Bericht der Parlamentarischen Untersuchungskommission Datensicherheit

vom 21. November 2025

Sehr geehrter Herr Kantonsratspräsident
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen den Bericht der Parlamentarischen Untersuchungskommission (PUK Datensicherheit) gemäss Ihrem Beschluss vom 3. Juli 2023 zu den Abklärungen über 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 (JI) und allfälligen weiteren kantonalen Stellen.

Im Namen der Kommission

Der Präsident:	Der Sekretär:
Benno Scherrer	Heiri Gander

Zusammenfassung des Berichts

Der Kantonsrat beschloss an seiner Sitzung vom 3. Juli 2023 die Einsetzung einer Parlamentarischen Untersuchungskommission (PUK) (KR-Nr. 172/2023). Die Parlamentarische Untersuchungskommission (PUK Datensicherheit) erhielt vom Kantonsrat den Auftrag, die Geschehnisse 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 (JI) und allfälligen weiteren kantonalen Stellen politisch aufzuarbeiten. Nach 50 Sitzungstagen, umfangreichem Aktenstudium und knapp 1000 Seiten protokollierter Befragungen von Auskunftspersonen, Zeuginnen und Zeugen kommt die PUK Datensicherheit zu folgendem Schluss:

1. War sich der Regierungsrat der Problematik der Datensicherheit und Entsorgung von Datenträgern bewusst? Hat der Regierungsrat im Rahmen seiner Verantwortlichkeiten und Zuständigkeiten die nötigen Regulative beschlossen?

Erkenntnisse aus den Kapiteln 5 und 6

Rückblickend lässt sich feststellen, dass die Informationssicherheit in den früheren gesetzlichen Grundlagen, wie dem Gesetz über den Schutz der Personendaten vom 6. Juni 1993 (Datenschutzgesetz, DSG) oder der Informatiksicherheitsverordnung vom 17. Dezember 1997 (ISV), gut geregelt war. Zum Umgang mit Papierakten sowie nicht mehr benötigten Informatikmitteln hatte der Regierungsrat früh ergänzende Weisungen beschlossen. Auch mit der Umsetzung der Sicherheitsinitiative des damaligen Datenschutzbeauftragten, Bruno Baeriswyl, versuchte der Regierungsrat 2004, die Informationssicherheit zu verbessern.

Der Regierungsrat hatte seine eigene, im Jahr 2008 verabschiedete Informatikstrategie jedoch ungenügend begleitet, was für die Umsetzung der Informationssicherheit nachteilige Folgen hatte. Der Aufbau einer kantonalen Informationssicherheitsorganisation verzögerte sich dadurch massiv und der Aufbau eines kantonalen Informationssicherheits-Managements konnte nicht an die Hand genommen werden. Das Scheitern der Informatikstrategie lag, wie auch die Geschäftsprüfungskommission (GPK) 2017 festgestellt hat, u. a. an der äusserst komplexen Entscheidungsstruktur der KITT-Organisation (Kantonales IT-Team), die Fortschritte verhinderte, sowie an der fehlenden Begleitung und Unterstützung durch den Regierungsrat. Dieser widmete der Umsetzung der Informatikstrategie, die für die Informationssicherheit wesentliche Inhalte enthielt, trotz der mahnenden Berichte des Datenschutzbeauftragten, Bruno Baeriswyl, der Aufsichtskommissionen und der Finanzkontrolle lange zu wenig Aufmerksamkeit.

Erkenntnisse aus Kapitel 10

Trotz der schwierigen Rahmenbedingungen des kantonalen IT-Teams gelang es 2015, die Stelle des Informatik-Sicherheitsbeauftragten (I-SiBe) zu schaffen und zu besetzen. Der Regierungsrat unterliess es aber, bei dieser Gelegenheit ein wirkliches Kompetenzzentrum Informationssicherheit aufzubauen. In der Folge stiess der I-SiBe bei seiner Arbeit auf Widerstand in den Direktionen und der Staatskanzlei und spürte kaum die Unterstützung des Regierungsrates.

Die vom Regierungsrat in Auftrag gegebene externe Analyse der kantonalen IT-Situation und die diesbezüglichen Feststellungen im Jahr 2016 hatten grosse Auswirkungen auf die kantonale IKT-Organisation. Auf Basis des externen Berichts zur Überprüfung der Informatik des Kantons Zürich vom 31. Oktober 2016 (BDO-Bericht) befasste sich der Regierungsrat eingehend mit der IT-Governance und machte sich daran, die Zentralisierung der IKT-Grundversorgung anzugehen. Infolge der Priorisierung der Umgestaltung der kantonalen Informatik rückten die weiterhin ungelösten Aufgaben im Bereich der kantonalen Informationssicherheit – Aufbau einer Sicherheitsorganisation, Aufbau eines Informationssicherheits-Managements und Revision der Informatiksicherheitsverordnung aus dem Jahr 1997 – in den folgenden Jahren allerdings in den Hintergrund.

Zudem hat die Informationssicherheit im Rahmen der Totalrevision der Informatiksicherheitsverordnung (ISV), die in den Jahren 2015–2019 realisiert worden war, eine Schwächung erfahren. Die heutige Verordnung über die Informationsverwaltung und -sicherheit (IVSV) enthält im Gegensatz zur früheren Verordnung kaum noch konkrete Regelungen zur Informationssicherheit. Beispielsweise sind die Regelungen zur Datenbearbeitung von Dritten, wie sie im Rahmen des Datensicherheitsvorfalls vorgekommen ist, nicht mehr auf Verordnungsstufe geregelt. Auch die lange Erarbeitungszeit der IVSV brachte Nachteile für die Informationssicherheit, da die eigentlich bis 2020 geltenden Bestimmungen der ISV in dieser Übergangszeit nicht mehr die gleiche Geltung entfalten konnten. So musste die PUK Datensicherheit feststellen, dass die internen Audits, wie sie gemäss der ISV vorgesehen gewesen wären, in den Direktionen und der Staatskanzlei kaum stattgefunden haben.

Mit seinem Entscheid, die konkreten Regelungen zur Informationssicherheit statt in einer Verordnung in einer Allgemeinen Informationssicherheitsrichtlinie (AISR) zu regeln, trug der Regierungsrat weiter zur Verminderung der Sichtbarkeit der Informationssicherheit in der kantonalen Verwaltung bei.

Die ausserordentlichen kantonalen Bemühungen, die kantonale Informatik stärker zu zentralisieren, schufen zwar in vielerlei Hinsicht die Basis für eine Verbesserung im Bereich der Informationssicherheit. In den diesbezüglichen neuen strategischen Grundlagen zur neuen IKT-Governance, der IKT-Strategie 2018 sowie der Grundlage für die weiteren Digitalisierungsbestrebungen, der Strategie Digitale Verwaltung und IKT 2018–2023, blieb die Informationssicherheit aber weitgehend unberücksichtigt. Es fehlt bis heute eine strategische Herangehensweise, die Fragen der IKT-Organisation, der Digitalisierung und der Informationssicherheit gemeinsam betrachtet.

Erkenntnisse aus Kapitel 14

Mit der Verabschiedung der AISR hat der Regierungsrat am 3. September 2019 eine Basis für die Umsetzung der Informationssicherheit geschaffen. Organisatorisch verstärkt wurde die Informationssicherheit jedoch erst 2020, als in den Direktionen und der Staatskanzlei dezidierte Stellen für Informationssicherheitsbeauftragte geschaffen wurden. Einen wichtigen Schub erhielt die Informationssicherheit schliesslich ab 2022, als die Informationssicherheitsstrategie (damals Cybersicherheitsstrategie) verschiedene Entwicklungen auf kantonaler Ebene, wie kantonale Schulungen, Audits oder Lieferantenüberprüfungen, erst möglich machte.

Diese Entwicklung und die ab 2022 verstärkten Massnahmen zeigen, dass die Erkenntnis, wie wichtig die Informationssicherheit ist, erst vor kurzer Zeit wirklich beim Regierungsrat angekommen ist. Das Bewusstsein für die Notwendigkeit einer kantonalen Herangehensweise an die Informationssicherheit fehlt jedoch weiterhin. So verortet die aktuelle Version der AISR vom 16. April 2025 die Umsetzung der Informationssicherheit stark in den Direktionen und der Staatskanzlei und nicht auf der Ebene des Kantons.

2. Wie war die Entsorgung von Datenträgern im fraglichen Zeitraum in den Direktionen, besonders in Bereichen mit sensitiven Daten, geregelt?

Erkenntnisse aus Kapitel 7

Die Direktion der Justiz und des Innern (JI) war bereits in frühen Jahren im Bereich der technischen Informationssicherheit äusserst gut aufgestellt. Sie verfügte ab 1996 über verschlüsselte und mit Chipkarte gesicherte Geräte. Mit der eigenen Informatikstrategie vom 11. Februar 2011 und dem Informatiksicherheitskonzept vom 14. November 2013 konnte die JI schon früh eigene Grundlagen vorweisen. Zudem hatte der damalige Leiter LFC, Renato Widmer, der Informationssicherheit innerhalb der JI die nötige Nachachtung verschafft. Ergänzend hatte die JI-Informatik ab 2009 ihr Qualitätsmanagement (QM) zertifizieren lassen. Die konkrete Frage der Entsorgung von Datenträgern war in diesen Unterlagen jedoch nur allgemein adressiert. Scheinbar erfolgte die Entsorgung über den beschriebenen QM-Prozess zur Rücknahme einzelner Arbeitsplätze, der in dieser Hinsicht jedoch ungenügend war.

Erkenntnisse aus Kapitel 9

Die anderen Direktionen und die Staatskanzlei gaben an, die Datenträgervernichtungen und Datenlöschungen intern vorgenommen oder die Entsorgung im Rahmen von Neubeschaffungen mit spezialisierten Auftragnehmern gelöst zu haben. Je nach Direktionsstruktur lag die Verantwortung für die Entsorgungsprozesse auch dezentral in den Ämtern. Zu diesen Prozessen liegen der PUK Datensicherheit keine lückenlosen Informationen vor. Deshalb sind in den anderen Direktionen und der Staatskanzlei frühere Risiken nicht auszuschliessen.

3. Über welchen Zeitraum hat sich der Datensicherheitsvorfall ereignet und wer hat ihn zu verantworten?

Erkenntnisse aus den Kapiteln 7 und 8

Der Zeitraum der unsachgemässen Entsorgungen lässt sich auf die Jahre 2002–2014 eingrenzen. In diesem Zeitraum war der fragliche Dienstleister, André Gisler, für die JI-Informatik tätig. Dokumentiert war er in den Jahren 2005/2006 in den Austausch von PC-Geräten involviert und übernahm in den Jahren 2011 und 2012 die, wie sich zeigte, unvollständige Löschung und Entsorgung der Geräte der Statthalterämter. Für die Geräte, welche im Rahmen eines ordentlichen Rollouts neuer Geräte entsorgt wurden, lässt sich für die JI ab dem Jahr 2010 hingegen belegen, dass die Löschung und Entsorgung korrekt abgelaufen sind.

Die konkreten Umstände der ursprünglichen Auftragserteilung an den Dienstleister liessen sich nicht mehr eruieren. Es liegen keine Anzeichen vor, dass es einen schriftlichen Vertrag gegeben hat. Somit geht die PUK Datensicherheit nicht davon aus, dass ein solcher im Rahmen der Räumungsaktion 2019 weggekommen wäre. Es liess sich auch nicht bestätigten, dass der Dienstleister gegenüber der JI-Informatik die korrekte Löschung der Datenträger schriftlich hätte bestätigen müssen. Weiter waren die Sicherheitsüberprüfung und die damalige Stichprobenkontrolle ungenügend.

Verantwortlich waren in jener Zeit der damalige Leiter der Abteilung Logistik, Finanzen und Controlling (LFC), Renato Widmer, sowie der damalige Leiter der JI-Informatik, Fredi Steiner. Renato Widmer trug die Verantwortung für die Aufsicht über die Informatik und war für das Vertragswesen sowie die Auftragserteilung zum Austausch von PC-Geräten zuständig. Fredi Steiner hatte die Sicherheitsvorgaben aus der Informatiksicherheitsverordnung umzusetzen und seine Mitarbeitenden zu kontrollieren und war für die Migration der Geräte bei Rollout-Projekten verantwortlich. Beide sind ihrer Verantwortung ungenügend nachgekommen. Die damals gelebten Prozesse wichen wesentlich von den festgehaltenen Zuständigkeiten ab. Der Leiter LFC, Renato Widmer, pflegte einen dominanten Führungsstil, wobei der Dienstweg nicht immer eingehalten wurde. Somit bleibt unklar, wer konkret für die Auftragserteilung an den Dienstleister verantwortlich war.

Der damals zuständige Generalsekretär, Christian Zünd, und die Direktionsvorsteher, Markus Notter und Martin Graf, haben rückblickend den Informatikbereich zu wenig eng begleitet und den beteiligten Personen angesichts der inhaltlich guten Arbeit dieser Abteilung stark vertraut.

Zum Ausmass des Datensicherheitsvorfalls lässt sich sagen, dass sich zwar eruieren liess, wie viele Datenträger potenziell an den Dienstleister hätten gehen können. Es lässt sich aber nicht sagen, wie viele Datenträger, über die von den Staatsanwaltschaften sichergestellten Geräte hinaus, konkret noch davon betroffen sind.

