ausdrücklich begrüsst. Wo das AFI organisatorisch angesiedelt ist oder sein sollte, ist Ansichtssache. Entscheidend sind vielmehr dessen Führung sowie die Koordination, Steuerung und Zusammenarbeit über alle Direktionen hinweg. Ebenfalls begrüsst die Mitte, dass der Regierungsrat prüft, einen einheitlichen kantonalen Entsorgungsprozess einzuführen. Schulungen, wie die Sensibilisierung auf Sicherheitsrisiken wie Phishing, sind heute schon verbindlich. Es ist festzulegen, welche weiteren Schulungsmodule zur Informationssicherheit und zum Datenschutz als obligatorisch festzulegen sind. Klare, rechtzeitige, transparente und umfassende Kommunikation ist das A und O, ist eine zentrale Voraussetzung für das Funktionieren einer Kollegialbehörde. Sie schafft Vertrauen und Verlässlichkeit, verhindert Missverständnisse und bildet die Grundlage für eine effiziente und konstruktive Zusammenarbeit. Eine Kollegialbehörde kann nur dann wirksam funktionieren, wenn das Miteinander mindestens gleich viel zählt wie der eigene Zuständigkeitsbereich. Wenn Herausforderungen gemeinsam mit gegenseitiger Verantwortung angegangen werden, stärkt es nicht nur das Gremium und die Verwaltung, sondern das Vertrauen der Bevölkerung und damit den ganzen Kanton.
Im Nachhinein ist man immer klüger. Entscheidend ist nicht nur die rückblickende Bewertung vergangener Fehler, sondern die Bereitschaft, daraus zu lernen und die richtigen Konsequenzen zu tragen. In diesem Sinne sind die Erkenntnisse der PUK als Chance zu verstehen, aus Fehlern zu lernen, Verbesserungen anzustossen und notwendige Massnahmen klar und konsequent umzusetzen. Dabei handelt es sich nicht um ein abgeschlossenes Projekt, sondern um eine dauerhafte Aufgabe. Auch wenn die Mitte dezidiert gegen die Einsetzung der PUK war, nach der Einsetzung der Kommission habe ich mich in diese Aufgabe geschickt, und

ja, es war eine lehrreiche Erfahrung. Abschliessend danke ich dem Präsidenten der PUK, dem Kommissionssekretär, der Rechtskonsulentin und den Protokollführerinnen für ihren grossen Einsatz und allen PUK-Mitgliedern für die gute, konstruktive Zusammenarbeit. Die Mitte nimmt den Bericht der PUK zur Kenntnis. Besten Dank.

Michael Bänninger (EVP, Winterthur): Auch meinerseits zuerst herzlichen Dank an Benno Scherrer für die souveränen Sitzungsleitungen, an meine Kolleginnen und Kollegen der Kommission für die kritischen Debatten und an Heiri Gander, Noëlle Glaus und Franziska Gasser für die Sitzungsvor- und -nachbereitungen.
Die EVP-Fraktion war gegenüber der Einsetzung dieser PUK kritisch eingestellt. Wir haben uns gefragt, ob eine PUK wirklich das geeignete Instrument ist oder ob nicht bestehende Aufsichtsstrukturen auch ausgereicht hätten. Heute stellen wir fest: Diese PUK war richtig, notwendig und letztlich wertvoll; nicht weil sie spektakuläre Skandale aufdeckte, sondern weil sie umfassend und systematisch die Gegebenheiten der Informationssicherheit in der kantonalen Verwaltung beleuchtete.
Der Bericht zeigt deutlich, dass der eigentliche Schaden nur beschränkt im konkreten Datensicherheitsvorfall liegt, sondern in den strukturellen Schwächen, die ihn überhaupt erst möglich gemacht haben. Über Jahre hinweg war die Informationssicherheit zwar formal geregelt, erhielt aber nicht die Priorität, die sie angesichts der Sensibilität staatlicher Daten zwingend hätte haben müssen. Die Verantwortung war zersplittert, die Umsetzung uneinheitlich, die Aufsicht schwach aufgestellt. Die Direktionen handelten weitgehend für sich, Silo-Denken statt Gesamtverantwortung.
Die Erkenntnisse der PUK sind klar formuliert. Der Regierungsrat war sich der Problematik grundsätzlich bewusst, hat aber die Umsetzung seiner eigenen Strategien über lange Zeit zu wenig begleitet und eingefordert. Wichtige Massnahmen verzögerten sich, Regulative wurden abgeschwächt oder auf tiefere Ebenen verschoben. Erst ab 2022 setzte eine spürbare Verstärkung ein, allerdings ohne eine bis heute überzeugende gesamtkantonale Strategie.
Besonders deutlich wird dies bei der Entsorgung von Datenträgern. Die Prozesse waren uneinheitlich, teils schlecht dokumentiert und unzureichend kontrolliert, selbst in Bereichen mit hochsensiblen Personendaten. Dass es hier über Jahre zu Fehlentsorgungen kommen konnte, ist nicht das Versagen Einzelner allein, sondern Ausdruck eines strukturellen Problems.
Die EVP anerkennt ausdrücklich, dass sich in den letzten Jahren vieles verbessert hat. Neue Richtlinien, stärkere Sensibilisierung, der Aufbau von Informationssicherheitsmanagementstrukturen und zusätzliche Audits gehen in die richtige Richtung. Doch es ist ebenso klar: Auf dem Papier allein genügt es nicht, in der Praxis bestehen weiterhin Risiken in der sehr unterschiedlich entwickelten Sicherheitskultur der Direktionen und Anstalten. Besonders wichtig sind deshalb die Empfehlungen der PUK. Zentral ist für uns als EVP die Forderung nach einer klaren Governance. Informationssicherheit darf keine Frage einzelner Direktionen sein, sie ist eine gemeinsame Verantwortung des gesamten Regierungsrates.

Die EVP begrüsst es, dass der Regierungsrat bereit ist zu prüfen, ob die Funktion des ISIK, des kantonalen Informationssicherheitsbeauftragten, allenfalls organisatorisch an anderer Stelle angegliedert werden sollte und mit einem eigenen Weisungsrecht ausgestattet werden kann. Wir erwarten, dass es nicht nur geprüft wird, sondern Wege gesucht und gefunden werden, wie dies umgesetzt werden kann.
Ebenso entscheidend ist für uns die Stärkung der externen Aufsicht, ob durch die Datenschutzbeauftragte, die Finanzkontrolle oder allenfalls durch eine unabhängige neue Instanz. Entscheidend ist nicht das Organ, sondern die Wirksamkeit der Kontrolle. Informationssicherheit braucht verbindliche Standards, regelmässige Prüfung und Transparenz gegenüber Parlament und Öffentlichkeit. Die Empfehlungen der PUK sind kein unverbindlicher Hinweis, sondern ein klarer Auftrag an Politik und Verwaltung. Es geht letztlich um Vertrauen, Vertrauen der Bevölkerung in den sorgfältigen Umgang mit ihren Daten, Vertrauen der Mitarbeitenden in klare Prozesse und Vertrauen des Parlaments in eine funktionierende digitale Governance. Entscheidend wird nicht sein, was heute beschlossen wird, sondern was in den kommenden Jahren tatsächlich umgesetzt wird. Wir brauchen keine Lippenbekenntnisse, sondern wir erwarten Taten.
Die EVP wird den Prozess kritisch, konstruktiv und mit Nachdruck begleiten. Herzlichen Dank.

