Medienmitteilung

Zürich, 12. Dezember 2025

**Regierungsrat hat Daten- und Informationssicherheit vernachlässigt**

**Die Parlamentarische Untersuchungskommission (PUK) Datensicherheit kritisiert in ihrem Bericht (KR-Nr. 172/2023) die Organisation der kantonalen Verwaltung bei der Daten- und Informationssicherheit. Diese lasse den Direktionen und der Staatskanzlei in der Umsetzung viel Spielraum. Das Silodenken, das den untersuchten Datensicherheitsvorfall in der Direktion der Justiz und des Innern (JI) erst ermöglichte, müsse überwunden werden.**

In den Jahren 2002 bis 2014 ist es in der JI zu unsachgemässen Entsorgungen von Datenträgern gekommen. Laut Staatsanwaltschaft wurden an zehn verschiedenen Orten 202 Datenträger wie Festplatten und USB-Sticks sichergestellt. Sie enthielten teilweise noch sensitive Daten. Unklar bleibt, wie viele Datenträger über die von den Staatsanwaltschaften sichergestellten Geräte hinaus vom Datensicherheitsvorfall betroffen sind. Die sichergestellten Daten zeigen, dass verschiedene Ämter der JI vom Vorfall, der im Dezember 2022 öffentlich bekannt wurde, betroffen waren. Es gibt indes keine Anzeichen dafür, dass Daten der eigentlichen Systeme der JI, namentlich das Rechtsinformationssystem, oder anderer Direktionen oder der Staatskanzlei in Umlauf gerieten. Da der PUK Datensicherheit jedoch zu den früheren Entsorgungsprozessen in den Direktionen und der Staatskanzlei keine lückenlosen Informationen vorliegen, lassen sich auch dort frühere Risiken nicht ausschliessen.

Die PUK Datensicherheit erhielt vom Kantonsrat den Auftrag, den Datensicherheitsvorfall politisch aufzuarbeiten. In ihrem Bericht zeigt sie detailliert auf, wie der Vorfall möglich wurde und welche Umstände ihn begünstigten. Weiter legt die PUK Datensicherheit auch dar, wie sich die rechtlichen und organisatorischen Grundlagen in Bezug auf die Informationssicherheit in der Zeit von 1990 bis heute entwickelt haben und wer die Verantwortung für die Informationssicherheit und den Datensicherheitsvorfall getragen hat. Konkret kommt die PUK Datensicherheit in ihrem Bericht zu den folgenden Schlüssen:

**Ungenügende Begleitung**
Die Informationssicherheit der kantonalen Verwaltung war durch gesetzliche Grundlagen aus den 1990er Jahren bereits früh angemessen geregelt. Der Regierungsrat hat der Informationssicherheit als gesamtkantonale Gemeinschaftsaufgabe über die Direktionen hinweg jedoch über Jahre zu wenig Beachtung geschenkt. Er hat die Thematik Informationssicherheit mit zu wenig Nachdruck vorangetrieben und ungenügend begleitet.

Das Scheitern der kantonalen Informatikstrategie 2008, auch eine Folge der damals äusserst komplexen Entscheidungsstruktur, hatte für die kantonale Informationssicherheit nachteilige Folgen. Der Aufbau einer professionellen kantonalen Informationssicherheitsorganisation und eines Informationssicherheits-Managements verzögerte sich, womit auch die Erarbeitung konkreter verbindlicher kantonaler Vorgaben, unter anderem zur sachgemässen Datenlöschung und Entsorgung von Datenträgern, erst spät vorlagen. 2015 schuf der Regierungsrat die Funktion des kantonalen Informationssicherheitsbeauftragten und erliess

Sekretariat PUK Datensicherheit, Parlamentsdienste, Haus zum Rechberg, Hirschengraben 40, Postfach, 8090 Zürich
Telefon: +41 43 259 23 81 – heiri.gander@pd.zh.ch

2019 die Allgemeine Informationssicherheitsrichtlinie. Ab 2020 folgten die Informationssicherheitsbeauftragten in den Direktionen und der Staatskanzlei sowie themenspezifische kantonale Vorgaben in Form der Besonderen Informationssicherheitsrichtlinien. Der Regierungsrat widmete der Umsetzung der Informatikstrategie trotz der mahnenden Berichte des damaligen Datenschutzbeauftragten, der Aufsichtskommissionen und der Finanzkontrolle aber lange zu wenig Aufmerksamkeit.

**Bewusstsein für kantonale Lösung fehlt weiterhin**
Die kantonalen Aktivitäten haben sich 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 fehlt 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.

Der frühere Datenschutzbeauftragte, die Geschäftsprüfungskommission und die Finanzkommission sowie die Finanzkontrolle machten zu diesen Fragen bereits früh Feststellungen und forderten Massnahmen. Für die PUK Datensicherheit ist es nicht nachvollziehbar, dass der Regierungsrat diese Empfehlungen nicht mit Nachdruck verfolgte und lange kantonalen Lösungen äusserst zurückhaltend gegenüberstand.