Im Rahmen der Kantonsratsdebatte vom 9. Januar 2023 wurde weiter die Frage aufgeworfen, inwieweit die JI sich bemüht habe, sensitive Akten, die im Umlauf waren, einzusammeln und zu vernichten. Hierzu lässt sich festhalten, dass die Staatsanwaltschaft Zürich-Sihl und, ergänzend dazu, die Staatsanwaltschaft III im Rahmen der Strafverfahren an zehn verschiedenen Orten rund 202 Datenträger sichergestellt haben.

Auf Basis der Erkenntnisse der Staatsanwaltschaft III zu den von ihr sichergestellten Datenträgern lässt sich feststellen, dass vom Datensicherheitsvorfall verschiedene Ämter der JI betroffen waren. Es gibt keine Anzeichen, dass Daten anderer Direktionen oder der Staatskanzlei in Umlauf geraten sind. Weiter waren die eigentlichen Systeme der JI, namentlich das Rechtsinformationssystem der JI, nicht betroffen.

4. Wurden die notwendigen Vorkehrungen getroffen, damit sich ein ähnlicher Datenmissbrauch künftig verhindern lässt? Hat die betroffene Direktion zweckmässig, zeitnah und rechtmässig auf den Datensicherheitsvorfall reagiert?

Erkenntnisse aus Kapitel 7

Nachdem die Finanzkontrolle 2014 zur IT-Situation in der JI wesentliche Feststellungen gemacht hatte, ergriff der damalige Direktionsvorsteher, Martin Graf, organisatorische und personelle Massnahmen. Letztere hätten rückblickend wohl früher ergriffen werden müssen.

Erkenntnisse aus Kapitel 11

Die aktuelle Direktionsvorsteherin der JI, Jacqueline Fehr, und die aktuelle Generalsekretärin der JI, Jacqueline Romer, haben durch die Reorganisation des Generalsekretariats, die Anpassungen bei Amtsübergaben, die Einführung eines Geschäftsverwaltungssystems sowie die Neubesetzung der IT-Leitung zu Verbesserungen im Bereich der Informationssicherheit beigetragen. Eine Aufarbeitung der schwierigen Situation in der JI-Informatik blieb aber aus.

Erkenntnisse aus Kapitel 12

Als die Direktionsvorsteherin der JI, Jacqueline Fehr, 2020 vom Datensicherheitsvorfall erfuhr, ordnete sie eine Administrativuntersuchung an und informierte den kantonalen Informationssicherheitsbeauftragten (ISIK) sowie die Datenschutzbeauftragte. Zwar wurde die Umsetzung der Massnahmen der Administrativuntersuchung mit dem ISIK koordiniert, eine gründliche Information des Gesamtregierungsrates über den Datensicherheitsvorfall und die Administrativuntersuchung blieb aber vorerst aus. Die Tatsache, dass im Bereich der Informationssicherheit keine Sofortmassnahmen angezeigt waren, liess das Geschäft auf der Prioritätenliste der JI nach unten rutschen. Weiter verzögerte sich die Umsetzung gewisser Massnahmen aus dem Schlussbericht der Administrativuntersuchung, weil die JI nach dem öffentlichen Bekanntwerden des Datensicherheitsvorfalls die Thematik im Rahmen einer weiteren vertieften Untersuchung breiter angehen wollte. Als Reaktion auf den Bericht vom 19. Dezember 2023 zu Datenschutz und Informationssicherheit in der Direktion der Justiz und des Innern (KPMG-Bericht) wurde im Generalsekretariat der JI schliesslich u. a. die Abteilung Business Support & Compliance aufgebaut, welche die Umsetzung von Datenschutz- und Informationssicherheitsmassnahmen unterstützen soll.

5. Haben der Regierungsrat, die direkt betroffene Direktion, die zuständigen Stellen und Behörden zeitnah die nötigen Schritte unternommen, um den Datensicherheitsvorfall aufzuarbeiten? Hat der Regierungsrat zweckmässig, zeitnah und rechtmässig auf den Datensicherheitsvorfall reagiert?

Erkenntnisse aus Kapitel 13

Die Massnahmen der JI stiessen trotz entsprechender Bemühungen bei den anderen Direktionen und der Staatskanzlei auf geringes Interesse. Eine gemeinsame Reaktion des Regierungsrates auf die Erkenntnisse der Administrativuntersuchung sowie des KPMG-Berichts war nicht erkennbar. In Bezug auf die im Rahmen der Kantonsratsdebatte vom 9. Januar 2023 gestellte Frage, ob die anderen Direktionen die unbedarfte Entsorgung von Festplatten bei sich hatten abklären lassen, lässt sich festhalten, dass zwar Nachforschungen in den vom Datensicherheitsvorfall nicht betroffenen Direktionen und der Staatskanzlei stattgefunden haben, allerdings in bescheidenem Mass.

Der kantonale Informationssicherheitsbeauftragte stiess im Nachgang zur Administrativuntersuchung verschiedene kantonale Verbesserungen an. Der Regierungsrat hat anlässlich des Datensicherheitsvorfalls ein weiteres Audit zur Informationssicherheit veranlasst. Sonst wurde er in der Sache aber nicht gesamtkantonal tätig.

6. Hat die direkt betroffene Direktion angemessen über den Datensicherheitsvorfall informiert?

Erkenntnisse aus den Kapiteln 12 und 13

Die Kommunikation der JI gegenüber den Behörden war ungenügend. So hatte die JI die Datenschutzbeauftragte, Dominika Blonski, erst auf deren zweite Nachfrage mit dem Bericht über die Administrativuntersuchung bedient. Die Frist der Datenschutzbeauftragten zur Umsetzung der Massnahmen liess die JI verstreichen. Die GPK wurde im Rahmen eines Referentengesprächs über den Datensicherheitsvorfall und die Administrativuntersuchung informiert, eine Zustellung des Schlussberichts nach Abschluss der Untersuchung blieb aus. Auch die Finanzkontrolle wurde nicht informiert. Regierungsrätin Jacqueline Fehr räumte diese Fehler aber rasch selbst ein.

Auch die Kommunikation der JI gegenüber dem Regierungsrat ist zu kritisieren. 2020 hatte Regierungsrätin Jacqueline Fehr den Vorfall bei der ersten mündlichen Information an der Regierungsratssitzung vom 18. November 2020 so beiläufig erwähnt, dass sich kaum jemand an diese Information erinnern konnte. Den Schlussbericht der Administrativuntersuchung erhielt der Regierungsrat erst im Vorfeld des Point de Presse vom 6. Dezember 2022. Am 21. Dezember 2022 fand aber schliesslich eine grundlegende Information des Regierungsrates statt.

7. Wann hat der Regierungsrat vom Datensicherheitsvorfall Kenntnis erhalten?

Erkenntnisse aus den Kapiteln 12 und 13

Nur wenige Mitglieder des Regierungsrates gaben an, sich an die mündliche Information im Zusammenhang mit der Vergabe eines Unterhaltsreinigungsauftrags zu erinnern, die anlässlich einer Regierungsratssitzung im Jahr 2020 erfolgt war. Die meisten Regierungsmitglieder meinten, erst vom Datensicherheitsvorfall Kenntnis erhalten zu haben, als dieser im Dezember 2022 öffentlich bekannt wurde.

8. Hat der Regierungsrat angemessen geprüft, ob für das Strafverfahren eine ausserkantonale Strafverfolgungsbehörde zu beauftragen ist?

Erkenntnisse aus Kapitel 13

Der Regierungsrat befasste sich am 21. Dezember 2022 im Beisein des damals zuständigen Leitenden Oberstaatsanwalts, Andreas Eckert, eingehend mit dieser Frage. Der Entscheid des Regierungsrates, das Strafverfahren nicht ausserkantonal zu führen, ist für die PUK Datensicherheit schlüssig und nachvollziehbar. Einerseits standen keine aktuell bei der kantonalen Verwaltung tätigen höheren Kadermitarbeitenden im Fokus. Andererseits war man für diese Abklärungen auf forensische Fähigkeiten angewiesen, wie sie fast nur bei der Kantonspolizei Zürich vorhanden sind.

9. Ist die Informationssicherheit in der kantonalen Verwaltung gewährleistet und die Datenvernichtung ausreichend reglementiert und dokumentiert?

Erkenntnisse aus Kapitel 14

Die Datenlöschung und die Entsorgung von Datenträgern ist heute in den Besonderen Informationssicherheitsrichtlinien (BISR) geregelt, die für die gesamte kantonale Verwaltung gelten. Die BISR 19 vom 19. Dezember 2022 zur Sicherheit von Informationssystemen schreibt vor, dass die Ausserbetriebnahme und fachgerechte Entsorgung von Informationssystemen nach einem dokumentierten Prozess zu erfolgen hat und Informationen auf den Speichermedien vor dem Austausch, der Entsorgung oder der Wiederverwendung irreversibel gelöscht werden müssen. Ein kantonaler Leitfaden hält fest, wie welche Arten von Datenträgern korrekt zu löschen und zu vernichten sind. Schliesslich gibt die kantonale HERMES-Projektmethodik vor, die korrekte Ausserbetriebnahme und Entsorgung sei im Rahmen eines Projektes konzeptuell zu behandeln.

Seit der Verabschiedung der Informationssicherheitsstrategie (damals Cybersicherheitsstrategie) im Jahr 2022 hat der Kanton seine Anstrengungen zur Informationssicherheit wesentlich verstärkt. Viele kantonale Angebote sind aber noch nicht lange etabliert. Auch die kantonalen Audits der Jahre 2021 und 2023 zeigen, dass Verbesserungen angezeigt sind.

So bestehen beispielsweise Informationssicherheitsrisiken in der Lieferkette oder beim Schwachstellenmanagement. Weiter ist der Aufbau eines Informationssicherheits-Managementssystems (ISMS) in den Direktionen und der Staatskanzlei unterschiedlich weit fortgeschritten. Es gilt hier die zu schützenden Werte zu erfassen und Massnahmen zu deren Schutz zu ergreifen und umzusetzen. Mit Beschluss vom 16. April 2025 will der Regierungsrat befristete Stellen für den Aufbau und die Weiterentwicklung des ISMS in den Direktionen und der Staatskanzlei einsetzen, was zeigt, dass sich das ISMS weiterhin in Entwicklung befindet. Damit sich wirkungsvolle Strukturen zur Umsetzung der Informationssicherheit etablieren können, sind im Bereich der Management-Attention Verbesserungen angezeigt.

In Bezug auf die kantonale Sicherheitsorganisation stellen sich verschiedene Governance-Fragen. Allgemein ist aus Sicht der PUK Datensicherheit die bisherige dezentrale Herangehensweise im Bereich der Informationssicherheit mit Risiken verbunden.

Die Governance ist zu überdenken. Die heutige Situation mit verschiedenen strategischen und rechtlichen Vorgaben im Bereich der Informationssicherheit (IKT-Strategie, Digitalisierungsstrategie 2025+, Informationssicherheitsstrategie, Allgemeine Informationssicherheitsrichtline) gilt es weiter zu bereinigen. Schliesslich ist die Aufsicht im Bereich der Informationssicherheit zu stärken.

10. Haben weitere zuständige kantonale Stellen und Behörden zeitnah die nötigen Schritte unternommen, um den Datensicherheitsvorfall aufzuarbeiten und sicherzustellen, dass ähnliche Vorfälle verhindert werden können?

Erkenntnisse aus Kapitel 16

Die PUK Datensicherheit liess sich im Rahmen ihrer Untersuchung von den konsolidierten, selbständigen öffentlich-rechtlichen Anstalten zum Stand der Informationssicherheit informieren. Die meisten Anstalten gaben an, nach dem Bekanntwerden des Datensicherheitsvorfalls, abgesehen von der erneuten Überprüfung der Prozesse in Einzelfällen, keine zusätzlichen Massnahmen ergriffen zu haben. Die Universität Zürich teilte hingegen mit, nach dem Vorfall die Stelle des Chief Information Security Officer (CISO) eingerichtet zu haben.

Aus den Antworten ging zudem hervor, dass in Bezug auf die Informationssicherheit zwischen den Anstalten wesentliche Unterschiede bestehen, selbst wenn diese vergleichbare Aufgaben erfüllen oder derselben Direktion zugeordnet sind. Viele der vorgelegten Regelwerke und Vorgaben zur Informationssicherheit wurden erst in den letzten Jahren eingeführt. Zur Sicherheitsorganisation lässt sich festhalten, dass nur ein Teil der Anstalten eine eigene CISO-Stelle etabliert hat.

11. Kantonsrätliche Fragen zur mutmasslichen Datenvernichtung im Zusammenhang mit einer Aufräumaktion innerhalb der JI-Informatik im Jahr 2019

Erkenntnisse aus Kapitel 11

Im Rahmen der Kantonsratsdebatte vom 9. Januar 2023 stellten verschiedene Ratsmitglieder Fragen zu den Umständen der Aktenvernichtung im Jahr 2019, die im Zuge der Administrativuntersuchung bekannt geworden war. Es stand zwischenzeitlich die Vermutung im Raum, dass der Leiter der JI-Informatik (2018–2020) einen Auftrag zur Aktenvernichtung erteilt habe. Aus Sicht der PUK Datensicherheit bestand vonseiten des damaligen Leiters der JI-Informatik, Axel Mayer, zwar ein Auftrag, die Büros, namentlich den Helpdesk, aufzuräumen. Es handelte sich aber ausdrücklich nicht um einen Auftrag zur Aktenvernichtung, sondern es ging darum, Ordnung zu schaffen. Überdies geht die PUK Datensicherheit inzwischen davon aus, dass in diesem Zusammenhang wohl die Inventarblätter, welche einzelne Gerätemutationen dokumentierten, weggekommen sind. Es ist aber nicht davon auszugehen, dass wesentliche Unterlagen, wie Verträge, Auftragspapiere oder Regelungen, auf diese Weise abhandengekommen sind.