Manuel Sahli (AL, Winterthur): Über zweieinhalb Jahre nach Einsetzung der PUK diskutieren wir heute über den entsprechenden Abschlussbericht. Ich glaube, es kann sicher gesagt werden, dass alle PUK-Mitglieder einen tiefen Einblick in das Funktionieren der Verwaltung und über die Entwicklung der Informatik derselben über die letzten Jahrzehnte erlangten. Die Zusammenarbeit in der PUK war gut, und ich möchte mich hierfür bei allen Kommissionsmitgliedern sowie auch bei den Parlamentsdiensten bedanken, denn ohne diese und auch die grossartige Mitarbeit mitunter von Kommissionssekretär Heiri Gander, der die unzähligen Unterlagen gekonnt aufarbeitete, und auch der juristische Beraterin Noëlle Glaus sowie der Protokollführerin Franziska Gasser wäre diese Arbeit für eine Milizkommission wie die unsrige nicht möglich gewesen.
Während den über zwei Jahren unserer Kommissionsarbeit ist uns an verschiedenen Stellen immer wieder dasselbe aufgefallen: Wir haben es hier mit sieben Königreichen zu tun, jede Direktion in unserem Kanton funktioniert eigenständig. Und sobald es um direktionsübergreifende Zusammenarbeit geht, wird es schwierig und kompliziert. Doch genau im Bereich der Informatik gibt es eben solche Grenzen nicht. Und irgendwelche direktionalen Empfindlichkeiten und Sonderwünsche sind der Informatiksicherheit oder auch allgemein einer effizienten Informatikorganisation gar nicht förderlich. Der Regierungsrat hat hier in seiner Gesamtheit in der Vergangenheit darin versagt, viel früher die Informatikorganisation in die richtigen Bahnen zu lenken. Daran scheiterte nicht zuletzt die erste Informatikstrategie 2008, bei der die Organisation nicht stimmte und es wohl auch an Unterstützung durch die damaligen Regierungsrätinnen und Regierungsräte mangelte. Wir anerkennen, dass hier in den letzten Jahren vorwärtsgemacht und die Informatik endlich unter einem Dach vereint wurde. Doch ist man mit diesem

Schritt immer noch viel später dran als andere Kantone, die hier die Zeichen der Zeit früher erkannten. Und auch heute noch gibt es viele Möglichkeiten für Ausnahmen, wodurch auch eigentlich vorhandene Richtlinien wieder ausgehebelt werden können. Wir fordern alle Regierungsrätinnen und Regierungsräte auf, hier vermehrt zusammenzuarbeiten. Wir begrüssen es, dass der Regierungsrat nun vorwärtsmacht und die bestehende Informatikstrategie in eine Verordnung giessen will, sowie auch die vorgesehene Überprüfung beziehungsweise hoffentlich auch die Zertifizierung nach ISO 27001 *(Internationale Organisation für Normung)*, die wohl nichts anderes als ein selbstverständlicher Standard im Bereich der Informatiksicherheit darstellen sollte. Die entsprechenden Revisionsberichte können Sie dann sicher auch den entsprechenden hierfür verantwortlichen Aufsichtskommissionen des Kantonsrates zur Kenntnis bringen. Solches Reporting ist für eine funktionierende Oberaufsicht wichtig und notwendig, egal in welcher Form diese in Zukunft zu diesem Rat ausgestaltet werden wird.
Es ist aber vorerst festzuhalten, dass all diese Massnahmen, auch auf einer allgemeinen Zeitleiste betrachtet, wohl sehr spät kommen. Wir haben nun das Jahr 2026 und wir können langsam festhalten, dass unser Kanton immerhin eine Übersicht über die im Kanton eingesetzten Applikationen hat, wohl eine absolute Grundlage, um überhaupt eine vernünftige IT-Sicherheit aufzubauen und um überhaupt eine sogenannte risikobasierte Überprüfung vorzunehmen, wie sie der Regierungsrat nun vorschlägt. Denn wie soll man ein Risikomanagement aufziehen, wenn man die hierfür notwendigen Risiko-Assets nicht kennt, man also nicht einmal weiss, auf welche Grundlagen man eine Risikoanalyse und Risikobeurteilung vornehmen soll? Dies ist lediglich die Basis für eine saubere Sicherheitsstrategie. Und wohlgemerkt besteht die Informatiksicherheit längst nicht nur aus Hoxhunt, denn an diesem Programm, auch wenn es definitiv nicht schlecht ist, habe ich mich inzwischen auch schon sattgehört. Und alle Phishing-Simulationen nützen am Ende auch nichts, wenn die übrigens Sicherheitslinien nicht «verhebed». Mir ist aber sehr wohl bewusst, dass die kantonale Sicherheitsstrategie glücklicherweise nicht nur aus diesem Produkt besteht. Hier sehen wir auch eine klare Stärkung der Informatiksicherheit innerhalb des Kantons, wenn die Stelle des ISIK, wie empfohlen, mit entsprechenden Kompetenzen ausgestattet wird. Gleichzeitig müssen wir konsterniert feststellen, dass sich der Kanton um das Thema «Microsoft 365» weiter herumdrückt. Trotz klarer Kritik von verschiedenen Datenschutzfachleuten und auch angesichts der jüngsten Entwicklungen in den USA hält der Kanton an seiner Cloud-Strategie unbeirrt fest. Nicht zuletzt hat sich unsere kantonale Datenschutzbeauftragte, Dominika Blonski, hierzu klar geäussert, doch diese Worte scheinen am Kanton unbeachtet vorbeizuziehen, sodass wir dann in ein paar Jahren vielleicht über eine PUK in Sachen Cloud-Benutzung diskutieren müssen. Während andere Kantone wie Bern und Basel-Stadt oder auch die Stadt Zürich reagieren, hinkt hier der Kanton Zürich weiter hinterher. Überlegungen zu Datenschutz und digitaler Souveränität sind weiterhin fremd. Insbesondere auch in der heutigen Zeit muss hier der Kanton reagieren und kann nicht weiter blind darauf vertrauen, dass hier schon alles gut kommt, zumal durchaus zu erwarten ist, dass die Kosten für Cloud-Dienstleistungen mit steigender

