

Beschluss des Kantonsrates über die Einsetzung einer Parlamentarischen Untersuchungskommission

(vom)

Der Kantonsrat,

nach Einsichtnahme in den Bericht und Antrag der Geschäftsprüfungskommission vom 27. April 2023 sowie in die Stellungnahme des Regierungsrates vom 20. April 2023,

beschliesst:

Minderheitsantrag Davide Loss, Leandra Columberg, Manuel Kampus und Manuel Sahli:

Auf den Antrag wird nicht eingetreten.

I. Es wird gestützt auf §§ 115 ff. des Kantonsratsgesetzes eine Parlamentarische Untersuchungskommission eingesetzt.

II. Gegenstand der Parlamentarischen Untersuchungskommission sind die Vorkommnisse rund um den mit der Anfrage KR-Nr. 456/2022 und der Interpellation KR-Nr. 462/2022 öffentlich bekannt gewordenen Datensicherheitsvorfall bei der Direktion der Justiz und des Innern und allfälligen weiteren kantonalen Stellen.

- Die Untersuchungskommission hat insbesondere zu untersuchen,
- über welchen Zeitraum sich der Datensicherheitsvorfall ereignet hat, wer ihn zu verantworten hat und wann der Regierungsrat und die direkt betroffenen Direktionen davon Kenntnis erhalten haben;

* Die Geschäftsprüfungskommission besteht aus folgenden Mitgliedern: Beat Habegger, Zürich (Präsident); Hans-Peter Amrein, Küsnacht; Leandra Columberg, Dübendorf; Edith Häusler, Kilchberg; Corinne Hoss-Blatter, Zollikon; René Isler, Winterthur; Manuel Kampus, Schlieren; Gregor Kreuzer, Zürich; Davide Loss, Thalwil; Romaine Roggenmoser, Bülach; Manuel Sahli, Winterthur; Sekretär: Christian Hirschi.

- ob der Regierungsrat und die direkt betroffenen Direktionen zweckmässig, zeitnah und rechtmässig auf den Datensicherheitsvorfall reagiert und angemessen darüber informiert haben;
- ob der Regierungsrat, die direkt betroffenen Direktionen und weitere zuständige kantonale Stellen und Behörden zeitnah die nötigen Schritte unternommen haben, um den Datensicherheitsvorfall aufzuarbeiten und sicherzustellen, dass ähnliche Vorfälle verhindert werden können;
- wie die Entsorgung von Datenträgern im fraglichen Zeitraum in den Direktionen geregelt war, besonders in Bereichen mit sensitiven Daten;
- ob die notwendigen Vorkehrungen getroffen worden sind, damit ein ähnlicher Datenmissbrauch künftig verhindert werden kann;
- ob der Regierungsrat sich der Problematik der Datensicherheit und Entsorgung von Datenträgern bewusst war sowie rechtzeitig und vorausschauend im Rahmen seiner Verantwortlichkeiten und Zuständigkeiten die nötigen Regulative beschlossen hatte;
- ob die Datensicherheit in der kantonalen Verwaltung gewährleistet und die Datenvernichtung ausreichend reglementiert und dokumentiert ist.

Aufgrund der Untersuchungsergebnisse hat die Untersuchungskommission organisatorische und strukturelle Verbesserungsvorschläge aufzuzeigen, wie solche Vorkommnisse durch die zuständigen Behörden frühzeitig erkannt und verhindert werden können und die Informations- und Datensicherheit des Kantons Zürich bestmöglich gewährleistet werden kann.

III. Die Untersuchungskommission erstattet dem Kantonsrat Bericht über die Ergebnisse ihrer Untersuchung, insbesondere über allfällige festgestellte Verantwortlichkeiten und institutionelle Mängel. Sie unterbreitet gegebenenfalls Vorschläge für Massnahmen organisatorischer und rechtlicher Art.

IV. Das Sekretariat der Untersuchungskommission wird von den Parlamentsdiensten geführt.

V. Die Geschäftsleitung beantragt auf der Basis einer Kosten-schätzung die für die Arbeit der Untersuchungskommission anfallenden Kosten (personelle und organisatorische Massnahmen) und ergänzt entsprechend das Budget des Kantonsrates.