Die PUK Datensicherheit hat zu ihren Feststellungen verschiedene Empfehlungen formuliert und in Kapitel 18 zusammengestellt.

Inhaltsverzeichnis

Abbildungsverzeichnis **16**

Tabellenverzeichnis **17**

Übersicht zu den Verantwortlichkeiten und Zuständigkeiten **18**

Abkürzungsverzeichnis PUK Datensicherheit **20**

Bericht **23**

1. Auftrag der Parlamentarischen Untersuchungskommission 23
- 1.1 Gesetzliche Grundlagen 23
- 1.2 Einsetzung der Parlamentarischen Untersuchungskommission Datensicherheit 23
- 1.3 Minderheitsantrag 25

2. Arbeitsweise 26
- 2.1 Mitglieder 26
- 2.2 Organisation 27
- 2.3 Verfahrensrechte und Verfahrensgrundsätze 27
- 2.4 Vorgehen 32

3. Kosten 45
- 3.1 Kostenschätzung 45
- 3.2 Kosten bis 21. November 2025 45

4. Kantonsrätliche Geschäfte und Vorstösse zum Datensicherheitsvorfall im Kanton Zürich 46

5. Kantonale Entwicklung 1990–2005: Herausforderung Informationssicherheit in Zeiten des technologischen Wandels 47
- 5.1 Kantonale Organisation der Informatik in den 1990er-Jahren 47
- 5.2 Erste rechtliche Grundlagen zur Informationssicherheit 48
- 5.3 Sicherheitsinitiative 2004 53
- 5.4 Würdigung durch die PUK 53

6. Kantonale Entwicklung 2006–2014: Das KITT-Umfeld und die gescheiterte Umsetzung der Informatikstrategie 2008 55
- 6.1 KITT-Umfeld 55
- 6.2 Informatikleitbild 2006 58
- 6.3 Vorgaben zur Informationssicherheit im Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007 59
- 6.4 Informatikstrategie 2008 und deren Umsetzung 60
- 6.5 Berichte der Finanzkontrolle zur Situation der kantonalen Informatik 62
- 6.6 Stand der Umsetzung der Informatiksicherheit im Jahr 2014 64
- 6.7 Einschätzung der Geschäftsprüfungskommission (GPK) im Rückblick 65
- 6.8 Würdigung durch die PUK 66

7. Informationssicherheit in der Direktion der Justiz und des Innern (JI) mit Fokus auf die Beschaffungs- und Entsorgungsprozesse von 2000–2014 68
- 7.1 Rechtliche Rahmenbedingungen und interne Regelwerke 68
- 7.2 Technische Informationssicherheit und Bewusstsein 73
- 7.3 Aufbau einer IT-Sicherheitsorganisation 78
- 7.4 Würdigung durch die PUK 79

8. Ausmass und Hintergründe des Datensicherheitsvorfalls 80
8.1 Ausmass des Datensicherheitsvorfalls 80
8.2 Umstände der Auftragsvergabe an den externen Dienstleister 82
8.3 Abläufe innerhalb der Direktion in der Praxis 87
8.4 Erneuerung der PC-Arbeitsplätze 95
8.5 Entsorgungen mit dokumentierter Beteiligung des externen Dienstleisters 97
8.6 Feststellungen der Finanzkontrolle 2014 100
8.7 Würdigung durch die PUK 103

9. 2000–2014: Entsorgungspraxis in den Direktionen und der Staatskanzlei 106
9.1 Einleitung 106
9.2 Situation in der Staatskanzlei 106
9.3 Situation in der Sicherheitsdirektion 107
9.4 Situation in der Finanzdirektion 108
9.5 Situation in der Volkswirtschaftsdirektion 108
9.6 Situation in der Gesundheitsdirektion 109
9.7 Situation in der Bildungsdirektion 109
9.8 Situation in der Baudirektion 110
9.9 Würdigung durch die PUK 110

10. Kantonale Entwicklung 2015–2019: Schritte auf dem Weg zum heutigen System der Informationssicherheit 111
10.1 Informationssicherheitsorganisation 111
10.2 Regelwerk Informationssicherheit 114
10.3 Entwicklung der kantonalen Informatik 119
10.4 Würdigung durch die PUK 125

11. Entwicklungen in der Direktion der Justiz und des Innern (JI) 2015–2020 127
11.1 Personelle und organisatorische Anpassungen 127
11.2 Räumungsaktion 2019 131
11.3 Würdigung durch die PUK 134

12. Umgang mit dem Datensicherheitsvorfall nach dem internen Bekanntwerden 137
12.1 Bereits laufende Verfahren der Staatsanwaltschaften 137
12.2 Kenntnisnahme durch die Direktion der Justiz und des Innern (JI) 138
12.3 Durchführung der Administrativuntersuchung 140
12.4 Exkurs: Administrativuntersuchungen im Allgemeinen 143
12.5 Meldung an die Datenschutzbeauftragte 143
12.6 Mündliche Information an den Gesamtregierungsrat 145
12.7 Erste Information an die Geschäftsprüfungskommission (GPK) 146
12.8 Würdigung durch die PUK 147

13. Umgang mit dem Datensicherheitsvorfall nach dem öffentlichen Bekanntwerden 148
13.1 Abgabe von Informationen an Behörden und Medien anlässlich der Berufungsverhandlung vom 4. November 2022 148
13.2 Bekanntmachung durch die Anfrage KR-Nr. 456/2022 148
13.3 Datensicherheitsvorfall in den Medien 149
13.4 Reaktion der Direktion der Justiz und des Innern (JI) 150
13.5 Ausweitung des Strafverfahrens 151
13.6 Point de Presse vom 6. Dezember 2022 151
13.7 Vertiefte Nachfrage durch die dringliche Interpellation KR-Nr. 462/2022 152
13.8 Eklat am Rande der Kantonsratssitzung vom 19. Dezember 2022 153

13.9 Zweite Information an die Geschäftsprüfungskommission (GPK) 154
13.10 Missverständnis zwischen der Direktion der Justiz und des Innern (JI) und der Datenschutzbehörde bezüglich der Information der Öffentlichkeit 155
13.11 Ausbleibende Information an die Finanzkontrolle 155
13.12 Umfassende Information des Gesamtregierungsrates 156
13.13 Massnahmen der Direktion der Justiz und des Innern (JI) 157
13.14 Abklärungen in den anderen Direktionen 161
13.15 Einstellung des Strafverfahrens 163
13.16 Würdigung durch die PUK 163

14. Heutiges kantonales System der Informationssicherheit 167
14.1 Geltendes Regelwerk 167
14.2 Aktuelle Sicherheitsorganisation 177
14.3 Kantonale Angebote zur Informationssicherheit 185
14.4 Koordination 189
14.5 Rolle weiterer Aufsichtsorgane 190
14.6 Rolle der parlamentarischen Aufsichtskommissionen 191
14.7 Würdigung durch die PUK 192

15. Stand der Informationssicherheit in den Direktionen und der Staatskanzlei 197
15.1 Einleitung 197
15.2 Direktionsinterne Grundlagen 197
15.3 Sicherheitsorganisation 199
15.4 Umsetzung der Informationssicherheit 200
15.5 Direktionsinterne Audittätigkeit 202
15.6 Würdigung durch die PUK 202

16. Stand der Informationssicherheit in den selbständigen öffentlich-rechtlichen Anstalten 204
16.1 Einleitung 204
16.2 Umsetzung der Informationssicherheit 204
16.3 Würdigung durch die PUK 206

17. State of the Art und diesbezügliche Entwicklungen 207
17.1 Einleitung 207
17.2 Standards und Zertifizierungen 207
17.3 Arten der Datenvernichtung und -löschung 208
17.4 Risikoreduzierende Massnahmen 209
17.5 Praxis der Datenvernichtung und -löschung 209
17.6 Datenträgerentsorgung und Datenvernichtung im Bankensektor 211
17.7 Würdigung durch die PUK 212

18. Empfehlungen der PUK Datensicherheit 214
18.1 Koordination und Zusammenarbeit innerhalb des Regierungsrates 214
18.2 Strategische Grundlagen, strategische Steuerung und Begleitung durch den Regierungsrat 214
18.3 Rechtliche Grundlagen 215
18.4 Sicherheitsorganisation 216
18.5 Koordinierte Weiterentwicklung der Informationssicherheit in den Direktionen und der Staatskanzlei 216
18.6 Informationssicherheit bei von der AISR nicht erfassten kantonalen Stellen 217
18.7 Kommunikation 218
18.8 Interne und externe Aufsicht und Oberaufsicht 218

Abbildungsverzeichnis

Abbildung 1 Zuständigkeiten und Verantwortlichkeiten im Zeitverlauf 18

Abbildung 2 Übersicht basierend auf dem Untersuchungskonzept 35

Abbildung 3 Umsetzung der Massnahmen der ISV 52

Abbildung 4 Kaskade zu den Grundlagen der Informationssicherheit 70

Abbildung 5 Geleistete Stunden gemäss den vorliegenden Arbeitsrapporten 89

Abbildung 6 Am 19. Dezember 2022 sichergestellte Akten, inkl. Behältnis 153

Abbildung 7 Aufbau des Regelwerks gemäss AISR 1.0 168

Abbildung 8 Aufbau des Regelwerks gemäss AISR 2.0 172

Tabellenverzeichnis

Tabelle 1	Mitglieder der PUK Datensicherheit	26
Tabelle 2	Koordination mit dem Strafverfahren	33
Tabelle 3	Aktenbeizüge von der Staatsanwaltschaft III	33
Tabelle 4	Gliederung des Schlussberichts	36
Tabelle 5	Befragungen im Rahmen der Informationsbeschaffungsphase	38
Tabelle 6	Betroffene Personen gemäss Beschluss vom 12. Januar 2024	39
Tabelle 7	Befragungen im Rahmen der Sachverhaltsermittlungsphase	40
Tabelle 8	Weitere als betroffen bezeichnete Personen	42
Tabelle 9	Kantonsrätliche Geschäfte und Vorstösse zum Datensicherheitsvorfall	46
Tabelle 10	Prinzipien des Datenschutzes und der Informationssicherheit	48
Tabelle 11	IDG-Bestimmungen zur Informationssicherheit	60
Tabelle 12	Grundsätze der Informationssicherheit	60
Tabelle 13	Zuständigkeiten gemäss Informatikstrategie der JI vom 14. Februar 2011	69
Tabelle 14	Übersicht zu den sichergestellten Datenträgern	81
Tabelle 15	Übersicht zu den IT-Ersatzbeschaffungen der JI	95
Tabelle 16	Übersicht zu Speicherkomponenten mit Entsorgungsbeteiligung von André Gisler	98
Tabelle 17	Zuständigkeiten für die Umsetzung der Informations- und Cybersicherheit	178
Tabelle 18	Zuständigkeiten für die Umsetzung der IKT-Strategie sowie der Strategie Digitaler Wandel an den Schulen der Sek II	178
Tabelle 19	Weisungen und Vorgaben zum Umgang mit Informatikmitteln und zur Informationssicherheit	197
Tabelle 20	Weisungen zum Umgang mit Informationen (Informationsverwaltung)	198
Tabelle 21	Vorgaben zur Klassifizierung von Informationen	198

Übersicht zu den Verantwortlichkeiten und Zuständigkeiten

Die Darstellung zeigt die verschiedenen Zuständigkeiten im Zeitverlauf (Abbildung 1). Es sind jene Zuständigkeiten abgebildet, welche im Rahmen des Schlussberichts auch behandelt werden.