Abhängigkeit von Microsoft auch noch weiter steigen, und auch der CLOUD Act ist nicht zu unterschätzen. Hier erwartet die AL eine klare Reaktion des Kantons. Nun habe ich viel allgemein zum Bericht gesprochen, aber kommen wir noch zu des Pudels Kern, denn für diese allgemeinen Erkenntnisse hat die bürgerliche Mehrheit hier im Rat diese teure PUK nicht eingesetzt. In Sachen Datensicherheitsvorfall, der diese PUK ausgelöst hat, müssen wir eindeutig festhalten, dass wir hier keine neueren Erkenntnisse haben als jene, die bereits bekannt waren. Die Justizdirektion war im Vergleich zu anderen Direktionen bereits früh gut aufgestellt. Wir konnten hier einzig Diskrepanzen in der Kommunikation seitens Frau Regierungsrätin Fehr verorten, und dies hat Frau Fehr, wie auch bereits gehört, bereits eingestanden. Dies will jedoch nicht heissen, dass bei der JI früher alles gut war. Jedoch war es nicht so, dass die Justizdirektion gemäss Erkenntnissen der PUK von anderen Direktionen abgefallen wäre. Wenn von der SVP bei der Veröffentlichung des PUK-Berichts dann Rücktrittsforderungen an Frau Regierungsrätin Fehr laut werden und jetzt in der Beratung sogar völlig sachfremde Themen herangezogen werden, so ist es doch offensichtlich, wie sehr diese an den Haaren herbeigezogen sind oder, um es anders zu formulieren, angelehnt an eine frühere populäre Fernsehsendung *(gemeint ist die Ratesendung «Was bin ich?»),* für solches können Sie einen Fünfliber in das Phrasenschwein *(in der TV-Sendung gab es ein Sparschwein)* werfen, denn viel mehr sind solche Verlautbarungen am Ende nicht wert. Vielmehr müssen Sie sich fragen, ob die halbe Million Franken, die Sie hier für die PUK ausgegeben haben, nicht am Ende herausgeschmissenes Geld ist. Wir von der AL waren bereits bei der Einsetzung der PUK gegen diese, und ich kann Ihnen auch zum Schluss sagen: Die PUK-Arbeit war interessant und hat uns einen guten Einblick in das Schaffen der kantonalen Verwaltung gebracht, aber eigentlich hat sie nichts wesentlich Neues zutage befördert, wir wären auch gut ohne sie gefahren. Die Fraktion der Alternativen Liste ist daher klar der Meinung, dass wir hier unnötigerweise eine PUK und damit das schärfste Mittel der parlamentarischen Oberaufsicht eingesetzt haben, und diesen «Tolggen» müssen sich die bürgerlichen Parteien ins Reinheft schreiben lassen, sie, die ja sonst immer auf den sorgsamen Umgang mit unseren Steuergeldern bedacht sind. Denn mit dieser Messlatte könnten wir noch zu vielen Themen, die möglicherweise aktuell sind, Parlamentarische Untersuchungskommissionen einsetzen. Umso wichtiger ist es, dass der Regierungsrat nun vorwärtsmacht in der Informatik und die Empfehlungen der PUK entsprechend umsetzt. Die AL steht voll hinter diesen. Besten Dank.

Ratspräsident Beat Habegger: Damit haben alle Fraktionen gesprochen. Wir kommen jetzt zur Runde der weiteren Kantonsratsmitglieder.

Corinne Hoss-Blatter (FDP, Zollikon): Unser Fraktionspräsident hat die politische Einordnung des Berichts aus Sicht der FDP vorgenommen. Als Mitglied der PUK melde ich mich trotzdem auch noch ganz schnell zu Wort, auch wenn schon vieles gesagt ist.

Ich weise nochmals darauf hin: Der PUK-Bericht wurde einstimmig abgenommen, das müssen wir jederzeit vor Augen haben. Dass die Linke dies nun so interpretiert, dass der Regierungsrätin Jacqueline Fehr mit unserem PUK-Bericht die Absolution erteilt wurde, finde ich schwierig. Der SP-Votant und der Votant der AL gehen sogar so weit, dass sie ihr fast einen Heiligenschein umlegen. Der SP betrachtet die PUK als Rohrkrepierer und die AL moniert das herausgeschmissene Geld – das ist etwas schwierig.
Es ist tatsächlich so, dass die Verantwortung für den Datensicherheitsvorfall nicht bei Jacqueline Fehr liegt, aber natürlich für alles, was nach dem Bekanntwerden geschah oder eben nicht geschah. Sie informierte kaum – wir haben es gehört – über die Ergebnisse ihrer Administrativuntersuchung, ja, auch kaum darüber, dass sie nach dem Bekanntwerden des Vorfalls überhaupt eine solche veranlasst hatte. Als sie dies dann erwähnte, war dies im Zusammenhang mit einem anderen Geschäft, auch das haben wir schon gehört. Es geschah so beiläufig, dass die anderen sechs Regierungsräte und Regierungsrätinnen sich bei der Befragung durch die PUK gar nicht mehr erinnern konnten. Jacqueline Fehr kommunizierte verzögert und versuchte anfangs, das Datenleck unter den Teppich zu kehren. Aus meiner Sicht zeugt diese Vogel-Strauss-Politik zumindest nicht von kompetenter Führung.
Ergänzen möchte ich noch etwas, was mich seit November umtreibt: Regierungsrätin Fehr machte in der Debatte zum IDG am 24. November 2025 eine erschreckende Aussage. Da wurde der Datenschützerin Blaming unterstellt. Nein, Frau Fehr, nicht direkt, das machen Sie auch sehr clever, aber im Zusammenhang mit Ihrer Aussage musste das so abgeleitet werden, indem Sie sagten, Zitat: «Es käme uns nie in den Sinn, unsere Aufsichtstätigkeit unter dem englischen Schlagwort ‹Blaming›», also Anklage, zu verstehen.» Sie sprachen dabei über Ihre Aufsicht über die Gemeinden. Wenig später sagten Sie dann, und ich zitiere noch einmal: «Einen etwas anderen Stil hat der Datenschutzbeauftragte.» Ziemlich respektlos, muss ich sagen. Und wenn dies die Zusammenarbeit zwischen Regierung und Datenschutzbeauftragten widerspiegelt, ist es schlecht bestellt um die Zukunft der Datensicherheit in unserem Kanton. Auch wenn die Stellungnahme, die die Regierung gestern zum PUK-Bericht veröffentlicht hat, aussagt, dass der Regierungsrat unsere Empfehlungen sehr ernst nehmen werde, dann, so hoffe ich doch sehr, nicht auf der Grundlage der Aussage von Regierungsrätin Fehr.

René Isler (SVP, Winterthur): Zwei Sachen haben mich jetzt gestört. Es geht da nicht um eine Person, aber um zwei Sachen, und da muss ich auch dem Herrn Regierungspräsidenten in seinem Votum widersprechen, oder sonst haben Sie sich falsch ausgedrückt. Es kann sein oder es wird so sein, dass in Sachen Strafverfolgungsbehörden beziehungsweise Strafuntersuchungsbehörden keine heiklen Daten in die Öffentlichkeit geraten sind. Was aber nicht wahr ist, und das wissen wir alle auch von unseren Polizeiverbänden: Stellen Sie sich vor, 2022 wurde ich von einer mir nicht bekannten Journalistin einer sehr grossen Tageszeitung an einem Sonntagabend kontaktiert. Und die konnte mir sämtliche Daten,