VI. Die Interfraktionelle Konferenz wird beauftragt, die Wahl der Mitglieder und des Präsidiums der Untersuchungskommission vorzubereiten.

VII. Mitteilung an den Regierungsrat.

Zürich, 27. April 2023

Im Namen der Kommission

Der Präsident:

Beat Habegger

Der Sekretär:

Christian Hirschi

Begründung

1. Ausgangslage

Mutmasslich zwischen 2000 und 2014 kam es in der Direktion der Justiz und des Innern (JI) zu Unregelmässigkeiten bei der Entsorgung von Computer-Hardware. Der Datensicherheitsvorfall wurde mit einer Anfrage im Kantonsrat vom 28. November 2022 (KR-Nr. 456/2022) publik. Die JI bestätigte mit einer Medienmitteilung vom 2. Dezember 2022, dass im genannten Zeitraum Computer-Hardware der JI durch einen externen Dienstleister vermutlich nicht wie vereinbart vernichtet und die darauf gespeicherten Daten nicht gelöscht wurden. Es sei denkbar, dass auch sensitive Daten betroffen sind.

Am 6. Dezember 2022 orientiert die Vorsteherin der JI anlässlich einer Medienkonferenz ausführlich über den Datensicherheitsvorfall. Offenbar informierte die Staatsanwaltschaft die Vorsteherin der JI im November 2020 über den Verdacht, dass bei der Entsorgung der Hardware sensible Daten in falsche Hände gelangt sind und deswegen eine Strafuntersuchung eingeleitet wurde. Nach internen Abklärungen und der Information der Datenschutzbeauftragten gab die Vorsteherin der JI Anfang Dezember 2020 eine Administrativuntersuchung in Auftrag. An der Medienkonferenz wurde ebenfalls bekannt, dass in der Informatikabteilung der JI im Jahr 2019 eine grosse Menge von Papierakten vernichtet wurde. Dies ging aus dem Schlussbericht der Administrativuntersuchung vom 30. März 2021 hervor, der anlässlich der Medienkonferenz vom 6. Dezember 2022 von der JI veröffentlicht wurde.

Ebenfalls am 6. Dezember 2022 kommunizierte die Oberstaatsanwaltschaft öffentlich, dass die Staatsanwaltschaft Zürich-Sihl seit November 2020 ein Strafverfahren im Zusammenhang mit dem Datensicherheitsvorfall führt. Zudem kündigte sie an, dass sie den «Teilaspekt der Datenentsorgung» einer vertieften strafrechtlichen Prüfung unterziehen wird. Gemäss Medienberichten von Anfang Dezember 2022 kam es aufgrund von Informationen aus dem Datenmissbrauchsvorfall im Zusammenhang mit anderen laufenden Strafverfahren offenbar zu Drohungen und Erpressungsversuchen. Inwiefern zum Vorschein gekommene vertrauliche Daten durch unsachgemässe Handhabung seitens der JI bzw. von ihr beauftragter Personen in Umlauf geraten sind, ist Gegenstand des laufenden Strafverfahrens.

Mit einer am 5. Dezember 2022 eingereichten dringlichen Interpellation (KR-Nr. 462/2022) wurden im Kantonsrat vom Regierungsrat zusätzliche Auskünfte zum Datensicherheitsvorfall und zu den Verantwortlichkeiten der JI verlangt. Die Vorsteherin der JI nahm im Namen des Regierungsrates an der Kantonsratssitzung vom 9. Januar 2023 dazu Stellung.