Abbildung 1 Zuständigkeiten und Verantwortlichkeiten im Zeitverlauf

	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
Regierungsrat														
SK	Beat Husi													
JI		Markus Notter												
DS														
FD														
VD														
GD														
BI														
BD												Ursula Gut-Winterberger		
Sicherheitsorganisation														
I-SiBe/ISIK														
Direktion JI														
GS JI														
Leiter LFC					Renato Widmer									
Leiter JI-Informatik		Leiter (1996–2000)					Fredi Steiner							
Behörden														
DSB	Bruno Baeriswyl													
Finanzkontrolle														

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
									Kathrin Arioli							
		Martin Graf				Jacqueline Fehr										
		Mario Fehr														
Ursula Gut-Winterberger						Ernst Stocker										
	Ernst Stocker					Carmen Walker Späh										
										Natalie Rickli						
						Silvia Steiner										
										Martin Neukom						
						Renzo Mühlebach					Philipp Grabher					
Christian Zünd							Jacqueline Romer									
						Fredi Steiner (IT-Leitung ad interim)										
(ab 2016 Hauptabteilung Informatik)									Axel Mayer			Urs Kaderli (ab 2021 DigiSol)				
											Dominika Blonski					
Martin Billeter																

Abkürzungsverzeichnis PUK Datensicherheit

A	**AFI**	Amt für Informatik
	AGB	Allgemeine Geschäftsbedingungen
	AGB SIK	Von der Schweizerischen Informatikkonferenz (SIK) erarbeitete AGB für IKT-Leistungen
	AGIK	Arbeitsgruppe Planung und Steuerung der Informatik und Kommunikation
	AID	Amt für Informatikdienste
	AIP	Abteilung für Informatikplanung
	AISR	Allgemeine Informationssicherheitsrichtlinie
	AJB	Amt für Jugend und Berufsberatung
	AOI	Abteilung für Organisation und Informatik
B	**BD**	Baudirektion des Kantons Zürich
	BDO AG	Schweizer Wirtschaftsprüfungs-, Treuhand- und Beratungsgesellschaft
	BI	Bildungsdirektion des Kantons Zürich
	BISR	Besondere Informationssicherheitsrichtlinien
	BSC	Abteilung Business Support & Compliance im Generalsekretariat der JI
C	**CBA AG**	Computer Broker AG
	CC I-Si	Competence Center Informatik-Sicherheit
	CCSC	Cantonal Cyber Security Centre / Kantonales Zentrum für Cybersicherheit
	CISO	Chief Information Security Officer
	CRG	Gesetz über Controlling und Rechnungslegung vom 9. Januar 2006
D	**DAP**	Digitaler Arbeitsplatz
	DigiSol	Digital Solutions (Informatikabteilung der JI)
	Dir	Direktion
	DS	Sicherheitsdirektion des Kantons Zürich
	DSB	Datenschutzbeauftragte/r
	DSC2	Digital Security Control Center
	DSG	Gesetz über den Schutz von Personendaten vom 6. Juni 1993 (Datenschutzgesetz)
	DSGVO	Datenschutz-Grundverordnung der Europäischen Union
	DSV	Datenschutzverordnung vom 7. Dezember 1994
E	**EKZ**	Elektrizitätswerke des Kantons Zürich
	ERZ	Entsorgung und Recycling Zürich
F	**FAGIS**	Fachgruppe IKT-Sicherheit / Fachgruppe Informationssicherheit
	FCL	Abteilung Finanzen, Controlling und Logistik im Generalsekretariat der JI
	FD	Finanzdirektion des Kantons Zürich
	FIKO	Finanzkommission
	FINMA	Eidgenössische Finanzmarktaufsicht
	FG I-Si	Fachgruppe Informatiksicherheit (später FAGIS)
G	**GATT/WTO**	General Agreement on Tariffs and Trade / World Trade Organization
	GD	Gesundheitsdirektion des Kantons Zürich
	GeschR	Geschäftsreglement der PUK Datensicherheit vom 6. Oktober 2023
	GEVER	(Elektronische) Geschäftsverwaltung
	GPK	Geschäftsprüfungskommission
	GS	Generalsekretariat
	GSK	Konferenz der Generalsekretärinnen und Generalsekretäre
	GVZ	Gebäudeversicherung Kanton Zürich

H	**HERMES**	Managementmethode für das Durchführen von Projekten und Programmen (Projektmanagement)
I	**IAM**	Identity and Access Management (Identitäts- und Zugriffsmanagement)
	IBIS08	Informatik BasisInfrastruktur Sicherheitsdirektion 2008
	IDG	Gesetz über die Information und den Datenschutz vom 12. Februar 2007
	IDV	Verordnung über die Information und den Datenschutz vom 28. Mai 2008
	IKS	Internes Kontrollsystem
	IKT	Informations- und Kommunikationstechnologien
	ISDS	Informationssicherheit- und Datenschutzkonzept
	ISiA	Informationssicherheitsbeauftragte/r in den Ämtern
	ISID	Informatik-Sicherheitsbeauftragte/r der Direktion oder Staatskanzlei / Informationssicherheitsbeauftragte/r der Direktion oder Staatskanzlei
	I-SiBeZH	Informatik-Sicherheitsbeauftragte/r des Kantons Zürich
	ISIK	Informationssicherheitsbeauftragte/r des Kantons (Neubezeichnung für I-SiBeZH), in AISR 1.0 noch Informatiksicherheitsbeauftragte/r
	I-SixD	Informatik-Sicherheitsbeauftragte/r der Direktion/Staatskanzlei (frühere Abkürzung)
	ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
	ISMS	Informationssicherheits-Managementsystem / Managementsystem für die Informatik-Sicherheit
	ISSE	Kantonale Informationssicherheitsservices
	ISST	Kantonale Informationssicherheitsstandards
	IT	Informatik
	IT JI	Hauptabteilung Informatik der JI (ab 1. Juli 2021 offiziell Digital Solutions)
	ISV	Informatiksicherheitsverordnung vom 17. Dezember 1997
	IVSV	Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019
	IVAD	Informatik-Beauftragter der Direktionen und der Staatskanzlei
	IZ-AOI	Informatikzentrum der Abteilung für Organisation und Informatik
J	**JI**	Direktion der Justiz und des Innern des Kantons Zürich
	JIOV	Organisationsverordnung der Direktion der Justiz und des Innern
	JUKO	Justizkommission
	JuWe	Amt für Justizvollzug und Wiedereingliederung
K	**KAPO**	Kantonspolizei Zürich
	kdmz	Kantonale Drucksachen- und Materialzentrale
	KFO	Kantonale Führungsorganisation
	KI	Künstliche Intelligenz
	KITT	Kantonales IT-Team
	KOSIF	Kommission für strategische Informatikführung
	KRG	Kantonsratsgesetz vom 25. März 2019
	KRR	Kantonsratsreglement vom 25. März 2019
L	**LFC**	Abteilung Logistik, Finanzen und Controlling im Generalsekretariat der JI
	LOSTA	Leitender Oberstaatsanwalt
M	**MBA**	Mittelschul- und Berufsbildungsamt
	MM	Medienmitteilung
N	**NB**	Notebook
	NIS	Neue Informatikstrategie
	NIST	National Institute of Standards and Technology
	NVM	Non-Volatile Memory
	NVMe	Non-Volatile Memory Express

O	**OG RR**	Gesetz über die Organisation des Regierungsrates und der kantonalen Verwaltung vom 6. Juni 2005
	OIS	Operative Informatiksteuerung (Gremium)
	ORGS	Organisationsreglement des Generalsekretariates (der JI)
	OSTA	Oberstaatsanwaltschaft
	OV	Organisationsverordnung
P	**PHZH**	Pädagogische Hochschule Zürich
	PIN	Personal Identification Number
	PJZ	Polizei- und Justizzentrum
	PKI	Public Key Infrastructure
	PUK	Parlamentarische Untersuchungskommission
	PUK	Psychiatrische Universitätsklinik Zürich
	PUK BVK	Parlamentarische Untersuchungskommission BVK Personalvorsorge des Kantons Zürich
Q	**QM**	Qualitätsmanagement
R	**RAID**	Redundant Array of Independent Disks
	RIS1/RIS2	Rechtsinformationssystem der Direktion der Justiz und des Innern
	RIVA	Risikoverantwortliche/r
	RLV	Rechnungslegungsverordnung vom 29. August 2007
	RR	Regierungsrat
	RRB	Regierungsratsbeschluss
S	**SDI**	Steuerung Digitale Verwaltung und IKT (Gremium)
	SEC	Projekt zur IKT-Sicherheit der kantonalen IKT-Strategie
	SECO	Staatssekretariat für Wirtschaft
	SFR	Bereich Support, Führung und Recht des Generalsekretariats der JI
	SK	Staatskanzlei des Kantons Zürich
	SOA	Statement of Applicability (Dokument, welches Auskunft über den Status der implementierten Sicherheitskontrollen gibt und allfällige Ausschlüsse begründet)
	SOC	Security Operation Center
	SRD	Stabs- und Rechtsdienst des Generalsekretariats (ab 2015)
	SSD	Solid-State-Disk
	StaZH	Staatsarchiv des Kantons Zürich
	STA.ZH	Staatsanwaltschaft Zürich
	StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007
T	**TFT-Display**	Flachbildschirm mit Dünnschichttransistor (thin-film transistor)
U	**UZH**	Universität Zürich
V	**VD**	Volkswirtschaftsdirektion des Kantons Zürich
	VOG RR	Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung vom 18. Juli 2007
	VPN	Virtual Private Network
W	**WIF!**	Wirkungsorientierte Führung der Verwaltung des Kantons Zürich
	WOV	Wirkungsorientierte Verwaltungsführung
	WOSTA	Weisungen der Oberstaatsanwaltschaft
Z	**ZB**	Zentralbibliothek
	ZKB	Zürcher Kantonalbank
	ZPO	Schweizerische Zivilprozessordnung vom 19. Dezember 2008
2	**2FA**	Zwei-Faktoren-Authentifizierung

Bericht

1. Auftrag der Parlamentarischen Untersuchungskommission

1.1 Gesetzliche Grundlagen

Bedürfen Vorkommnisse von grosser Tragweite im Zuständigkeitsbereich der parlamentarischen Kontrolle des Kantonsrates der Klärung, kann zur Ermittlung der Sachverhalte und zur Beschaffung weiterer Beurteilungsgrundlagen eine Parlamentarische Untersuchungskommission eingesetzt werden.[1]

1.2 Einsetzung der Parlamentarischen Untersuchungskommission Datensicherheit

1.2.1 Erste Diskussionen zum Datensicherheitsvorfall

Die Anfrage KR-Nr. 456/2022 vom 28. November 2022 im Kantonsrat machte den bis dahin erst intern bekannten Datensicherheitsvorfall öffentlich. Die Anfrage hielt fest, dass zahlreiche eigentlich zur Entsorgung vorgesehene Computerfestplatten mit teilweise hochsensiblen, ungelöschten bzw. mühelos wieder lesbar gemachten Daten an verschiedene Personen im Zürcher Drogen- und Sexmilieu gelangt seien. Die Vorfälle, aber auch die diesbezüglichen Verantwortlichkeiten der Direktion der Justiz und des Innern (JI) sowie deren Vorsteherin, Jacqueline Fehr, waren ab dem 2. Dezember 2022 auch im Fokus der Medien. Verschiedenen Medienschaffenden wurden auch Unterlagen zugespielt. Die JI bestätigte in ihrer ersten Medienmitteilung vom 2. Dezember 2022 lediglich, dass es einen Datensicherheitsvorfall gegeben habe, und kommunizierte ansonsten äusserst zurückhaltend. Als jedoch klar wurde, dass viele Informationen bereits im Umlauf waren, setzte die JI für den 6. Dezember 2022 einen Point de Presse an und informierte über den Vorfall und die diesbezüglichen Massnahmen der JI. In diesem Rahmen zeigte sich die Direktionsvorsteherin, Jacqueline Fehr, gegenüber möglichen Abklärungen der Geschäftsprüfungskommission des Kantonsrates (GPK) oder der Einsetzung einer Parlamentarischen Untersuchungskommission (PUK) offen. Die GPK nahm sich der Sache an und lud die Direktionsvorsteherin der JI am 8. Dezember 2022 zum Gespräch ein. Sie beschloss angesichts der grossen politischen Bedeutung des Datensicherheitsvorfalls, eine Subkommission einzusetzen, um vertiefte Abklärungen vorzunehmen (Umgang der JI und allfälliger weiterer kantonaler Stellen mit dem Datensicherheitsvorfall, Umsetzung der Empfehlungen aus der Administrativuntersuchung, aktueller Umfang des Vorfalls mit Daten und Informationen in der JI).[2] An ihrer Sitzung vom 12. Dezember 2022 legte die GPK die Zusammensetzung und den Auftrag der Subkommission fest.[3]

Nach § 115 Abs. 2 lit. a KRG[4] können Aufsichtskommissionen die Einsetzung einer PUK beantragen, nachdem sie eigene Prüfungen und Abklärungen zu diesen Vorkommnissen vorgenommen haben. Gemäss § 115 Abs. 2 lit. b KRG können auch Kan-

---

1 § 115 Abs. 1 Kantonsratsgesetz vom 25. März 2019 (KRG; LS 171.1).

2 Protokoll der Sitzung der Geschäftsprüfungskommission vom 8. Dezember 2022; Geschäftsprüfungskommission, Medienmitteilung vom 8. Dezember 2022 «GPK leitet Untersuchung zum Umgang der JI mit dem Datenmissbrauchsvorfall ein».

3 Protokoll der Sitzung der Geschäftsprüfungskommission vom 12. Dezember 2022.

4 Kantonsratsgesetz vom 25. März 2019 (KRG; LS 171.1).

tonsratsmitglieder die Einsetzung einer PUK verlangen, wenn vorgängig mit einer Interpellation Aufschluss über die Vorkommnisse verlangt worden war. Im Rahmen der Debatte des Kantonsrates über die dringliche Interpellation KR-Nr. 462/2022, die am 5. Dezember 2022 eingereicht worden war, forderten verschiedene Ratsmitglieder die Einsetzung einer PUK. Im Nachgang zu dieser Debatte ging deshalb bei der GPK ein Antrag zur Einsetzung einer PUK ein.

1.2.2 Antrag der Geschäftsprüfungskommission vom 27. April 2023

Am 26. Januar 2023 beschloss die GPK, dem Kantonsrat einen Antrag auf Einsetzung einer PUK zu stellen.[5] Sie informierte die Öffentlichkeit über ihren Entscheid und die parallele Fortführung der Abklärungen der Subkommission.[6] Die Subkommission führte in der Folge die im Mandat festgehaltenen Untersuchungen durch und wurde von der GPK zusätzlich beauftragt, den Antrag auf Einsetzung einer PUK vorzubereiten.[7] Die Subkommission hörte am 26. Januar 2023 die Datenschutzbeauftragte, Dominika Blonski, und am 2. Februar 2023 den Leitenden Oberstaatsanwalt, Andreas Eckert, an. Die GPK schliesslich verabschiedete an der Sitzung vom 27. April 2023 ihren Bericht und den Antrag auf Einsetzung einer PUK (KR-Nr. 172/2023).