meine persönlichen Berufsdaten, übermitteln, die nirgends öffentlich niedergeschrieben sind. Ich hatte mal als Polizeischulleiter der Stadtpolizei Winterthur bei der Kantonspolizei Zürich in einem besseren Abstellbüro eine interne Telefonnummer, auch diese hat die Journalistin gewusst. Also sind doch dort Daten hinausgegangen, was für mich aus persönlicher Betroffenheit für gewisses Befremden gesorgt hat. Dass so ganz und gar nichts an die Öffentlichkeit gelangt sei, so ist es also nicht.
Ich weiss bis heute nicht – und dazu macht auch der PUK-Bericht keine Angaben –, wie dann diese Daten zu diesen Stellen, auch zu den Medien gelangt sind. Das ist mal Punkt 1.
Punkt 2 ist: Wenn ich meinem lieben, sonst sehr, sehr geschätzten Kollegen von der Sozialdemokratischen Partei *(gemeint ist Davide Loss)* anhöre, könnte man meinen, niemand habe zu keiner Zeit etwas falsch gemacht. Ich glaube, da sind wir uns einig, dass dem eben nicht so ist. Das Problem ist doch einfach, dass man das irgendwann erkannt hat und dann ganz lange eigentlich gar nicht recht gewusst hat, was wir jetzt damit machen. Welche Daten sind raus? Und da reden wir von einem Zeitfenster von fast zehn Jahren. Selbstverständlich war die Urheberin nie die betreffende, die heutige Justizdirektorin, absolut nicht, da sind wir uns alle einig. Aber von dem Moment an, als man merkte oder wissentlich gewusst hat, dass da irgendetwas mal falsch gelaufen ist, bis zu dem Zeitpunkt, bis 2022, bis uns die Medien und die andere dunkle Person *(gemeint ist Roland Gisler, der im Besitz der unsachgemäss entsorgten Daten war)* in Oerlikon *(damals Tagungsort des Kantonsrates)* uns den ganzen «Prägel» vor die Füsse geworfen haben, in dieser Zeitspanne hätte man ganz sicher früher intervenieren müssen – seitens der Gesamtregierung selbstverständlich. Und das ungute Gefühl bleibt nach wie vor. Ich bin mir nicht sicher, welche Daten heute noch irgendwie und irgendwo in dunklen Kanälen herumschwirren. Vielleicht weiss das der Sicherheitsdirektor *(Regierungsrat Mario Fehr)* besser, aber es gibt tatsächlich Medienschaffende und es hat bis 2022 Medienschaffende von ganz grossen Tageszeitungen gegeben, die von Personen, von betroffenen Polizistinnen und Polizisten des gesamten Kantons Zürich, Daten hatten, Geschäftsdaten notabene, und das gibt einfach ein sehr ungutes Gefühl. Und hier einfach alles hinzustellen, wie wenn das Friede, Freude, Eierkuchen wäre, meine Damen und Herren, so ist es auch nicht. Und am Ende des Tages, immer am Ende des Tages, ob nun Ursache, Verursacher oder nicht, wenn irgendjemand einer Direktion vorsteht, egal wer das ist, am Ende des Tages muss diese Person die Verantwortung tragen und sich auch hinstellen und sagen können «Das haben wir so vielleicht auch nicht gut gemacht» oder «Wir wissen es bis heute noch nicht ganz genau, welche Daten irgendwo noch deponiert sind». Also so viel Ehrlichkeit und so viel Sachlichkeit braucht es einfach am Ende des Tages.

Beatrix Stüssi (SP, Niederhasli): Ich nehme kurz Replik zu meinem Vorredner: Es geht um die Daten. Die Justizdaten sind zu jener Zeit wohl die bestgeschützten Daten überhaupt gewesen. Sie waren verschlüsselt, weswegen man auch sehr lange davon ausging, dass diese nicht aus den Geräten geholt werden können und

auch bis jetzt nicht aus den Geräten geholt werden konnten. Es ist auf jeden Fall nicht bekannt, dass irgendwo Daten noch öffentlich sind.
Aber nun zu meinem Votum: Eine PUK ist ein starkes Instrument der parlamentarischen Kontrolle und sollte nicht zum Wahlkampfmittel werden. Das beschädigt das Vertrauen in unsere Institutionen und verursacht hohe Kosten, wie wir gemerkt haben, weswegen wir dem Einsatz der PUK vorerst abgeneigt gegenüberstanden. Trotzdem anerkenne ich im aktuellen Fall den Mehrwert einer Behandlung durch eine PUK, weil diese sehr viel umfassender recherchieren und ermitteln und schlussendlich Mängel aufzeigen konnte. Ich hoffe, nein, ich gehe davon aus, dass der Bericht und die darin formulierten Empfehlungen mehr Gewicht haben, als es bislang die mahnenden Berichte und Empfehlungen von Datenschützenden, GPK und Finanzkontrolle je hatten. Es ist also klar und zwingend notwendig, dass der Regierungsrat die unmissverständlich aufgezeigten Empfehlungen zur Organisation der kantonalen IT zügig koordiniert umsetzt. Es ist nicht zielführend, auch nicht angebracht, Schuldzuweisungen zu machen, welche keiner Grundlage entsprechen. Wir brauchen jetzt endlich eine solide gemeinsame IT- und IT-Sicherheitsstrategie, für deren Umsetzung auch die Ressourcen gesprochen werden müssen. Der Kantonsrat ist gefragt, die geeigneten Instrumentarien und das notwendige Controlling dafür einzurichten und mit den entsprechenden Kompetenzen auszustatten. Nur so lässt sich eine Wiederholung einschränken, nicht verhindern, wir haben es gehört. Der PUK-Bericht – wir haben auch das mehrfach gehört – wurde einstimmig gutgeheissen. Die SP wird die Auflösung der PUK und den Bericht mit den Empfehlungen genehmigen und erwartet dies dementsprechend von allen Parteien.

Gabriel Mäder (GLP, Adliswil) spricht zum zweiten Mal: Ich komme gerne in meinem zweiten Votum noch kurz auf meine Stellungnahme zum Bericht des Regierungsrates von gestern Abend zurück: Der Regierungsrat kommt ja zu einer insgesamt positiven Selbsteinschätzung. Er attestiert sich sinngemäss ein «gut» und verweist ausführlich auf die zahlreichen Massnahmen, die seit dem Datenträgervorfall ergriffen wurden. Diese Fortschritte sind tatsächlich real und sie sind wichtig, das anerkennen wir ausdrücklich, aber, geschätzter Regierungsrat, Selbsteinschätzungen ersetzen keine unabhängige Beurteilung. Gerade in einer Zeit, in der politische Selbstzuschreibungen inflationär gebraucht werden, ist Zurückhaltung angebracht. Entscheidend ist nicht, was geschaffen wurde, sondern was wirkt, insbesondere dann, wenn es ernst wird. Und hier bleibt der Bericht des Regierungsrats aus Sicht der Grünliberalen hinter den Erkenntnissen der PUK zurück, auch wenn es einige Lichtblicke gibt, so zum Beispiel beim Weisungsrecht, das ich positiv vernommen habe. Sofern ich den Ausführungen des Regierungsratspräsidenten richtig zugehört habe, soll nun doch ein Weisungsrecht des ISIK geprüft werden, das hatte ich so aus dem Bericht noch nicht geschlossen. Aber ja, die Thematik scheint sehr dynamisch zu sein, das ist natürlich zu begrüssen.
Auch die Absicht, die Finanzkontrolle entlasten zu wollen und eine externe Zertifizierungsstelle mit den Überprüfungen zu beauftragen, ist prüfenswert. Stirn-

runzeln hingegen bereitet weiterhin das Direktions- und Silo-Denken. Der Regierungsrat anerkennt dieses Problem, relativiert es aber zugleich mit dem Hinweis auf unterschiedliche Aufgaben und Besonderheiten einzelner Bereiche, etwa der Polizei. Unterschiedliche Aufgaben rechtfertigen unterschiedliche Umsetzungen, was jedoch weiterhin offenbleibt, ist die entscheidende Frage: Wer entscheidet verbindlich, wann die Differenzierung sachlich geboten ist und wann sie zur Blockade gesamtkantonaler Standards wird? Solange diese Entscheidung faktisch bei den Direktionen verbleibt, bleibt die Gesamtsteuerung schwach. Und es stellt sich die Frage, ob dies wirklich schon der angesprochene Kulturwandel ist, den auch Ratskollege Davide Loss eingefordert hat.
Kritisch zu würdigen ist auch der Vorwurf an den Kantonsrat und die STGK unter Punkt 5.5 der Stellungnahme: Die Darstellung, wonach durch das Nicht-Eintreten auf die Vorlage zu den elektronische Basisdiensten *(Vorlage 5985)* ein zentrales Gesetz weggefallen sei, greift zu kurz. Tatsache ist, dass es der zuständigen Direktion nicht gelungen ist, eine Mehrheit der Kommission vom Nutzen dieser Vorlage zu überzeugen, handelt es sich doch um ein weitgehend fakultatives Gesetz mit zahlreichen Kann-Formulierungen. Wie damit ein wirksamer Durchgriff hätte erreicht werden sollen, bleibt offen, wir werden das zu einem späteren Zeitpunkt besprechen. Aber der Datenvorfall ist kein Ausdruck von zu wenigen Gesetzen, sondern von schwacher Governance. Und vor diesem Hintergrund wirken die Bemühungen zur Einführung einer Aufsichtskommission zur Digitalisierung im Kantonsrat dringender denn je. Besten Dank.