Auch die neueren Untersuchungen zum Datensicherheitsvorfall hat der Regierungsrat nicht zum Anlass genommen die kantonale Situation grundsätzlich zu analysieren und noch stärker gesamtkantonale Vorgaben vorzusehen. Die PUK Datensicherheit bemängelt den weiterhin bestehenden Fokus des Regierungsrats auf die einzelnen Direktionen statt auf den Kanton. Ein kausales Fehlverhalten des Regierungsrats oder deren Direktionsvorsteherinnen und -vorsteher für den eigentlichen Datensicherheitsvorfall in der JI kann die PUK Datensicherheit hingegen nicht feststellen.

**Datensicherheitsvorfall in der JI**
Den Zeitraum des Datensicherheitsvorfalls in der JI konnte die PUK Datensicherheit auf die Jahre 2002–2014 eingrenzen, in denen der externe Dienstleister, über den Datenträger der JI abhandengekommen sind, für die JI-Informatik tätig war. Die konkreten Umstände der Auftragsvergabe an den externen Dienstleister liessen sich für die PUK Datensicherheit nicht mehr eruieren. Sie stiess auf keinen schriftlichen Vertrag und es fehlt auch an Belegen, dass die korrekte Löschung von Daten schriftlich bestätigt wurde. Es bestehen auch keine Anzeichen, dass im Rahmen einer Aufräumaktion 2019, anders als anfänglich angenommen, wirklich relevante Unterlagen abhandengekommen sind.

Die Aufsicht, die internen Kontrollen sowie die Dokumentation waren in der JI-Informatik in jener Zeit ungenügend. Hierfür verantwortlich waren der ehemalige Leiter der Hauptabteilung Logistik, Finanzen und Controlling (LFC) sowie der damalige Abteilungsleiter der JI-Informatik. Die gelebten Prozesse wichen von den festgehaltenen Zuständigkeiten ab und der Dienstweg wurde gemäss Aussagen nicht immer eingehalten. Es bleibt unklar, wer für die Auftragserteilung an den externen Dienstleister verantwortlich war. Beide Personen sind jedoch ihrer Verantwortung nicht ausreichend nachgekommen. Sicher ist auch, dass der damalige Generalsekretär und die damaligen Vorsteher der JI den Abteilungsleitern stark

vertrauten. Nachdem die Finanzkontrolle zur JI-Informatik 2014 wesentliche Feststellungen gemacht hatte, ergriff der damalige Direktionsvorsteher organisatorische und personelle Massnahmen.

Die aktuelle Direktionsvorsteherin und die aktuelle Generalsekretärin haben durch organisatorische und personelle Veränderungen zu einer Verbesserung der Informationssicherheit beigetragen. Eine weitergehende Aufarbeitung der schwierigen Situation in der JI-Informatik blieb aber aus.

**Ungenügende Information der Direktionsvorsteherin der JI**
Als die aktuelle Direktionsvorsteherin der JI im November 2020 vom Datensicherheitsvorfall erfuhr, ordnete sie eine Administrativuntersuchung an und informierte den kantonalen Informationssicherheitsbeauftragten sowie die Datenschutzbeauftragte. Die Kommunikation der JI gegenüber den Behörden war jedoch ungenügend. Die Finanzkontrolle wurde nicht informiert und die Datenschutzbeauftragte erhielt den Schlussbericht erst auf wiederholte Nachfrage. Die Geschäftsprüfungskommission des Kantonsrates erfuhr zwar im Rahmen eines Referentengesprächs im März 2021 vom Datensicherheitsvorfall. Eine Zustellung des Schlussberichts blieb aber aus.

Kritisiert wird von der PUK Datensicherheit die Kommunikation der JI-Direktionsvorsteherin gegenüber dem Regierungsrat. Bei der ersten mündlichen Information an der Regierungsratssitzung vom 18. November 2020 erwähnte sie den Vorfall so beiläufig, dass sich später kaum jemand an diese Information erinnern konnte. Den Schlussbericht zur Administrativuntersuchung erhielt der Regierungsrat erst im Vorfeld des Point de Presse vom 6. Dezember 2022. Erst am 21. Dezember 2022 wurde der Regierungsrat über den Datensicherheitsvorfall grundlegend informiert.

**50 Empfehlungen an Regierungsrat und Kantonsrat**
Zu den in 50 Sitzungstagen und umfangreichen Aktenstudien und Befragungen erlangten Erkenntnissen hat die PUK Datensicherheit einen Schlussbericht mit 50 Empfehlungen einstimmig verabschiedet. Damit empfiehlt sie insbesondere eine intensivere Zusammenarbeit, einheitliche Regelungen und eine gemeinsame Verantwortung der Regierung bei allen Aspekten der Informationssicherheit und der Informatik. Zudem ist die Berichterstattung innerhalb der Regierung und gegenüber den Aufsichtskommissionen zu stärken und die Aufsicht über IT-Projekte und Informationssicherheit sicherzustellen.

*Kontakt:*
PUK-Datensicherheit-Präsident: Benno Scherrer (GLP, Uster), 077 445 44 49