1.2.3 Auftrag der Parlamentarischen Untersuchungskommission Datensicherheit

Der Kantonsrat folgte diesem Antrag am 3. Juli 2023 mit 92 zu 76 Stimmen und setzte eine PUK mit folgendem Auftrag ein:[8]

«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;
– 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;

---

5 Protokoll der Sitzung der Geschäftsprüfungskommission vom 26. Januar 2023.

6 Geschäftsprüfungskommission, Medienmitteilung vom 26. Januar 2023 «PUK soll Datenmissbrauchsvorfall untersuchen».

7 Protokoll der Sitzung der Geschäftsprüfungskommission vom 9. Februar 2023.

8 Protokoll der Sitzung des Kantonsrates vom 3. Juli 2023, S. 3–60; Antrag der Geschäftsprüfungskommission vom 27. April 2023 (KR-Nr. 172/2023).

– 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 Kostenschätzung 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.»

1.3 Minderheitsantrag

Vier Mitglieder der GPK (Davide Loss, Leandra Columberg, Manuel Kampus und Manuel Sahli) stellten einen Minderheitsantrag und beantragten die Ablehnung der Einsetzung einer PUK. Der Minderheitsantrag wurde in der Folge abgelehnt.[9]

[9] Antrag der Geschäftsprüfungskommission vom 27. April 2023 (KR-Nr. 172/2023).

2. Arbeitsweise

2.1 Mitglieder

Am 4. September 2023 wählte der Kantonsrat auf Antrag der Interfraktionellen Konferenz (IFK) folgende Mitglieder in die PUK Datensicherheit (KR-Nr. 274/2023; Tabelle 1):[10]

Tabelle 1 Mitglieder der PUK Datensicherheit

Scherrer	**Benno**	**(GLP, Uster; Präsident)**
Bänninger	Michael	(EVP, Winterthur)
Bürgin	Yvonne	(Die Mitte, Rüti)
Camenisch	Linda	(FDP, Wallisellen)
Dalcher	Pierre	(SVP, Schlieren)
Dietschi	Urs	(Grüne, Lindau)
Hoss-Blatter	Corinne	(FDP, Zollikon)
Loss	Davide	(SP, Thalwil)
Meyer	Karl Heinz	(SVP, Neerach)
Pflugshaupt	Elisabeth	(SVP, Gossau)
Sahli	Manuel	(AL, Winterthur)
Stüssi	Beatrix	(SP, Niederhasli)

2.1.1 Präsident und Vizepräsident

Als Präsidenten der PUK Datensicherheit wählte der Kantonsrat Benno Scherrer.[11] An ihrer zweiten Sitzung wählte die PUK Datensicherheit Michael Bänninger zu ihrem Vizepräsidenten.[12]

2.1.2 Mitgliedermutation

Anlässlich der ersten Sitzung legten die PUK-Mitglieder allfällige Kontakte und Verbindungen offen, die den Anschein der Befangenheit in Bezug auf das laufende Strafverfahren im Zusammenhang mit dem Datensicherheitsvorfall begründen könnten. Pierre Dalcher wies insbesondere darauf hin, dass er als Bezirksrat in seiner Funktion der JI angehöre und dass er diese Angelegenheit vor seinem Einsitz in die PUK Datensicherheit mit dem Statthalter und dem Fraktionspräsidenten besprochen habe. Davide Loss hielt weiter fest, dass er den Leitenden Oberstaatsanwalt, Andreas Eckert, aus seiner beruflichen und politischen Tätigkeit kenne, mit ihm aber weder besonders befreundet noch verfeindet oder sonst eng verbunden sei. Die PUK Datensicherheit kam zum Schluss, dass bei keinem PUK-Mitglied eine Befangenheit vorliegt.[13]

Im Rahmen der Gesamterneuerungswahl des Nationalrates vom 22. Oktober 2023 wurde das bisherige PUK-Mitglied Yvonne Bürgin in den Nationalrat gewählt. Sie trat deshalb während der laufenden Legislaturperiode 2023–2027 aus dem Kantonsrat und der PUK Datensicherheit zurück. Als ihre Nachfolgerin in der PUK Datensicherheit wählte der Kantonsrat Marzena Kopp (Die Mitte, Meilen).[14] Marzena Kopp bestätigte

[10] Protokoll der Sitzung des Kantonsrates vom 4. September 2023, S. 5–6.

[11] Protokoll der Sitzung des Kantonsrates vom 4. September 2023, S. 5–6.

[12] Protokoll der Sitzung der PUK Datensicherheit vom 6. Oktober 2023, S. 4–5.

[13] Protokoll der Sitzung der PUK Datensicherheit vom 22. September 2023, S. 14.

[14] KR-Nr. 364/2023; Protokoll der Sitzung des Kantonsrates vom 20. November 2023, S. 4.

ebenfalls, dass sie keine Kontakte und Verbindungen pflege, die den Anschein der Befangenheit in Bezug auf das laufende Strafverfahren im Zusammenhang mit dem Datensicherheitsvorfall begründen könnten.[15]

2.2 Organisation

2.2.1 Geschäftsreglement vom 6. Oktober 2023

Die PUK Datensicherheit verabschiedete ein Geschäftsreglement, in welchem insbesondere ihr Auftrag, die Organisation der Arbeit, die Geheimhaltung und der Geheimnisschutz sowie die Information der Öffentlichkeit geregelt wurden.[16] Am 27. Oktober 2023 präzisierte die PUK Datensicherheit die Regelung zur Zulässigkeit von Kopien.[17] Das Geschäftsreglement wurde am 24. November 2023 um einen Absatz ergänzt, der den Umgang mit persönlichen Notizen innerhalb des Geschäftsverwaltungssystems regelt.[18]

2.2.2 Sekretariat

Das Sekretariat der PUK Datensicherheit wurde von den Parlamentsdiensten des Kantonsrates geführt, wobei Heiri Gander, wissenschaftlicher Mitarbeiter, als Sekretär der PUK Datensicherheit im Umfang von 80 Stellenprozenten eingesetzt wurde.[19] Als Entlastung wurde dem Sekretariat eine Protokollführung für die PUK Datensicherheit zugeordnet. Zudem wurde per 1. Oktober 2023 für die PUK Datensicherheit Rechtsanwältin Noëlle Glaus als Rechtskonsulentin im Umfang von 20 Stellenprozenten, befristet für die Dauer der Tätigkeit der PUK Datensicherheit, angestellt und zur Stellvertreterin des PUK-Sekretärs, Heiri Gander, ernannt.

Die Akten der PUK Datensicherheit wurden im Geschäftsverwaltungssystem des Kantonsrates abgelegt; der Zugriff auf diese Akten war auf die PUK-Mitglieder, den PUK-Sekretär, die Rechtskonsulentin und die Protokollführerin beschränkt. Im Haus zum Rechberg stand ein Büro mit abschliessbaren Schränken zur Verfügung. Aufgrund der Vertraulichkeit der physischen Akten, deren Anzahl durch die elektronische Ablage im Geschäftsverwaltungssystem auf ein Minimum reduziert war, hatten lediglich der PUK-Sekretär und die Rechtskonsulentin Zugang zu diesen Schränken, weiteren Personen war der Zugang verwehrt.

2.3 Verfahrensrechte und Verfahrensgrundsätze

2.3.1 Gesetzliche Grundlagen

Im Kantonsratsgesetz vom 25. März 2019 (KRG; LS 171.1) finden sich zu Auftrag, Einsetzung und Verfahren einer PUK insgesamt neun Bestimmungen.[20] Das Gesetz äussert sich zu verschiedenen Verfahrensfragen nicht im Detail, verweist jedoch für die Vornahme von Augenscheinen und den Beizug von Sachverständigen auf die Be-

---

15 Protokoll der Sitzung der PUK Datensicherheit vom 24. November 2023, S. 3.

16 Protokoll der Sitzung der PUK Datensicherheit vom 6. Oktober 2023, S. 9–12.

17 Protokoll der Sitzung der PUK Datensicherheit vom 27. Oktober 2023, S. 21.

18 Protokoll der Sitzung der PUK Datensicherheit vom 24. November 2023, S. 8–9.

19 Beschluss des Kantonsrates vom 3. Juli 2023, Ziffer IV.

20 §§ 115–123 KRG.

stimmungen der Schweizerischen Zivilprozessordnung (ZPO)[21] sowie für die Einvernahme von Zeuginnen und Zeugen auf die Bestimmungen der Schweizerischen Strafprozessordnung (StPO)[22], die sinngemäss anzuwenden sind.[23]

Zudem wurden die Arbeitspapiere und Richtlinien der PUK BVK (Korruptionsfall, BVK Personalvorsorge des Kantons Zürich) beigezogen, in denen die damaligen Bestimmungen des Kantonsratsgesetzes (KRG) ausgelegt und konkretisiert worden waren. In der Zwischenzeit haben sich die Bestimmungen des KRG zur PUK geändert, weshalb die bestehenden Arbeitspapiere und Richtlinien entsprechend angepasst wurden. Die PUK Datensicherheit verabschiedete ihre eigenen Verfahrensrichtlinien in der Sitzung vom 24. November 2023.[24]

2.3.2 Ermittlung des Sachverhalts und Beweiserhebung

Die Würdigung des Sachverhalts und die Schlussfolgerungen der PUK Datensicherheit erfolgen nach freiem Ermessen. Sie orientiert sich bei der Sachverhaltsermittlung und der Beweiserhebung an den einschlägigen Prozessordnungen. Sie führt jedoch eine parlamentarische und keine gerichtliche Untersuchung durch. Ihre Mitglieder sind Parlamentarierinnen und Parlamentarier und keine Richterinnen und Richter. Die PUK Datensicherheit hat das Recht, die erhobenen Beweise frei zu würdigen. Dabei steht ihr – wie auch der Richterin oder dem Richter – ein breiter Ermessensspielraum zu. Die Beweislast für allfällige Amtspflichtverletzungen und Nachlässigkeiten liegt bei der PUK Datensicherheit. Diese hat im Rahmen des Beweisverfahrens abzuklären, ob solche Pflichtverletzungen nachgewiesen werden können. Kann dieser Beweis nicht erbracht werden, hat die PUK Datensicherheit dies zu akzeptieren und eine Belastung der Betroffenen fällt ausser Betracht.[25]

2.3.3 Vornahme von Augenscheinen und Beizug von Sachverständigen

Die PUK Datensicherheit kann im Rahmen ihrer Untersuchung Augenscheine vornehmen und Sachverständige beiziehen.[26]

2.3.4 Einholung von Auskünften und Herausgabe von Akten

Zur Sachverhaltsermittlung kann die PUK Datensicherheit von Amtsstellen, Behördenmitgliedern, Angestellten des Kantons und Privatpersonen, soweit diese der Zeugenpflicht unterstehen, mündlich oder schriftlich direkt Auskünfte einholen.[27] Weiter kann die PUK Datensicherheit von allen Personen in öffentlichen Funktionen sowie von Privatpersonen, soweit sie der Zeugenpflicht unterstehen, Akten erhalten[28] und sämtliche Akten der Verwaltung, des Regierungsrates, der Justizverwaltung, der öffentlichen Anstalten und der Finanzkontrolle beiziehen.[29]

---

21 Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (ZPO; SR 272).

22 Schweizerische Strafprozessordnung vom 5. Oktober 2007 (StPO; SR 312.0).

23 § 120 Abs. 3 KRG.

24 Richtlinien zum Verfahren der Parlamentarischen Untersuchungskommission Datensicherheit gemäss Beschluss der Parlamentarischen Untersuchungskommission Datensicherheit vom 24. November 2023.

25 Ziff. 1.3 der Richtlinien zum Verfahren der parlamentarischen Untersuchungskommission Datensicherheit; siehe auch Bericht der PUK BVK 2012, S. 6.

26 § 119 lit. a und b KRG.

27 § 119 lit. e KRG.

28 § 119 lit. f KRG.

29 § 119 lit. g KRG.

2.3.5 Befragungen von Auskunftspersonen und Einvernahme von Zeuginnen und Zeugen

Im Rahmen ihrer Untersuchung kann die PUK Datensicherheit Auskunftspersonen befragen[30] sowie Zeuginnen und Zeugen einvernehmen[31]. Die PUK Datensicherheit stützte sich bei der Rollenzuteilung jeweils auf die vorliegende Sach- und Rechtslage und entschied vor der Informationsbeschaffungsphase und vor der Sachverhaltsermittlungs- und Beweiserhebungsphase, ob eine Person als Auskunftsperson oder als Zeugin oder Zeuge zu befragen bzw. einzuvernehmen sei. In ihrer Sitzung vom 8. Dezember 2023 legte sie fest, dass sie den in § 121 Abs. 2 KRG genannten Personenkreis im Grundsatz als Auskunftspersonen befragen wird.

Amtsgeheimnis

Die Mitglieder des Regierungsrates oder eines obersten Gerichts sowie die Angestellten des Kantons sind generell vom Amtsgeheimnis entbunden.[32] Das Gleiche hat aus Sicht der PUK Datensicherheit auch für ehemalige Mitglieder des Regierungsrates oder eines obersten Gerichtes sowie für ehemalige Angestellte des Kantons zu gelten, da ihnen die Informationen, die dem Amtsgeheimnis unterliegen, während ihrer Amtszeit oder während ihrer Anstellungsdauer anvertraut worden sind. Mitglieder des Kantonsrates sind hiervon nicht erfasst und deshalb zur Aussage zu ermächtigen.

Hingegen hätte die JI Personen, die in einem Auftrags- oder Mandatsverhältnis für die JI tätig waren, vor der Befragung bzw. Einvernahme durch die PUK Datensicherheit vom Amts- oder Anwaltsgeheimnis entbinden müssen.