Davide Loss (SP, Thalwil) spricht zum zweiten Mal: Ich möchte gerne noch auf ein paar Voten replizieren, zunächst zu Karl Heinz Meyer: Es ist beim Projekt «Helium», das Sie angesprochen haben, nicht etwa so, dass der Kanton hier einfach vorpreschen würde und irgendetwas mal aufs Gratwohl entwickelt. Das Projekt «Helium» ist ein notwendiges Projekt, weil nämlich der Kanton Zürich den Anschluss an die Plattform «justitia.suisse» gewährleisten muss. Das ist eine Plattform, die der Bund im Rahmen des Projekts «Justitia 4.0» vorschreibt, und der Kanton muss hier sozusagen eine Dockingstation gewährleisten können, damit die Daten entsprechend übermittelt werden können.
Nun zu meiner geschätzten Kollegin Hoss: Ich weiss nicht, ob Sie in einer anderen Debatte waren als ich, aber ich habe auf jeden Fall keine Absolution an Regierungsrätin Jacqueline Fehr erteilt. Ich habe sie für die Kommunikation kritisiert, wie wir das im PUK-Bericht auch gemacht haben. Ich habe mich hier an den PUK-Bericht gehalten und habe einfach gesagt, dass man den Vorfall nicht politisch einzig Regierungsrätin Jacqueline Fehr in die Schuhe schieben kann – mehr nicht. Ich habe auch nicht gesagt, dass die PUK ein Rohrkrepierer war, da verdrehen Sie mir die Worte im Mund, im Gegenteil: Der PUK-Bericht ist, wie gesagt, ein solides Grundlagerwerk. Es hat sich gelohnt, dass wir hier viel Zeit und Energie investiert haben. Wir haben auch 50 Empfehlungen, nämlich wirklich umsetzbare, griffige Massnahmen abgegeben, und das ist alles andere als ein Rohrkrepierer. Ich habe lediglich gesagt, dass es vielleicht für einige anders herausgekommen ist, als sie das erwartet haben.

Bezüglich der Administrativuntersuchung, da gebe ich Ihnen recht, hätte besser informiert werden können. Es ist jedoch so, dass es sicherlich nicht die einzige Administrativuntersuchung in der kantonalen Verwaltung ist. Und es ist auch nicht so, dass wir über jede einzelne Administrativuntersuchung informiert würden, da gibt es sicher ganz viele in den verschiedenen Direktionen.
Nun zu René Isler: Ich habe ebenfalls nicht gesagt, dass nie jemand irgendetwas falsch gemacht habe, so ist das nicht. Wie gesagt, der Gesamtregierungsrat hat hier versagt. Er hätte mehr Sensibilität bezüglich der IT- und Informationssicherheit walten lassen und aus diesem Silo-Denken rauskommen müssen. Das ist das, was der PUK-Bericht kritisiert und wo er hier griffige Massnahmen fordert. Der Datenabfluss, den Sie hier erwähnt haben, sehr geschätzter Kollege Isler, hat nichts direkt mit dem Datensicherheitsvorfall in der Justizdirektion zu tun. Diese Daten können auch aus öffentlichen Quellen kommen, aus anderen Quellen im Internet et cetera. Es ist nicht erwiesen, dass dies auf den Datensicherheitsvorfall zurückzuführen ist. Und ich halte noch einmal fest, dass die Justizdirektorin Sie persönlich über diesen Datensicherheitsvorfall informiert hat, wenn auch nicht mit der notwendigen Vehemenz.
Ich halte fest: Dieser Schlussbericht wurde in der PUK einstimmig verabschiedet, das ist so. Wir haben einstimmig gesagt, dass der Regierungsrat diese Verantwortung stärker wahrnehmen muss. Hinter diesem Schluss stehen wir, wir stehen auch hinter jeder Silbe dieses Berichts.
Zur Stellungnahme des Regierungsrates, auf diese möchte ich noch kurz eingehen: Ich habe jetzt aus dem Votum des Regierungspräsidenten vernommen, dass man doch gewisse Punkte anschauen darf. Deshalb ist mein Fazit, dass man hier mit etwas angezogener Handbremse vorgehen will, aber doch ein bisschen einsieht, dass man aus diesem Silo-Denken herauskommen muss. Wichtig ist auch, dass man dem Informationssicherheitsbeauftragten ein Weisungsrecht einräumen muss. Die PUK hat 50 Massnahmen gefordert. Wir werden mit Akribie und Argusaugen darauf achten, wie diese Massnahmen umgesetzt werden. Diese Arbeit wird weitergehen, mit dem heutigen Bericht ist die Arbeit noch nicht getan. Dasselbe gilt natürlich für Sie, geschätzte Regierungsrätinnen und Regierungsräte. Besten Dank.

Karl Heinz Meyer (SVP, Neerach) spricht zum zweiten Mal: Ich möchte kurz auf Davide Loss und Manuel Sahli replizieren:
Davide Loss, ich habe nicht das Projekt «Helium» infrage gestellt, sondern das Projektmanagement macht mir Sorgen. 92 Millionen Franken sind eine Riesennummer, also für mich wenigstens, und da mache ich ein grosses Fragezeichen: Kommt das gut? Es ist ja nicht das erste Mal, dass in der JI ein Softwareprojekt strandet.
Und Manuel Sahli, du hast zu Recht die hohen Kosten beanstandet. Das ist richtig, eine halbe Million ist viel Geld. Wenn aber dieser PUK-Bericht nur einen ähnlichen Fall verhindern konnte – wir werden das wahrscheinlich nie wissen –, dann hat es sich gelohnt, mehr als gelohnt. Und wenn ich die Reaktion des Regierungsrates im RRB 41/2026 vom 14. Januar 2026 sehe, dann sehe ich im Gegensatz zu

Urs Dietschi schon eine gewisse Morgenröte, dass man gewisse Punkte bereits übernommen und auf den Weg gebracht hat. Also ich sehe das nicht so pessimistisch. Besten Dank.