2. Abklärungen der Geschäftsprüfungskommission

Die Geschäftsprüfungskommission (GPK) wurde von der Vorsteherin der JI anlässlich eines Referentengesprächs am 1. März 2021 mündlich und schriftlich über den Datenmissbrauchsvorfall und die laufende Administrativuntersuchung informiert. Es wurde mitgeteilt, dass der Datenmissbrauch vermutlich auf die unsachgemässe Entsorgung von Datenträgern durch einen von der JI mandatierten externen Partner zurückzuführen ist und davon ausgegangen werden muss, dass auch sensitive Daten betroffen sind. Die GPK wurde auch darüber informiert, dass die Administrativuntersuchung in enger Absprache mit dem Amt für Informatik und dem kantonalen Sicherheitsverantwortlichen (heute: Kantonaler Informatik-Sicherheitsbeauftragter) erfolgt und der Vorfall umgehend der kantonalen Datenschutzbeauftragten gemeldet worden sei. Der Schlussbericht mit den Empfehlungen liege in der ersten Jahreshälfte 2021 vor. Über den Schlussbericht wurde die GPK seitens der JI jedoch nicht informiert, hat diesen aber auch nicht nachgefragt.

Am 30. November 2022 kontaktierte die Vorsteherin der JI den GPK-Präsidenten und den GPK-Referenten für die JI im Zusammenhang mit der zwei Tage zuvor im Kantonsrat eingereichten Anfrage KR-Nr. 456/2022. Der in der Anfrage erwähnte Vorfall habe sich 2008 und damit vor bald 15 Jahren zugetragen. Spätestens seit 2013 gelte ein professioneller Prozess zur Entsorgung von Datenträgern in der JI. Seither

werde jede einzelne Entsorgung dokumentiert und mit den dafür nötigen Zertifikaten versehen. Dieser Prozess sei völlig unabhängig vom Vorfall aus dem Jahr 2008 installiert worden. Der Datenmissbrauch stehe seit 2020 im Raum. Zudem verwies die Vorsteherin der JI auf das GPK-Referatengespräch vom 1. März 2021 und die dort kommunizierten Informationen zur Administrativuntersuchung.

Die GPK befragte daraufhin die Vorsteherin der JI am 8. Dezember 2022. Im Vordergrund der Befragung standen die im Auftrag der JI durchgeführte Administrativuntersuchung sowie das Vorgehen der JI, nachdem der Vorfall der JI im November 2020 bekannt geworden ist. Die GPK teilte der Vorsteherin der JI auch mit, dass die Kommission von der JI proaktiv über die Ergebnisse der Administrativuntersuchung hätte informiert werden müssen.

Im Anschluss an diese Anhörung beschloss die GPK, eine Untersuchung zum Umgang der JI und allfälliger weiterer kantonaler Stellen mit dem Datensicherheitsvorfall einzuleiten, und setzte dafür eine Subkommission ein. In diesem Zusammenhang sollte auch überprüft werden, ob und wie die Empfehlungen der Administrativuntersuchung umgesetzt wurden und ob der Umgang mit Daten und Informationen in der JI heute den gesetzlichen Anforderungen entspricht. Bevor die Subkommission ihre Untersuchung in Angriff genommen hatte, beschloss die GPK, dem Kantonsrat einen Antrag auf Einsetzung einer PUK zu stellen, und beauftragte die Subkommission mit den dafür nötigen Arbeiten.

In der Folge hörte die Subkommission am 26. Januar 2023 die Datenschutzbeauftragte und am 2. Februar 2023 den Leitenden Oberstaatsanwalt an. Die Subkommission befragte die Datenschutzbeauftragte zur gesetzlichen Meldepflicht des Datensicherheitsvorfalls (§ 12 Gesetz über die Information und den Datenschutz [IDG, LS 170.4]) und zur Frage, ob vom Datensicherheitsvorfall mutmasslich betroffene Personen darüber hätten informiert werden müssen. Darüber hinaus befasste sich die Subkommission mit der Frage, ob die Behörden nicht auch die Öffentlichkeit früher über den Datenmissbrauchsvorfall hätten informieren müssen.

Der Leitende Oberstaatsanwalt informierte die Subkommission über das laufende Strafverfahren im Zusammenhang mit dem Datensicherheitsvorfall. Dieses wurde eingeleitet, nachdem es gegen Angehörige der Staatsanwaltschaft zu Drohungen und Erpressungsversuchen kam. Dabei stellt sich heraus, dass dafür Informationen verwendet wurden, die von Datenträgern der JI herrührten. Die Staatsanwaltschaft befasst sich demnach seit November 2020 mit dieser Angelegenheit, wobei anfänglich nicht der Datensicherheitsvorfall im Vordergrund stand.