Einvernahme von Zeuginnen und Zeugen

Die Einvernahme von Zeuginnen und Zeugen richtet sich nach den Bestimmungen der StPO.[33] Als Zeuginnen und Zeugen gelten demnach jene Personen, die an der Begehung einer Straftat nicht beteiligt sind, die aber der Aufklärung dienende Aussagen machen können.[34] Zeuginnen und Zeugen sind verpflichtet, wahrheitsgemäss auszusagen, vorbehalten bleiben jedoch die Zeugnisverweigerungsrechte.[35] Eine Zeugin oder ein Zeuge kann gemäss Gesetz unter anderem aufgrund persönlicher Beziehungen, zum eigenen Schutz oder zum Schutz nahestehender Personen, aufgrund eines Amts- oder Berufsgeheimnisses oder aufgrund weiterer Geheimhaltungspflichten das Zeugnis verweigern.[36]

Wie bereits ausgeführt, sind Mitglieder des Regierungsrates oder eines obersten Gerichts sowie die Angestellten des Kantons vom Amtsgeheimnis entbunden, weshalb sich die entsprechenden Personen nicht auf das Zeugnisverweigerungsrecht aufgrund des Amtsgeheimnisses berufen können, sollten sie als Zeuginnen oder Zeugen einvernommen werden.[37]

Verweigert eine Zeugin oder ein Zeuge das Zeugnis, ohne dazu berechtigt zu sein, kann sie oder er mit einer Ordnungsbusse bestraft und zur Tragung der Kosten und Entschädigung verpflichtet werden, die durch die Verweigerung verursacht worden

---

30 § 119 lit. c KRG.

31 § 119 lit. d KRG.

32 § 120 Abs. 1 und 2 KRG.

33 § 120 Abs. 3 lit. d KRG.

34 Art. 162 StPO.

35 Art. 163 Abs. 2 StPO; Art. 168–176 StPO.

36 Art. 168–176 StPO.

37 § 120 Abs. 1 KRG.

sind.[38] Die Zeuginnen und Zeugen wurden im Rahmen der Einvernahme durch die PUK Datensicherheit neben ihren Zeugnis- und Wahrheitspflichten auf die strafrechtlichen Folgen der falschen Anschuldigung, der Irreführung der Rechtspflege, der Begünstigung und des falschen Zeugnisses hingewiesen.[39]

Befragung von Auskunftspersonen

Das KRG verweist hinsichtlich der Auskunftspersonen auf keine Prozessordnung, weshalb dem Begriff «Auskunftsperson» im Rahmen einer PUK eine eigenständige Bedeutung zukommt. Die Auskunftsperson ist weder im KRG noch im kantonalen Verwaltungsrechtspflegegesetz (VRG) näher definiert. Als Grundlage und zu Abgrenzungszwecken kann die Definition der StPO beigezogen werden. Demnach gelten als Auskunftspersonen unter anderem Personen, die in einer gewissen Form in den zu untersuchenden Sachverhalt involviert sind oder bei denen eine Involvierung nicht ausgeschlossen werden kann.[40] Ausgehend von dieser Definition und den Besonderheiten einer PUK sind daher im Verfahren einer PUK die Personen, gegen die sich die Untersuchung ganz oder überwiegend richten, als Auskunftspersonen zu vernehmen.

Das KRG unterscheidet bei der Befragung von Auskunftspersonen zwischen Mitgliedern des Regierungsrates, der obersten Gerichte sowie Angestellten des Kantons und anderen Auskunftspersonen:

Auskunftspersonen aus dem Regierungsrat, den obersten Gerichten und der Verwaltung

– Die Mitglieder des Regierungsrates oder eines obersten Gerichts sowie die Angestellten des Kantons sind verpflichtet, über Wahrnehmungen bezüglich des Untersuchungsgegenstandes, die sie in Ausübung ihres Dienstes gemacht haben und die ihre dienstlichen Angelegenheiten betreffen, wahrheitsgemäss und vollständig Auskunft zu erteilen (lex specialis).[41] Das Recht, sich selbst oder nahestehende Personen nicht belasten zu müssen, wird dadurch nicht aufgehoben. Die Auskunftsperson hat aber nach dem Wortlaut des Gesetzes wahrheitsgetreu und insbesondere proaktiv über die untersuchten Sachverhalte zu berichten. Über Belange, die ausserhalb des Untersuchungsauftrags liegen bzw. über ausserdienstliche Belange, ist die Auskunftsperson nicht verpflichtet auszusagen. Aufgrund der Immunität ehemaliger Regierungsmitglieder in Bezug auf ihre Handlungen und Äusserungen im Amt fallen auch diese unter die Regelung von § 120 Abs. 2 KRG.

Auskunftspersonen ausserhalb des Regierungsrates, der obersten Gerichte und der Verwaltung

– Personen, die nicht Mitglieder des Regierungsrates oder eines oberen Gerichts oder Angestellte des Kantons sind, fallen nicht unter die Regelung von § 120 Abs. 2 KRG. Sie können demnach ihre Aussage auch verweigern.

Die PUK Datensicherheit wies die Auskunftspersonen zu Beginn der Befragung auf die strafrechtlichen Folgen der falschen Anschuldigung, der Irreführung der Rechtspflege und der Begünstigung hin. Auch wenn das KRG für Auskunftspersonen ausserhalb des Regierungsrates und der Verwaltung nicht auf die StPO verweist, machte die PUK Datensicherheit die zu befragenden Personen zu Beginn der Befragung sinngemäss auf ihre Aussagepflicht, ihre Aussage- und Zeugnisverweigerungsrechte und die Verwendung ihrer Aussagen als Beweismittel aufmerksam.

---

[38] Art. 176 Abs. 1 StPO.

[39] Art. 177 Abs. 1 StPO.

[40] Art. 178–181 StPO.

[41] § 120 Abs. 2 KRG.

Protokollierung der Befragungen und Einvernahmen

Die Aussagen der Auskunftspersonen sowie der Zeuginnen und Zeugen wurden jeweils auf Tonträger aufgezeichnet und im Anschluss an die Befragung bzw. die Einvernahme in Form eines Wortprotokolls protokolliert. Die Auskunftspersonen sowie die Zeuginnen und Zeugen konnten die Protokolle im Rahmen ihres Akteneinsichtsrechts einsehen. Bei Protokollberichtigungsanträgen von Auskunftspersonen sowie Zeuginnen und Zeugen wurde der Tonträger eingesehen, die entsprechende Stelle abgehört und auf dieser Grundlage über den Berichtigungsantrag entschieden.

Entschädigung von Auskunftspersonen sowie Zeuginnen und Zeugen

Für die Entschädigung von Auskunftspersonen sowie Zeuginnen und Zeugen fand die Entschädigungsverordnung der obersten Gerichte sinngemäss Anwendung.[42]

2.3.6 Rechte der Betroffenen

Betroffenen kommen in einem Verfahren der PUK besondere Rechte zu.[43] Personen, die durch die Untersuchung einer PUK unmittelbar in ihren Interessen betroffen sind, haben das Recht, Augenscheinen, Beizügen von Sachverständigen sowie Einvernahmen von Zeuginnen und Zeugen beizuwohnen und Ergänzungsfragen zu stellen.[44] Darüber hinaus können Betroffene in die herausgegebenen Akten, die Gutachten und die Einvernahmeprotokolle einer PUK Einsicht nehmen.[45] Für die Akteneinsicht hat die PUK Datensicherheit entschieden, den Betroffenen die Akten mittels der kantonalen Plattform «WebTransferZH» bzw. über das Geschäftsverwaltungssystem des Kantonsrates zur Verfügung zu stellen.[46]

Die PUK Datensicherheit erachtete eine Person als «unmittelbar in ihren Interessen betroffen», wenn diese durch das Ergebnis der Untersuchung befürchten musste, dass ihr Verhalten im Untersuchungsbericht negativ gewürdigt wird. Für die Ermittlung der Betroffenheit ist somit von den faktischen Wirkungen des Untersuchungsberichts auszugehen, wobei keine allzu hohen Anforderungen an die unmittelbare Betroffenheit zu stellen sind.

Aus Gründen der Transparenz wurden bereits vor der Informationsbeschaffungsphase diejenigen Personen, die aufgrund der zu diesem Zeitpunkt vorliegenden Sach- und Rechtslage als Betroffene anzusehen waren, schriftlich über ihre Rolle und ihre Rechte informiert. Nach Abschluss der Informationsbeschaffungsphase wurden sodann fortlaufend die weiteren Personen, die aufgrund der vorliegenden Sach- und Rechtslage als betroffen erachtet wurden, schriftlich informiert.

Auch wenn eine unmittelbare Betroffenheit anzunehmen ist, kann die PUK Datensicherheit die Anwesenheit von Betroffenen bei der Sachverhaltsermittlung und die Akteneinsicht verweigern, sofern dies im Interesse der laufenden Untersuchung oder zum Schutz anderer Personen unerlässlich ist.[47] Wird die Anwesenheit oder die Akteneinsicht verweigert, kann auf die betreffenden Beweismittel nur dann abgestellt wer-

---

[42] Verordnung der obersten kantonalen Gerichte über die Entschädigung der Zeugen und Zeuginnen, Auskunftspersonen und Sachverständigen (Entschädigungsverordnung der obersten Gerichte; LS 211.12).

[43] § 121 KRG.

[44] § 120 Abs. 2 KRG.

[45] § 120 Abs. 3 KRG.

[46] Protokoll der Sitzung der PUK Datensicherheit vom 14. März 2025; Schreiben der PUK Datensicherheit vom 26. März 2025 «Mitteilung an die durch die Untersuchung der PUK Datensicherheit betroffenen Personen – Aktueller Beschluss bzgl. Verweigerung der Akteneinsicht und Rechte der betroffenen Personen».

[47] § 120 Abs. 4 KRG.

den, wenn deren wesentlicher Inhalt den betroffenen Personen eröffnet und ihnen Gelegenheit geboten wurde, sich dazu zu äussern und Gegenbeweismittel zu bezeichnen.[48]

Nach Abschluss der Ermittlungen und vor der Berichterstattung an den Kantonsrat ist denjenigen Personen, die Gegenstand des Verfahrens einer PUK bilden, Gelegenheit zu geben, sich zu den Teilen des Berichtsentwurfs, die sie betreffen, zu äussern.[49]

2.3.7 Anordnungen und Entscheide der PUK Datensicherheit

Gegen Anordnungen des Kantonsrates und seiner Organe ist die Beschwerde an das Verwaltungsgericht unzulässig.[50] Das Verwaltungsgericht des Kantons Zürich hat in seinem Urteil VB.2015.00649 vom 2. Dezember 2015 bestätigt, dass Zwischenentscheide einer PUK nicht mit einem Rechtsmittel angefochten werden können, weil gegen den Schlussbericht der PUK ebenfalls kein Rechtsmittel zulässig ist.[51] Auch gemäss Regierungsrat gilt der Ausschluss der Verwaltungsgerichtsbeschwerde ebenfalls für Untersuchungshandlungen einer PUK.[52] Zur Begründung führte der Regierungsrat aus: «Obwohl es bei diesen Akten im Wesentlichen um Einzelpersonen geht, sollte im Fall einer Rechtsstreitigkeit der Weiterzug an ein Gericht gleichwohl grundsätzlich ausgeschlossen sein. Denn die Allgemeinheit hat daran in der Regel ein grosses Interesse und der Kantonsrat entscheidet in breiter Abwägung der Interessen. Gerade deswegen hat der Gesetzgeber diese Akte dem Kantonsrat zugewiesen. Dadurch zeichnen sie sich als solche mit vorwiegend politischem Charakter aus. Dem Verwaltungsgericht soll nicht zugemutet werden, darüber entscheiden zu müssen.»[53]

2.4 Vorgehen

2.4.1 Sitzungsrhythmus

Im Herbst 2023 hat die PUK Datensicherheit in den ersten sechs Sitzungen die Grundlagen für ihre Arbeit gelegt. In der Informationsbeschaffungsphase von Mitte Januar 2024 bis Ende März 2024 führte die PUK Datensicherheit insgesamt acht Sitzungen durch. Im April und Mai 2024 befasste sich die PUK Datensicherheit in vier Sitzungen mit Aktenbeizügen, koordinierte ihr Vorgehen mit der Staatsanwaltschaft III des Kantons Zürich[54] und bereitete die folgende Befragungsphase vor. In der Sachverhaltsermittlungs- und Beweiserhebungsphase, welche sich über den Zeitraum von Anfang Juni 2024 bis Ende Januar 2025 erstreckte, waren es insgesamt 17 Sitzungen. In der Auswertungsphase, die von Anfang Februar 2025 bis April 2025 dauerte, wurden zwei Sitzungen sowie ein ganztägiger Workshop durchgeführt. In weiteren acht Sitzungen erarbeitete und behandelte die PUK Datensicherheit ihre Teilberichte und schliesslich den gesamten Entwurf des provisorischen Berichts. Bis zur Verabschiedung des provisorischen Berichtsentwurfs wurden somit insgesamt 36 Halbtagessitzungen und 10 Ganztagessitzungen durchgeführt. Für die Beratung und Bereinigung des Schlussberichts bis zu dessen Verabschiedung zuhanden des Kantonsrates benötigte die PUK Datensicherheit drei weitere Sitzungen. Zur Vorbereitung der Pressekonferenz vom 12. Dezember 2025 fand vorgängig eine weitere Sitzung statt.

---

48 § 122 Abs. 1 KRG.

49 § 122 Abs. 2 KRG.