Thomas Forrer (Grüne, Erlenbach): Was bleibt zum Schluss nach dieser langen Geschichte, die wir hier jetzt während Jahren in diesem Kantonsrat behandelt haben? Begonnen hat es im November/Dezember 2022 mit einem grossen Wahlkampfgetöse. Es hat mit Anfeindungen von rechts gegen eine Regierungsrätin begonnen. Und was haben wir zweieinhalb Jahre später von der PUK Datensicherheit bekommen? Einen sehr soliden und sachlichen Bericht. Und wir müssen den Mitgliedern der PUK Datensicherheit danken, dass sie ohne politische Voreingenommenheit, wie das bei gewissen Leuten im November und Dezember 2022 der Fall war, dass sie ohne politische Voreingenommenheit diese Untersuchung gemacht haben und uns hier jetzt sachliche, akribisch aufgearbeitete Fakten präsentieren. Diese Fakten hätten, Hand aufs Herz – nicht in dem Umfang selbstverständlich –, zu einem grossen Teil auch durch die GPK aufgearbeitet werden können. Wir haben dafür 800'000 Franken bis ungefähr 1 Million Franken ausgegeben; wir werden noch sehen, wie viel genau, aber in dem Rahmen liegt es. Die SVP, die an vorderster Front für diese PUK gekämpft hat – mit Wahlkampfabsichten, muss man immer wieder betonen –, die SVP war bereit, dieses Geld für diesen Bericht auszugeben. Wenn ich die Empfehlungen in Kapitel 18 anschaue, dann müssen Sie selber mit sich ins Reine kommen, ob diese durchaus wichtigen, nachzuahmenden und zu befolgenden Empfehlungen 1 Million Franken wert sind; das müssen Sie selber wissen.
Was ich sagen kann, und das ist mir wichtig: Wir erfahren – und das wurde hier häufig gesagt –, wir erfahren in diesem Bericht, dass Regierungsrätin Jacqueline Fehr besser hätte kommunizieren können. Aber Hand aufs Herz, das wussten wir schon im November 2022, da hat uns die PUK gar nichts Neues gebracht. Das Neue sind die Empfehlungen in Kapitel 18. Jacqueline Fehr – und das lesen wir in dem Bericht – hat sich entschuldigt und die Fehler rasch eingeräumt, und es wurde auch im PUK-Bericht, der in der Kommission einstimmig angenommen worden ist, breit anerkannt, dass dies geschehen ist. Wir müssen also sagen, und das ist mir eigentlich wichtig: Sie von der SVP können jetzt zeigen, dass Ihnen dieser Bericht nicht nur ein Wahlkampfgetöse wert war, sondern Sie können jetzt zeigen, dass Sie auch bereit sind, die Empfehlungen in Kapitel 18 mit umzusetzen. Es ist einfach, nur der Regierung zu sagen «Machen Sie, machen Sie jetzt, wir wollen das jetzt!» und so weiter. Sie haben in der ganzen Debatte noch nicht gefragt, was diese Empfehlungen in Kapitel 18 dann kosten, wenn wir sie umsetzen. Und da bitte ich Sie und da werden Sie dann zeigen können, wie ernst es Ihnen mit diesem ganzen Bericht ist. Wenn Sie bereit sind, den Stacheldraht aus Ihrem Portemonnaie zu nehmen, liebe SVP, und dann auch wirklich das Portemonnaie zu öffnen und die Gelder, die für die Umsetzung der Empfehlungen nötig sind, zu bewilligen, dann haben Sie gezeigt, dass Ihnen dieser Bericht mehr wert ist als Wahlkampfgetöse. Wir werden Sie daran messen, wenn es darum geht, wenn es um Franken und Rappen geht. Und wir werden Sie daran erinnern, ob diese

800'000 Franken bis 1 Million Franken Ihnen tatsächlich so wichtig sind und ob dieser Bericht tatsächlich so wichtig ist, dass Sie dann die Empfehlungen auch umsetzen und Geld in die Hand nehmen wollen. Wir werden sehen. Sie können selber zeigen, wie ernst Ihnen die ganze Sache tatsächlich ist.

René Isler (SVP, Winterthur) spricht zum zweiten Mal: Jetzt ist aber irgendwann der Zapfen ab. Für dieses Geschäft braucht es weiss Gott nicht mehr Geld, sondern da braucht es schlicht und ergreifend etwas Verstand. Wenn Sie ja wissen, woher dieser Datenmissbrauch kommt, dann halte ich mal dieses Handy rauf *(der Votant zeigt sein Telefon)*, nur ein Handy, auch nach oben zur Zuschauertribüne. Wer von uns würde dieses Handy irgendwo in einem Shop hinlegen und sagen «Ich nehme jetzt ein neues, machen Sie den Datentransfer», und dann laufe ich aus diesem Haus hinaus, ohne dass ich das Handy zuvor wieder in die Werkseinstellungen zurückgesetzt hätte? Da braucht es nicht Intelligenz, da braucht es kein Geld, da braucht es schlicht und ergreifend etwas Verstand, auch 2021. Mit ein bisschen Verstand wäre es gar nie zu diesem Datenmissbrauch gekommen, es hätte einfach intern jemand diese Daten so vernichten müssen. Man kann jedes Laufwerk extern, intern oder in einer Wolke, Sie oder alle, die berechtigt sind, können diese Daten ein für alle Mal löschen, aber sicher nicht einfach aus der Hand geben und sagen «Machen Sie dann mal!», und das ohne Leistungsvereinbarung. Da braucht es nicht mehr Geld, da braucht es einfach etwas Sachverstand, so sagen wir dem.

Lorenz Habicher (SVP, Zürich): Es wird an der Zeit sein, dass man als einer, der im Dezember 2022 tatkräftig dahinterstand, dass etwas geht, auch wieder das Wort ergreift. Thomas Forrer spielt auf Valentin Landmann an, das hat er schon immer getan, das hat er auch im Frühjahr 2023 getan. Thomas Forrer war auch immer der Meinung, dass eine Subkommission der GPK das Geschäft hätte erledigen können. Vielleicht wäre der Bericht auch so umfangreich gewesen, vielleicht wäre die GPK-Subkommission jetzt noch am Arbeiten. Wir wissen, dass die ABG *(Aufsichtskommission für Bildung und Gesundheit)* auch schon einen schönen Bericht gemacht hat *(gemeint ist der Bericht über die Untersuchung zu besonderen Vorkommnissen an mehreren Kliniken des Universitätsspitals Zürich, KR-Nr. 58/2021)*. Er hatte dann 78 Empfehlungen, die man auch umsetzen musste. Wir können natürlich jetzt nicht mehr darüber sprechen, was besser und was schlechter gewesen ist, aber wir wissen, dass das, was jetzt hier vorliegt, schon ein bisschen Fleisch am Knochen hat. Ich zweifle aber daran, dass von 180 Kantonsratsmitgliedern, die diesen Bericht im Dezember 2025 bekommen haben, auch 180 Mitglieder diesen Bericht gelesen oder zumindest hineingeschaut haben. Daran zweifle ich. Und ich glaube, ich darf auch an der Aussage von Manuel Sahli zweifeln, dass es nichts Neues gebracht hat. Manuel Sahli, der selbst Präsident der Subkommission der GPK werden wollte, um es aufzuarbeiten, der selbst Mitglied in dieser PUK ist, sagt plötzlich: «Es hat ja nichts Neues gebracht. Man hat ein paar Sitzungen gemacht, man hat ein bisschen Geld verdient.» Finde ich Manuel Sahli nicht in diesem Bericht? Oder soll ich die Seiten aufrufen, wo Manuel

Sahli etwas beigetragen hat? Ich denke, wir haben es gut gemacht und sollten jetzt weiterschauen und weiterarbeiten. Und dann ist der Punkt, nicht sofort nach Geld zu schreien, sondern zuerst muss man wissen, wie wir weiterschreiten. Wir haben es von der Regierung gehört, sie will eine Strategie vorlegen, sie hat eine Idee und die wird sie uns präsentieren. Und wir können danach darüber berichten oder befinden, was es dann kostet und was wir bereit sind zu bezahlen. Wichtig ist, dass wir, wenn wir jetzt die IT-Kosten in allen Direktionen anschauen – und diese explodieren schon heute –, dass wir das Ganze in den Griff bekommen. Und dieser Bericht kann auch dort helfen, dass nicht jede Direktion die IT ausbaut und macht, was sie möchte. Insofern Silo-Denken aufgeben, weitermachen.
Für mich ist das Wichtigste an der ganzen Sache, was Martin Hübscher *(Altkantonsrat und Nationalrat)* an der 9. Sitzung dieser Legislatur am 3. Juli 2023 gesagt hat, er war nämlich der Erstunterzeichner der dringlichen Interpellation 462/2022. Und er hat sein Votum dort eröffnet mit: «Wissen Sie, was das höchste Gut eines Staates ist? Es ist das Vertrauen der Bevölkerung in den Staat.» Und wenn wir mit diesem Bericht und dieser Aufarbeitung wieder ein bisschen Vertrauen herstellen können, dann hat es sich gelohnt. Ich danke Ihnen.