Nach den der GPK vorliegenden Informationen hat die Kommission den Eindruck, dass sich das Ausmass des Datensicherheitsvorfalls erst allmählich zeigte, nachdem bei verschiedenen Hausdurchsuchungen eine grosse Zahl an Datenträgern sichergestellt wurden. Der Leitende Oberstaatsanwalt orientierte die Subkommission auch darüber, dass das Strafverfahren in der Zwischenzeit erweitert wurde. So ist die erwähnte Aktenvernichtung in der JI aus dem Jahr 2019 ebenfalls Teil des Strafverfahrens. Am 9. März 2023 wurde zudem in einem Zeitungsbericht erwähnt, dass auch die Staatsanwaltschaft III, die auf die Strafverfolgung im Bereich der Wirtschaftskriminalität spezialisiert ist, wegen des Verdachts auf ungetreue Amtsführung ermittelte.

3. Aufgaben und Ziele der parlamentarischen Oberaufsicht sowie Möglichkeiten und Grenzen einer Parlamentarischen Untersuchungskommission (PUK)

Es ist der gesetzliche Auftrag der parlamentarischen Kontrolle (Oberaufsicht), das Handeln des Regierungsrates, der öffentlichen Verwaltung sowie weiterer Träger von öffentlichen Aufgaben des Kantons zu beaufsichtigen sowie besondere Vorkommnisse zu untersuchen (Art. 57 Kantonsverfassung [LS 101] in Verbindung mit §§ 104 und 105 Kantonsratsgesetz [KRG, LS 171.1]). Dadurch leistet die Oberaufsicht einen wichtigen Beitrag zur Transparenz des staatlichen Handelns und zur Vertrauensbildung in der Öffentlichkeit gegenüber den staatlichen Institutionen.

Um den Auftrag der parlamentarischen Oberaufsicht wie umschrieben zu erfüllen, genügt es nicht, sich auf die von der JI durchgeführte Administrativuntersuchung abzustützen. Wie aufgezeigt, stellen sich rund um die Administrativuntersuchung selbst Fragen, zum Beispiel zur Information des Regierungsrates, der weiteren Direktionen und des Kantonsrates. Zudem brachte die Administrativuntersuchung hervor, dass die Datenentsorgung aus den Jahren 2000 bis 2014 womöglich gar nicht mehr aktenbasiert aufgearbeitet werden kann, da eine grosse Menge an physischen Akten im Jahr 2019 vernichtet wurde. Es ist zudem unklar, ab wann sich der Regierungsrat der grundsätzlichen Problematik der Datensicherheit und der Entsorgung von Datenträgern bewusst war und ob er rechtzeitig die nötigen Regulative beschlossen hat.

Die nach dem öffentlichen Bekanntwerden des Datensicherheitsvorfalls im Dezember 2022 gestartete Untersuchung der GPK zeigte schnell, dass die sich stellenden grundsätzlichen Fragen im Rahmen der ordentlichen Kommissionstätigkeit kaum innert nützlicher Frist untersucht werden können. Vor allem wenn die Untersuchung auf die gesamte

Verwaltung ausgedehnt werden soll, übersteigt dies die personellen und zeitlichen Ressourcen der Kommission. Alternativ würde die Kommissionstätigkeit durch diese Untersuchung über Gebühr belastet, was zu grossen Verzögerungen bei anderen laufenden Prüfungen der GPK führen würde.

Gestützt auf Erfahrungswerte aus der PUK zu den Vorkommissionen bei der BVK Personalvorsorge des Kantons Zürich (KR-Nr. 253/2010) ist bei einer PUK von einem Budget zwischen 800 000 und 1,1 Mio. Franken auszugehen (Sitzungen, Aktenstudium, externe Gutachtertätigkeiten, PUK-Sekretariat).