50 § 42 lit. b VRG.

51 Verwaltungsgericht des Kantons Zürich, Urteil vom 2. Dezember 2015 (VB.2015.00649).

52 Vorlage 4600, Gesetz über die Anpassung des kantonalen Verwaltungsverfahrensrechts, S. 98–99.

53 Vorlage 4600, Gesetz über die Anpassung des kantonalen Verwaltungsverfahrensrechts, S. 98.

54 Für eine bessere Lesbarkeit werden im folgenden Bericht die kürzeren Begriffe «Staatsanwaltschaft III» und «Staatsanwaltschaft Zürich-Sihl» verwendet.

Das Sekretariat der PUK Datensicherheit traf sich während der gesamten Dauer des Verfahrens ein- bis zweimal wöchentlich mit dem Präsidenten, um die Sitzungen vorzubereiten und die laufenden Geschäfte zu behandeln.

2.4.2 Koordination mit dem Strafverfahren

Am 27. Oktober 2023 orientierte der Leitende Oberstaatsanwalt, Andreas Eckert, die PUK Datensicherheit über den aktuellen Stand der Strafverfahren, die seit November 2020 von der Staatsanwaltschaft Zürich-Sihl und seit Dezember 2022 zusätzlich von der Staatsanwaltschaft III geführt wurden. Dabei wurde vereinbart, dass die PUK Datensicherheit nach Absprache mit der Verfahrensleitung für spezifische Fragestellungen Einsicht in die Akten nehmen und diese beiziehen könne.[55]

In der Folge entschloss sich die PUK Datensicherheit dazu, eine Koordination mit dem Strafverfahren der Staatsanwaltschaft III anzustreben, da dieses Verfahren den Teilaspekt der Datenentsorgung einer vertieften strafrechtlichen Prüfung unterzog. Zudem ermittelte die Staatsanwaltschaft Zürich-Sihl wegen verschiedener Delikte gegen Roland Gisler, unter anderem Gewalt und Drohung gegen Beamte sowie unrechtmässige Beschaffung von Personendaten.[56] Von einer Koordination mit der Staatsanwaltschaft Zürich-Sihl wurde abgesehen, da deren Untersuchungsgegenstand sich nicht mit dem Auftrag der PUK Datensicherheit deckt und die Staatsanwaltschaft III ihrerseits Akten der Staatsanwaltschaft Zürich-Sihl beigezogen hat.

Im Rahmen der Koordination hat sich die PUK Datensicherheit mit folgenden Personen ausgetauscht (Tabelle 2):

Tabelle 2 Koordination mit dem Strafverfahren

Eberli	Mathias	Staatsanwalt / Abteilungsleiter [Verfahrensleitung]	Staatsanwaltschaft III
Eckert	Andreas	ehem. Leitender Oberstaatsanwalt	Oberstaatsanwaltschaft
Zogg	David	ehem. Leitender Staatsanwalt	Staatsanwaltschaft III

Zur Koordination mit dem Strafverfahren der Staatsanwaltschaft III erfolgte am 3. Mai 2024 die Befragung des Leitenden Staatsanwalts, David Zogg, sowie des fallführenden Staatsanwalts der Staatsanwaltschaft III, Mathias Eberli.[57] Im Nachgang zu diesem Gespräch zog die PUK Datensicherheit die folgenden Akten aus dem Verfahren der Staatsanwaltschaft III bei (Tabelle 3):

Tabelle 3 Aktenbeizüge von der Staatsanwaltschaft III

Polizeiliche Ermittlungs- und Visionierungsberichte	Aktenbeizug vom 23. Mai 2024 Aktenbeizug vom 18. Juni 2024 Aktenbeizug vom 24. Januar 2025
Einvernahmeprotokolle mit Beilagen	Aktenbeizug vom 4. Juni 2024
Polizeiliche Schlussberichte der Verfahren (Staatsanwaltschaft Zürich-Sihl / Staatsanwaltschaft III)	Aktenbeizug vom 4. Juni 2024 Aktenbeizug vom 18. Januar 2025

[55] Protokoll der Sitzung der PUK Datensicherheit vom 27. Oktober 2023, S. 6–14.

[56] Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 1–2.

[57] Protokoll der Sitzung der PUK Datensicherheit vom 3. Mai 2024, S. 5; Protokoll der Befragung von David Zogg und Mathias Eberli vom 3. Mai 2024.

Mit Schreiben vom 20. September 2024 beantragte die PUK Datensicherheit zudem Einsicht in die Akten eines anderen, bereits rechtskräftig abgeschlossenen Verfahrens der Staatsanwaltschaft III.[58] Am 15. Oktober 2024 gewährte die Oberstaatsanwaltschaft die Einsicht in den Strafbefehl und die Einstellungsverfügung.[59]

Am 31. Januar 2025 fand eine weitere Befragung des fallführenden Staatsanwalts der Staatsanwaltschaft III, Mathias Eberli, statt.[60] Dabei konnte die PUK Datensicherheit Einsicht in die im Rahmen der Kantonsratssitzung vom 19. Dezember 2022 sichergestellten physischen Akten nehmen. Im Nachgang zu diesem Austausch zog die PUK Datensicherheit am 11. Februar 2025 von der Staatsanwaltschaft III weitere spezifische Unterlagen zu diesem Sachverhalt bei.

Der Beizug der oben aufgelisteten Akten erfolgte im Austausch mit der Verfahrensleitung vom Mai 2024 bis Januar 2025; insgesamt wurden über 450 Aktenstücke in elektronischer Form mittels gesicherten Datentransfers beigezogen.

Die PUK Datensicherheit informierte den verfahrensleitenden Staatsanwalt, Mathias Eberli, sowohl vor der Informationsbeschaffungsphase als auch vor und während der Sachverhaltsermittlungs- und Beweiserhebungsphase zwecks Koordination über das weitere Vorgehen. Als Abschluss der Sachverhaltsermittlung befragte die PUK Datensicherheit am 28. Februar 2025 den ehemaligen Leitenden Oberstaatsanwalt, Andreas Eckert.[61]

Im September 2025 teilte die Verfahrensleitung der Staatsanwaltschaft III der PUK Datensicherheit mit, dass das von ihr geführte Strafverfahren abgeschlossen wurde. Die PUK Datensicherheit konnte hierzu auch die Einstellungsverfügung einsehen.[62]

2.4.3 Beizug der JI-Akten

Mit Schreiben vom 2. November 2023 informierte die PUK Datensicherheit die Direktionsvorsteherin der JI, Jacqueline Fehr, über den Beginn ihrer Arbeiten und bat um die Zustellung des Schlussberichts der Administrativuntersuchung.[63] Am 15. November 2023 tauschten sich das Präsidium und das Sekretariat der PUK Datensicherheit mit der Generalsekretärin der JI, Jacqueline Romer, über die Form und Organisation des Aktenaustausches zwischen der JI und der PUK Datensicherheit aus. Es ging insbesondere um Unterlagen, welche die JI seit Sommer 2023 im Hinblick auf die Tätigkeit der PUK Datensicherheit intern zusammengetragen hatte.[64] Im Rahmen des Gesprächs übergab die Generalsekretärin dem Präsidium und dem Sekretariat der PUK Datensicherheit das von der Konferenz der Generalsekretärinnen und Generalsekretäre erarbeitete Merkblatt für das Personal der Verwaltung.[65] Im Nachgang beantragte die PUK Datensicherheit, wie im Gespräch vereinbart, mit Schreiben vom 21. Novem-

---

58 Schreiben der PUK Datensicherheit an die Staatsanwaltschaft III vom 20. September 2024 betreffend Antrag auf Einsicht in die Akten bzw. den Verfahrensabschluss.

59 Schreiben der Oberstaatsanwaltschaft an die PUK Datensicherheit vom 15. Oktober 2024 betreffend Ersuchen um Akteneinsicht.

60 Protokoll der Sitzung der PUK Datensicherheit vom 31. Januar 2025, S. 7–9; Protokoll der Befragung von Mathias Eberli vom 31. Januar 2024.

61 Protokoll der Sitzung der PUK Datensicherheit vom 28. Februar 2025, S. 6–8; Protokoll der Befragung von Andreas Eckert vom 28. Februar 2024.

62 Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025.

63 Schreiben der PUK Datensicherheit an Regierungsrätin Jacqueline Fehr vom 2. November 2023 betreffend Aktenzustellung.

64 Aktennotiz des Sekretariats der PUK Datensicherheit zum Austausch mit der Generalsekretärin der JI vom 15. November 2023.

65 Kanton Zürich, Merkblatt «Parlamentarische Untersuchungskommission (PUK) im Kanton Zürich» für Angestellte des Kantons Zürich vom 9. November 2023.

ber 2023 den Zugriff auf die JI-Akten und bat erneut um die Zustellung des ungeschwärzten Schlussberichts der Administrativuntersuchung.[66] Der Schlussbericht traf am 30. November 2023 mit Beilagen ein.[67] Am 22. Januar 2024 erhielt die PUK Datensicherheit zudem den Bericht und Aktionsplan «Datenschutz und Informationssicherheit in der Direktion der Justiz und des Innern» vom 19. Dezember 2023 zugestellt.[68] Die GPK, deren Präsidium den erwähnten Bericht und Aktionsplan zusammen mit dem Finanzkommissionspräsidium bereits am 11. Januar 2024 erhalten hatte, hatte die Übermittlung an die PUK Datensicherheit angeregt.[69]

Nachdem das Generalsekretariat und die Informatik der JI (Digital Solutions) die organisatorischen und technischen Voraussetzungen für einen Fernzugriff auf das Geschäft im Geschäftsverwaltungssystem der JI im Dezember 2023 geschaffen hatten, war der Zugriff für das Sekretariat der PUK Datensicherheit am 7. Februar 2024 implementiert.[70] In der Folge hat das Sekretariat der PUK Datensicherheit die Akten der JI in die Ablage der PUK Datensicherheit überführt. Im Rahmen des Aktenbeizugs nahm die PUK Datensicherheit insgesamt 224 Dokumente zu ihren Akten. Im März 2025 nahm die PUK Datensicherheit drei weitere Dokumente zu den Akten, welche in der Zwischenzeit in der Ablage der JI abgelegt worden waren.

2.4.4 Konzeptphase

Die Untersuchungsgegenstände aus dem Untersuchungsauftrag der GPK vom 27. April 2023 bezogen sich einerseits auf die vergangenen Ereignisse, andererseits aber auch auf den aktuellen Stand der Informationssicherheit des Kantons. Weiter waren die JI, aber auch der Regierungsrat, die Direktionen und die Staatskanzlei sowie weitere kantonale Stellen adressiert.

Die PUK Datensicherheit konkretisierte ihr Vorgehen und entschied, die Untersuchung zeitlich und thematisch wie folgend dargestellt zu gliedern (Abbildung 2):

Abbildung 2 Übersicht basierend auf dem Untersuchungskonzept

	Zeitraum 1	**Zeitraum 2**		**Zeitraum 3**		**Zeitraum 4**	
	Datensicherheits-vorfall			nach dem internen Bekanntwerden		nach dem öffentlichen Bekanntwerden	
Zeitraum	2010–2014	2015–2019		2020–2022		2022–heute	
Inhalt	Datensicherheits-vorfall	Praxis in der JI	Aufräum-aktion 2019	Verhalten der JI	Administrativunter-suchung (AU)	Reaktion auf den Vorfall	Aufarbei-tung des Vorfalls

In Bezug auf die *Vergangenheit (Zeitraum 1 und 2)* war die PUK Datensicherheit daran interessiert, die konkreten Umstände des Datensicherheitsvorfalls in der JI (Zeitraum, Ausmass, Verantwortlichkeiten) zu klären und festzustellen, wie die Entsorgung von Datenträgern im fraglichen Zeitraum geregelt war, sowie zu untersuchen,

---

66 Schreiben der PUK Datensicherheit «Antrag auf Zugriff zu den JI-intern bereitgestellten Akten im CMI» an die Generalsekretärin der JI vom 21. November 2023.

67 Gesicherte E-Mail der Generalsekretärin der JI an das Sekretariat der PUK Datensicherheit vom 30. November 2023.

68 E-Mail der JI «Bericht Datenschutz und Informationssicherheit» an die Präsidien der GPK, Subkommission IKT und die PUK Datensicherheit vom 22. Januar 2024.

69 Protokoll der Sitzung der Geschäftsprüfungskommission vom 18. Januar 2024 und Schreiben der GPK an Regierungsrätin Jacqueline Fehr vom 19. Januar 2024.

70 Bis zu diesem Termin konnten die technischen Schwierigkeiten dank dem Einsatz des ICT-Architekten der DigiSol ausgeräumt werden.

ob der Regierungsrat im Rahmen seiner Verantwortlichkeiten und Zuständigkeiten auf der kantonalen Ebene rechtzeitig und vorausschauend Regulative zur Informationssicherheit und zur Entsorgung von Datenträgern beschlossen hatte und ob er sich der diesbezüglichen Problematik ausreichend bewusst war.

Rückblickend war zudem zu eruieren, ob bereits in den *Jahren 2015–2019 (Zeitraum 2)* in der JI, aber auch allgemein im Kanton Vorkehrungen zur Verhinderung von Datenmissbrauch getroffen worden waren. Ausserdem waren die ebenfalls in der Vergangenheit liegenden Umstände rund um die mutmassliche Aktenvernichtung innerhalb der JI im Jahr 2019, welche die Administrativuntersuchung zutage gebracht hatte, zu klären.