Yiea Wey Te (FDP, Unterengstringen): Ich halte mich ganz kurz. Es wurde in der Debatte verschiedentlich der Eindruck erweckt oder gesagt, dass die PUK eine reine Gegenkampagne gegen ein einzelnes Regierungsratsmitglied sei. Das ist falsch, das ist schlichtweg falsch. Es kann sein, dass gewisse Mitglieder des Rates in diese Richtung gesprochen haben, aber das entspricht einfach nicht der Aufgabe der PUK. Die Aufgabe der PUK war klar beschrieben, klar definiert, und da kann man lesen, was die PUK hätte machen sollen und auch gemacht hat. Ich möchte an dieser Stelle klar festhalten: Die politische Aufarbeitung des Datensicherheitsvorfalls ist eine zentrale Aufgabe des Kantonsrates. Dafür gibt es oder deshalb existieren die Aufsichtsinstrumente. Wenn wir beginnen, diese Aufgabe schlechtzumachen, diese Aufgabe zu delegitimieren, dann müssten wir uns konsequenterweise auch fragen, ob es die GPK überhaupt noch braucht, ob wir diese Kommission noch brauchen. Und ich sage: Ja, wir brauchen sie, denn Aufsicht ist kein Misstrauensvotum, sondern eine Kernfunktion dieses Parlaments. Und die PUK hat eine super Arbeit gemacht. Und mit dem Bericht, mit den notwendigen Vorschlägen, mit denen müssen wir jetzt arbeiten und sicherstellen, dass die kantonale IT sicherer wird. Besten Dank.

Manuel Sahli (AL, Winterthur) spricht zum zweiten Mal: Wir hören hier relativ viele Phrasen vonseiten der SVP. Der eine will die ganze Informatiksicherheit mit ein wenig Verstand betreiben, Geld braucht es hierfür offenbar nicht, das Ganze soll sich wohl aus der uneigennützigen Motivation der Angestellten des Kantons nähren, damit das alles funktioniert. Der andere attackiert mich ein wenig. Ja, in Sachen Datensicherheitsvorfall und mit diesem Hintergrundgedanken, gepaart mit den Attacken gegen Frau Regierungsrätin Fehr, haben Sie diese PUK eingesetzt. Und genau unter diesen Gesichtspunkten, dem Datensicherheitsvorfall und

diesen ganzen Attacken, muss man klar sehen, dass sich hier nicht viel bewahrheitet hat. Ich habe nicht gesagt, dass wir nichts hervorbracht haben, sonst wäre mein Votum zuvor, mein Eintretensvotum, nicht so lang gewesen. Wir haben sehr wohl, die PUK hat sehr wohl 50 Empfehlungen in ihren Bericht gebracht, sie hat gründlich gearbeitet und hier sehr wohl einen guten Bericht abgeliefert, mit dem wir hier auch arbeiten können. Aber man muss sich trotzdem wieder fragen: Wäre es auch anders gegangen? Und da denke ich: Ja, es wäre anders gegangen, vor allem wenn man sieht, wofür diese PUK eingesetzt wurde und was dabei herausgekommen ist.

Regierungspräsident Martin Neukom: Herzlichen Dank für diese Debatte und die Würdigung. Die FDP hat sich offensichtlich zum Ziel gesetzt, kein Bashing zu betreiben, das hat uns sehr gefreut. Ob das gelungen ist, lassen wir an dieser Stelle unbeantwortet *(Heiterkeit)*.
Zu den Vorfällen in der Vergangenheit: Schauen Sie, 2002, das ist 24 Jahre her. Es sieht vielleicht nicht so aus, aber von den hier anwesenden Regierungsmitgliedern ist keines schon 24 Jahre dabei. Im Jahr 2002 hatte ich gerade mit meiner Lehre begonnen, das heisst zu diesen Vorfällen in der Vergangenheit können wir nicht wahnsinnig viel beitragen oder sagen. Wir können sie zur Kenntnis nehmen und wir können versuchen, Lehren daraus zu ziehen, sofern es überhaupt noch möglich ist, daraus Lehren zu ziehen, weil sich, wie ich gesagt habe, die Fragestellung um die IT-Sicherheit in den letzten 20 Jahren massiv verändert hat.
Es wurde kritisiert, dass der Kanton Zürich aus sieben Königreichen bestehe. Wenn Sie dann an dieser Deutung festhalten wollen, dann müssen Sie doch mindestens anerkennen, dass diese sieben Königreiche untereinander einen Friedensvertrag geschlossen haben und sich zumindest sehr viel Mühe geben, sehr gut zusammenzuarbeiten. Die deutlichste Kritik hat eigentlich den Zeitpunkt betroffen, zu dem wir Ihnen diesen Regierungsratsbeschluss zugestellt haben. Das hat uns jetzt etwas überrascht, ehrlich gesagt, weil wir Ihnen mit diesem Zeitpunkt entgegengekommen sind. Grundsätzlich wäre das so geplant gewesen wie bei einer dringlichen Interpellation, dass ich Ihnen hier vortrage, was die Haltung der Regierung ist, und dann nach meiner Rede der RRB veröffentlicht wird. Wir dachten aber, dass das für Sie etwas schwierig ist, diese zwölf Seiten dann während der Ratsdebatte zu studieren, und haben uns darum entschlossen, Ihnen den RRB frühzeitig zuzustellen, und auch gleich dem gesamten Rat, also nicht nur den Mitgliedern der PUK, damit Sie sich vorbereiten können. Wenn wir diesen RRB jetzt natürlich schon am Donnerstag zugestellt hätten, dann wäre wahrscheinlich die mediale Berichterstattung nicht heute erfolgt, sondern schon letzte Woche, und das wäre vermutlich nicht in Ihrem Sinn gewesen. Deshalb haben wir im Glauben, dass Sie das so befürworten, Ihnen den RRB am Sonntagabend zugestellt, sodass Sie es nicht schon heute Morgen in der Zeitung lesen, sondern erst morgen früh, also haben wir hier eigentlich in Ihrem Sinne gehandelt.
Damit kann ich schliessen. Ich danke nochmals der PUK für ihre Arbeit. Die PUK ist jetzt beendet. Die Diskussionen um die Weiterentwicklung der Datensicherheit im Kanton Zürich werden sicher noch fortgeführt werden. Besten Dank.