Neben den für die Untersuchung zur Verfügung stehenden Ressourcen bietet eine PUK gegenüber einer GPK-Untersuchung den Vorteil, dass im Rahmen des PUK-Verfahrens alle Personen in öffentlicher Funktion sowie Privatpersonen befragt werden können, soweit sie der Zeugenpflicht unterstehen (§ 119 KRG). In einer GPK-Untersuchung beschränkt sich die Auskunftspflicht neben den Mitgliedern des Regierungsrates sowie weiteren Leitungspersonen kantonaler Behörden im Wesentlichen auf alle Angestellten des Kantons (§ 111 KRG).

Sowohl im Rahmen eines PUK-Verfahrens als auch in einer GPK-Untersuchung gilt es, auf das laufende Strafverfahren Rücksicht zu nehmen. Im PUK-Verfahren gibt es eine Mitwirkungs- und Aussagepflicht für Auskunftspersonen (§ 120 KRG). Im Strafverfahren wiederum gilt das Recht, sich selbst nicht belasten zu müssen (Art. 113 Strafprozessordnung [SR 312.0]). Das Recht, als beschuldigte Person in einem Strafverfahren die Aussage und die Mitwirkung im Strafverfahren zu verweigern, kann durch das PUK-Verfahren nicht umgangen werden. Solange das Strafverfahren nicht abgeschlossen ist, droht somit eine Kollision zwischen PUK-Verfahren und Strafverfahren, weil davon auszugehen ist, dass es teilweise die gleichen Personen sind, die sowohl im Rahmen des Strafverfahrens als auch durch die PUK zu befragen sind. Deshalb sollen die PUK-Untersuchungen koordiniert zum Strafverfahren (insbesondere bei Anhörungen) erfolgen, um dieses nicht zu behindern.

Wann das Strafverfahren abgeschlossen sein wird, kann zum derzeitigen Zeitpunkt nicht abgeschätzt werden. Aufgrund der jüngst erfolgten Ausweitung des Strafverfahrens ist davon auszugehen, dass dieses noch längere Zeit laufen wird. Die GPK ist deshalb der Auffassung, dass trotz der potenziellen Kollision zwischen PUK und Strafverfahren mit der politischen Aufarbeitung des Datensicherheitsvorfalls nicht zugewartet werden darf.

4. Untersuchungsgegenstände

Aufgrund der Abklärungen der GPK stellen sich zum bekannt gewordenen Datensicherheitsvorfall sowie generell zur Problematik der Datensicherheit und Entsorgung von Datenträgern in der kantonalen Verwaltung verschiedene Fragen zu den nachfolgend umschriebenen Untersuchungsgegenständen.

Zeitraum des mutmasslichen Datensicherheitsvorfalls

Zum Zeitraum des Datenmissbrauchs liegen der Kommission unterschiedliche Informationen vor. Gemäss den Informationen anlässlich des GPK-Referentengesprächs von Anfang März 2021 wurde seitens der JI davon ausgegangen, dass der Zeitraum zwischen 2008 und 2013/14 betroffen ist. In einer Medienmitteilung der JI vom 2. Dezember 2022 wurde der Vorfall auf die Jahre 2006 bis 2012 eingegrenzt. Gemäss den der GPK von der Datenschutzbeauftragten vorliegenden Informationen muss davon ausgegangen werden, dass in den Jahren 2000 bis 2014 Personendaten auf den zur Entsorgung vorgesehenen Geräten nicht wie vereinbart gelöscht bzw. die Geräte nicht wie vereinbart entsorgt wurden und dadurch unbefugte Personen Zugang zu den gespeicherten Daten erhalten haben. Aus Sicht der GPK ist der unklare Zeitrahmen des Datensicherheitsvorfalls ein Hinweis darauf, dass das Ausmass des Vorfalls nach wie vor nicht deutlich eingegrenzt werden kann.

Umgang mit dem Datensicherheitsvorfall seitens Regierungsrat, Direktionen und weiterer Behörden

Nachdem die JI im Zusammenhang mit einem laufenden Strafverfahren von der Staatsanwaltschaft im November 2020 über den mutmasslichen Datenverlust informiert wurde, leitete die Vorsteherin der JI Anfang Dezember 2020 eine Administrativuntersuchung ein. Parallel dazu wurde der Vorfall der Datenschutzbeauftragten gemeldet. Gemäss den der GPK bekannten Informationen wurde der Regierungsrat von der Vorsteherin der JI im November 2020 am Rande der Beratung eines anderen Geschäfts mündlich über den Datensicherheitsvorfall informiert. Die GPK wurde, wie erwähnt, anlässlich des Referentengesprächs vom Anfang März 2021 über die laufende Administrativuntersuchung informiert, jedoch nicht über deren Abschluss und Ergebnisse. Aus Sicht der GPK ist deshalb nach wie vor offen, ob die verschiedenen Organe und allfällige weitere Stellen rechtmässig und zweckmässig auf den Datensicherheitsvorfall reagiert haben und ob angemessen darüber informiert wurde. Es ist deshalb auch unklar, ob tatsächlich die nötigen Schritte unternommen worden sind, um den Datensicherheitsvorfall aufzuarbeiten und um zu verhindern, dass sich ähnliche Vor-

fälle künftig wiederholen. Zu untersuchen ist auch, ob der Regierungsrat angemessen geprüft hat, für die Strafuntersuchung allenfalls eine ausserkantonale Strafverfolgungsbehörde zu beauftragen.

Informationssicherheit in der kantonalen Verwaltung

Der Datensicherheitsvorfall in der JI und der Umgang damit werfen aus Sicht der GPK grundsätzliche Fragen zur Informationssicherheit und zur Entsorgung von Datenträgern in der kantonalen Verwaltung auf. Das IDG verpflichtet die öffentlichen Organe unter dem Titel «Informationssicherheit», Informationen durch angemessene organisatorische und technische Massnahmen zu schützen (§ 7 Abs. 1 IDG). Diese Massnahmen dienen den Schutzziele Vertraulichkeit, Unversehrtheit, Zurechenbarkeit und Nachvollziehbarkeit (§ 7 Abs. 2 IDG). Sie richten sich nach Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik (§ 7 Abs. 3 IDG). Gestützt auf das IDG erliess der Regierungsrat mit Beschluss Nr. 795/2019 eine neue allgemeine Informationssicherheitsrichtlinie.

Aus Sicht der GPK ist zu untersuchen, ob diese Vorgaben ausreichend sind, nicht nur, um Datensicherheitsvorfälle bestmöglich zu verhindern, sondern auch, um bei deren Auftreten angemessen darauf reagieren zu können. Weiter ist aus Sicht der GPK zu prüfen, ob Datenvernichtungen in der kantonalen Verwaltung generell ausreichend dokumentiert werden und die Anforderungen an die Vernichtung von Akten in der kantonalen Verwaltung angemessen ausgestaltet sind. Es stellt sich auch die grundsätzliche Frage, ob sich der Regierungsrat im Rahmen seiner Verantwortlichkeiten und Zuständigkeiten der Problematik der Datensicherheit und Entsorgung von Datenträgern bewusst war und ob er vorausschauend die nötigen Regulative beschlossen und umgesetzt hat.

5. Stellungnahme des Regierungsrates

Der Regierungsrat hat den Entwurf der GPK zum Antrag an den Kantonsrat auf Einsetzung einer PUK zur Stellungnahme erhalten. Er hält in seiner Stellungnahme fest, dass die Einsetzung einer PUK in der Kompetenz des Kantonsrates liege. In welcher Form und mit welchen Instrumenten der Kantonsrat seine Oberaufsicht wahrnehme, überlasse er dem Kantonsrat. Er sichere in jedem Fall seine volle Kooperation zu.

6. Antrag auf Einsetzung einer PUK

Nach Würdigung der gesamten Umstände kommt die GPK zum Schluss, dass die Einsetzung einer PUK vorliegend angezeigt ist. Die GPK beantragt deshalb dem Kantonsrat die Einsetzung einer PUK gemäss §§ 115 ff. KRG.