Benno Scherrer (GLP, Uster), Präsident der PUK Datensicherheit: Zuerst einmal danke ich Ihnen persönlich für die Diskussion und als Präsident der PUK danke ich dem Regierungsrat für die Stellungnahme zu unseren Empfehlungen.
Wir müssen darauf setzen, dass die Informationssicherheit in der kantonalen Verwaltung nun wirklich die Bedeutung hat, die dem Thema angemessen ist, und gerade auch im Hinblick auf Angriffe von Cyberkriminellen, wie das der Regierungspräsident erwähnt hat, alles Notwendige unternommen wird, um solche zu verhindern, zu unterbinden, dass aber auch das grosse Bild nicht vergessen geht, gerade auch, weil der Staat digitaler unterwegs ist. Die Kriminellen ruhen nicht, auch der Kanton darf sich keinesfalls ausruhen, um grösste Sicherheit zu gewährleisten.
Der Regierungsrat hat es richtig gesagt, wir sagen das auch: Informationssicherheit ist eine Daueraufgabe, es ist eine Kernaufgabe und es ist eine Gemeinschaftsaufgabe. Die PUK Datensicherheit begrüsst es, dass der Regierungsrat gewillt ist, die noch offenen Empfehlungen auch mit dem Kantonsrat in aller Offenheit zu prüfen.
Bezüglich Silo-Denken darf ich erfreut feststellen, dass der Begriff auch von der Regierung aufgenommen wurde und hoffentlich zu vertieften Diskussionen anregt. Wir haben in der Kommission dieses Denken immer wieder festgestellt, und es bestätigt sich halt auch zum Teil bereits im Regierungsratsbeschluss schon wieder, indem nämlich gleich wieder Gründe vorgebracht werden, weshalb eine konsequent durchgehende Anwendung, eine konsequent übergreifende Anwendung eben doch nicht gehen würde. Hier empfehlen wir dringend, nicht aufgrund der Unterschiede in den Direktionen nach den Ausnahmen für die eigenen Silos zu suchen, sondern die vertiefte Auseinandersetzung mit den Gemeinsamkeiten zu stärken.
Die Empfehlung bezüglich der Zuordnung des AFI sollte ebenfalls nochmals weitergedacht werden. Wir haben sie als PUK bewusst offen formuliert, und möglicherweise ergibt sich mittelfristig eine neue Idee, so wie das im Satz, Zitat, «Prüfenswert erscheinen dem Regierungsrat hingegen vertiefte Überlegungen dazu, wie die Koordination, die Zusammenarbeit und die Steuerung ganzheitlicher erfolgen könnten» angedacht wird. Wir sind der Ansicht, dass gerade eine gesamtkantonale Steuerung nur eine gesamtkantonale Steuerung dem, wiederum Zitat, «Anspruch auf eine wirksame und wirkungsvolle Leistungserbringung» gerecht wird.
Die PUK Datensicherheit begrüsst auch, dass der Regierungsrat das Gefüge nun vereinfachen und harmonisieren möchte, und wir sind gespannt auf die erneute Informationssicherheitsstrategie. Auch bei dieser Strategie wird die Umsetzung entscheidend sein. Es darf nicht noch einmal vorkommen, dass zwar eine Strategie formuliert wird, dann aber der konkreten Umsetzung einer solchen Strategie nicht das nötige Gewicht verliehen, nicht die nötige Aufmerksamkeit geschenkt wird. Wir sind auch gespannt auf die angedachte Verordnung über die Informations- und Kommunikationstechnologie in der kantonalen Verwaltung. Und auch

bezüglich der Zuständigkeiten für die IKT und die Kompetenzen für das AFI im Bereich der Grundversorgung warten wir auf die Details.
Bezüglich der Verordnung der AISR als Weisung gehen die Ansichten von PUK Datensicherheit und Regierungsrat anscheinend noch auseinander, wobei mit der neuen IKTV und IVSV neu auch Regelungen auf Verordnungsstufe, wie von uns eben angeregt, vorgesehen sind. Wir sehen, dass diesbezüglich Überlegungen gemacht worden sind, und regen nun an, diese nochmals vertieft zu prüfen. Und erfreut nehmen wir und nimmt der Rat zur Kenntnis, dass der ISIK gestärkt werden soll und dass er eine starke Position bekommt. Wir haben ja dezidiert gefordert, dass der ISIK organisatorisch so angegliedert werden soll, dass er mit einem Weisungsrecht ausgestattet werden kann. Hier sehen wir in der Stellungnahme, die uns vorliegt, erfreulicherweise eine grössere Offenheit für diese Frage als noch in den Befragungen durch die PUK. Der Regierungspräsident hat auch hier diese Überlegungen dargelegt. Auch die Positionierung der ISID wurde in unserem Sinne hier vom Regierungspräsidenten erwähnt.
Erfreulich auch, dass der Regierungsrat die Anregungen bezüglich der Risiken bei Cloud-Anwendungen ernst nimmt. Auch für uns war diese Diskussion nicht abgeschlossen, weshalb wir uns für eine differenzierte, ergebnisoffene Anregung entschieden haben, die der Regierungsrat nun ebenfalls aufgreift. Hier ist wirklich, wie angeregt, eine vertiefte Auseinandersetzung notwendig, in der Debatte wurde das bereits schon angesprochen.
Noch ein Wort zu den Administrativuntersuchungen: Hier hat die PUK ein unterschiedliches Verständnis davon festgestellt, was Administrativuntersuchungen eigentlich sind. Und wir bemängeln eben, dass diese nicht genügend zur Kenntnis gebracht werden, deshalb unsere Empfehlung 42. Wir erachten es als dringend notwendig, dass der Regierungsrat über laufende Administrativuntersuchungen, welche über rein personalrechtliche Abklärungen von geringer Tragweite hinausgehen, in geeigneter Form informiert.
Nun, wir haben ja durchaus intensiv debattiert, und es ist wohl ein Zeichen für die Arbeit und die differenzierte Ausformulierung des Berichts, dass die Kommission diesen einstimmig verabschieden konnte, obwohl Interpretationen und Schlussfolgerungen von den Fraktionen divergent gesehen werden können. Die PUK steht einstimmig hinter den Forderungen. Und ich als Präsident bin überzeugt davon – und ich nehme an, die PUK-Mitglieder teilen diese Ansicht –, dass eine GPK oder eine GPK-Subkommission nicht in dieser Tiefe hätte Abklärungen machen können, und das nicht nur aufgrund der mangelnden Möglichkeiten, sondern schlicht aufgrund der zeitlichen und auch finanziellen Ressourcen. Im Bericht in Kapitel 3.2 ist die Zahl detailliert ausgewiesen: Es sind 570'000 Franken, die diese PUK gekostet hat, nicht 800'000 Franken, nicht 1 Million, wie das gerne kolportiert worden ist, und diese 570'000 Franken umfassen alles, von Sitzungsgeldern über Berichterstattung, über Protokollführung und so weiter und so weiter, 570'000 Franken.
Ich bin überzeugt, dass die breite Auslegeordnung wichtig ist. Sie hat auch einen historischen Aspekt, und für mich als Historiker war das jetzt noch eine schöne Sache, nochmals historisch arbeiten zu können. Ich hätte selber grosse Lust, die

Stellungnahme mit der PUK Datensicherheit und Vertretern der Regierung und Spezialisten der Verwaltung noch einmal vertieft zu diskutieren. Das wird leider nicht mehr möglich sein, weil heute, jetzt der Beschluss gefasst wird, dass die PUK Datensicherheit ihre Arbeit getan hat und aufgelöst werden kann. In diesem Sinne nochmals ein herzliches Dankeschön an alle für ihr Vertrauen und für die Mitarbeit.

Ratspräsident Beat Habegger: Mit dem Votum des PUK-Präsidenten haben wir den Bericht der Parlamentarischen Untersuchungskommission durchberaten.

Detailberatung

I.–V.

Keine Wortmeldung, so genehmigt.

Ratspräsident Beat Habegger: Ich danke den Mitgliedern der PUK, auch dem Präsidenten und allen Mitarbeitenden der Parlamentsdienste für ihre umfangreiche und wertvolle Arbeit. Ich danke auch den Mitgliedern des Regierungsrates für ihre Unterstützung bei den Untersuchungen und dass sie sich heute Morgen die Zeit genommen haben, dieser Debatte hier beizuwohnen.

Das Geschäft ist erledigt.

Ratspräsident Beat Habegger: Bevor wir mit den nächsten Traktanden weiterfahren, habe ich eine erfreuliche Mitteilung zu machen: Unser Kollege Tobias Weidmann hat heute Geburtstag. Herzliche Gratulation. *(Applaus)*