In Bezug auf den *Zeitraum nach dem internen Bekanntwerden (Zeitraum 3)* war zu untersuchen, wann die direkt betroffene Direktion und der Regierungsrat vom Vorfall erfahren hatten und ob der Regierungsrat bereits zu diesem Zeitpunkt angemessen über den Datensicherheitsvorfall informiert worden war. Weiter war für den Zeitraum 3 auch zu prüfen, ob die direkt betroffene Direktion zweckmässig, zeitnah und angemessen auf den Datensicherheitsvorfall reagiert hatte. Hier waren namentlich die Einleitung der Administrativuntersuchung sowie die Kommunikation gegenüber der Regierung und den weiteren kantonalen Stellen in den Blick zu nehmen.

Für den *Zeitraum nach dem öffentlichen Bekanntwerden (Zeitraum 4)* war zu prüfen, ob neben der direkt betroffenen Direktion auch der Regierungsrat und weitere kantonale Stellen zeitnah die nötigen Schritte unternommen hatten, um den Datensicherheitsvorfall aufzuarbeiten und künftig ähnliche Vorfälle zu verhindern. Dabei waren neben den Massnahmen des Kantons und aller Direktionen und der Staatskanzlei gemäss dem Beschluss der PUK Datensicherheit vom 23. November 2023 auch die Massnahmen der konsolidierten selbständigen öffentlich-rechtlichen Anstalten zu berücksichtigen.

Auch die im Rahmen der Kantonsratsdebatte vom 9. Januar 2023 aufgebrachte Frage, ob der Regierungsrat angemessen geprüft habe, ob für die strafrechtlichen Untersuchungen eine ausserkantonale Strafverfolgungsbehörde einzusetzen sei, galt es zu klären. Abschliessend sollte untersucht werden, ob die Informationssicherheit in der kantonalen Verwaltung aktuell gewährleistet und die Datenvernichtung ausreichend reglementiert und dokumentiert ist.

Der folgende Bericht gliedert sich folglich entlang dieser verschiedenen Zeiträume und Fragestellungen (Tabelle 4):

Tabelle 4 Gliederung des Schlussberichts

Kapitel des Berichts	Fragestellungen gemäss KR-Nr. 172/2023	Ebene
5. Kantonale Entwicklung 1995–2005: Herausforderung Informationssicherheit in Zeiten des technologischen Wandels	– War sich der Regierungsrat der Problematik der Datensicherheit und Entsorgung von Datenträgern bewusst und hatte er rechtzeitig und vorausschauend im Rahmen seiner Verantwortlichkeiten und Zuständigkeiten die nötigen Regulative beschlossen?	Kanton
6. Kantonale Entwicklung 2006–2014: Das KITT-Umfeld und die gescheiterte Umsetzung der Informatikstrategie 2008		
7. Informationssicherheit in der JI mit Fokus auf die Beschaffungs- und Entsorgungsprozesse von 2000–2014	– Über welchen Zeitraum hat sich der Datensicherheitsvorfall ereignet und wer hat ihn zu verantworten?	JI
8. Ausmass und Hintergründe des Datensicherheitsvorfalls		

Kapitel des Berichts	Fragestellungen gemäss KR-Nr. 172/2023	Ebene
9. 2000–2014: Entsorgungspraxis in den Direktionen und der Staatskanzlei	– Wie war die Entsorgung von Datenträgern im fraglichen Zeitraum in den Direktionen geregelt, besonders in Bereichen mit sensitiven Daten? – Wurden die notwendigen Vorkehrungen getroffen, damit ein ähnlicher Datenmissbrauch künftig verhindert werden kann?	Dir/SK
10. Kantonale Entwicklung 2015–2019: Schritte auf dem Weg zum heutigen System der Informationssicherheit	– War sich der Regierungsrat der Problematik der Datensicherheit und Entsorgung von Datenträgern bewusst und hatte er rechtzeitig und vorausschauend im Rahmen seiner Verantwortlichkeiten und Zuständigkeiten die nötigen Regulative beschlossen?	Kanton
11. Entwicklungen in der Direktion der Justiz und des Innern (JI) 2015–2020	– Haben die direkt betroffene Direktion und zuständige kantonale Stellen und Behörden zeitnah die nötigen Schritte unternommen, um den Datensicherheitsvorfall aufzuarbeiten und sicherzustellen, dass ähnliche Vorfälle verhindert werden können? – Wurden die notwendigen Vorkehrungen getroffen, damit ein ähnlicher Datenmissbrauch künftig verhindert werden kann?	JI
12./13. Umgang mit dem Datensicherheitsvorfall nach dem internen respektive öffentlichen Bekanntwerden	– Haben der Regierungsrat und die direkt betroffenen Direktionen angemessen über den Datensicherheitsvorfall informiert? – Wann haben der Regierungsrat und die direkt betroffenen Direktionen vom Datensicherheitsvorfall Kenntnis erhalten? – Haben der Regierungsrat und die direkt betroffene Direktion zweckmässig, zeitnah und rechtmässig auf den Datensicherheitsvorfall reagiert? – Haben der Regierungsrat und die direkt betroffene Direktion zeitnah die nötigen Schritte unternommen, um den Datensicherheitsvorfall aufzuarbeiten und sicherzustellen, dass ähnliche Vorfälle verhindert werden können? – Hat der Regierungsrat angemessen geprüft, für das Strafverfahren eine ausserkantonale Strafverfolgungsbehörde zu beauftragen?	Kanton/JI
14. Heutiges kantonales System der Informationssicherheit	– Ist die Datensicherheit in der kantonalen Verwaltung gewährleistet und ist die Datenvernichtung ausreichend reglementiert und dokumentiert?	Kanton
15. Stand der Informationssicherheit in den Direktionen und der Staatskanzlei	– Ist die Datensicherheit in der kantonalen Verwaltung gewährleistet und ist die Datenvernichtung ausreichend reglementiert und dokumentiert? – Haben weitere zuständige kantonale Stellen und Behörden zeitnah die nötigen Schritte unternommen, um den Datensicherheitsvorfall aufzuarbeiten und sicherzustellen, dass ähnliche Vorfälle verhindert werden können?	Dir/SK
16. Stand der Informationssicherheit in den selbständigen öffentlich-rechtlichen Anstalten		Selbständige öffentlich-rechtliche Anstalten
17. State of the Art und diesbezügliche Entwicklungen		

2.4.5 Informationsbeschaffungsphase

Befragungen und Einvernahmen

Ziel der Informationsbeschaffungsphase war es, zur Umsetzung des Gesetzes über die Information und den Datenschutz (IDG) allgemein, zur Informationssicherheit, zur fachgerechten Entsorgung und Löschung von Datenträgern und Daten sowie zum Archivwesen Wissen aufzubauen. Dazu fanden zwischen Ende Januar 2024 und Ende März 2024 erste Einvernahmen und Befragungen von folgenden Personen statt (Tabelle 5):[71]

Tabelle 5 Befragungen im Rahmen der Informationsbeschaffungsphase

Umsetzung des Gesetzes über die Information und den Datenschutz (IDG)			
Blonski	Dominika	Kantonale Datenschutzbeauftragte	als Auskunftsperson
Gussmann	Marianne	Fachbereich Rechtsmittel, Generalsekretariat, Gesundheitsdirektion	als Auskunftsperson
Hösli	Peter	Chef Rechtsdienst / Stv. Staatsschreiber, Staatskanzlei[72]	als Auskunftsperson
Stauffacher	Werner	Fach- und Rechtsdienst, Generalsekretariat, Bildungsdirektion	als Auskunftsperson
Informationssicherheit			
Bolinger	Roman	Informationssicherheitsbeauftragter, Volkswirtschaftsdirektion (ISID BD, ad interim)	als Auskunftsperson
Grabher	Philipp	Kantonaler Informationssicherheitsbeauftragter (ISIK)	als Auskunftsperson
Poell	Jörg	Informationssicherheitsbeauftragter, Finanzdirektion (ISID FD)	als Auskunftsperson
Fachgerechte Entsorgungsprozesse			
Bänziger	David	Leiter IT-Operations, Systems Integration und Digitaler Arbeitsplatz, Zürcher Kantonalbank	als Zeuge
Nenadovic	Predrag	Geschäftsführer CBA Computer Broker AG	als Zeuge
Wydler	Michael	Leiter IT-Asset Management, Zürcher Kantonalbank	als Zeuge
Archivwesen			
Gnädinger	Beat	Staatsarchivar	als Auskunftsperson

Die Fragen, die den Auskunftspersonen resp. den Zeuginnen und Zeugen gestellt werden sollten, wurden jeweils durch das PUK-Sekretariat und den PUK-Präsidenten vorbereitet, den PUK-Mitgliedern im Geschäftsverwaltungssystem elektronisch zugänglich gemacht und vor der Befragung oder Einvernahme im Rahmen einer Kommissionssitzung besprochen. Die Befragungen und Einvernahmen wurden durch den PUK-Präsidenten geführt, während dessen Abwesenheit durch den Vizepräsidenten. Zu Beginn wurden die Auskunftspersonen, Zeuginnen und Zeugen auf ihre Rechte und Pflichten hingewiesen. Die PUK-Mitglieder sowie der PUK-Sekretär und die Rechtskonsulentin der PUK erhielten jeweils nach Abschluss eines Themenkomplexes Gelegenheit, Ergänzungsfragen zu stellen. An den einzelnen Einvernahmen nahmen keine betroffenen Personen teil.

---

[71] Die PUK Datensicherheit legte den Befragungsplan der Informationsbeschaffungsphase am 12. Januar 2024 definitiv fest und setzte die betroffenen Personen am 16. Januar 2024 darüber in Kenntnis.

[72] In Vertretung der Leitung der Koordinationsstelle IDG.

Die in der Informationsbeschaffungsphase gewonnenen Einsichten dienten als Basis für die weiteren Untersuchungen. In Kapitel 17 werden die unterschiedlichen Formen der Datenträgervernichtung und Datenlöschung beschrieben und aufgezeigt, wie sich diese Praxis über die Zeit entwickelt hat.

Aktenbeizug im Rahmen der Informationsbeschaffungsphase

Im Rahmen der Befragungen und Einvernahmen der Informationsbeschaffungsphase hat die PUK Datensicherheit verschiedene Akten erhalten oder diese nachträglich bei den befragten Personen eingefordert. In diesem Zusammenhang hat die PUK Datensicherheit u. a. vom kantonalen Informationssicherheitsbeauftragten (ISIK)[73] sowie vom Informationssicherheitsbeauftragten der Finanzdirektion (ISID FD)[74] Unterlagen zur Informationssicherheit und vom befragten Geschäftsführer der CBA Computer Broker AG Dokumente zur Praxis der Datenlöschung[75] erhalten.

Bezeichnung der Betroffenen

Um eine grösstmögliche Transparenz zu gewährleisten und den Betroffenen möglichst frühzeitig ihre Rechte einzuräumen, hat die PUK Datensicherheit am 12. Januar 2024, basierend auf dem damaligen Wissensstand, in der Informationsbeschaffungsphase folgende Personen als durch die Untersuchung in ihren Interessen unmittelbar betroffen bezeichnet (Tabelle 6):[76]

Tabelle 6 Betroffene Personen gemäss Beschluss vom 12. Januar 2024

Arioli	Kathrin	Staatsschreiberin
Baeriswyl	Bruno	ehem. kantonaler Datenschutzbeauftragter
Blonski	Dominika	Kantonale Datenschutzbeauftragte
Fehr	Jacqueline	Regierungsrätin
Fehr	Mario	Regierungsrat
Grabher	Philipp	Kantonaler Informationssicherheitsbeauftragter (ISIK)
Neukom	Martin	Regierungsrat
Rickli	Natalie	Regierungsrätin
Steiner	Silvia	Regierungsrätin
Stocker	Ernst	Regierungsrat
Walker Späh	Carmen	Regierungsrätin

Die betroffenen Personen wurden über den Beschluss informiert und auf ihre Rechte im Verfahren der PUK Datensicherheit hingewiesen. Gleichzeitig wurde ihnen eine Liste der geplanten Befragungen und Einvernahmen mit Datum und Sitzungsort zugestellt. Bei Änderungen wurden die betroffenen Personen informiert.

---

[73] Die PUK Datensicherheit erhielt physische Unterlagen im Rahmen der Befragung vom 8. März 2024 und ergänzend am 14. und 15. März 2024 Unterlagen in elektronischer Form. Weitere Informationen zur neuen AISR, zur Lieferantensicherheit, zum Vertragswesen sowie zu den kantonalen Informationssicherheitsstandards konnten am 9. und 12. Mai 2025 beigezogen werden.

[74] Aktenbeizug vom 18. März 2024.

[75] Aktenbeizug vom 17. April 2024.

[76] Protokoll der Sitzung der PUK Datensicherheit vom 12. Januar 2024.

2.4.6 Sachverhaltsermittlungs- und Beweiserhebungsphase

Befragungen und Einvernahmen

Nach dem Wissensaufbau machte sich die PUK Datensicherheit daran, die früheren Bemühungen zur Entwicklung der Informationssicherheit auf kantonaler Ebene sowie den Datensicherheitsvorfall im engeren Sinne und die diesbezüglichen politischen Verantwortlichkeiten zu untersuchen (siehe hierzu auch die Abbildung in Kapitel 2.4.4). Schliesslich befasste sie sich mit den Umständen des internen Bekanntwerdens, den Massnahmen der JI sowie der Räumungsaktion 2019, bevor sie abschliessend die politischen Verantwortlichkeiten der Direktionsvorsteherin der JI, Jacqueline Fehr, sowie der weiteren Regierungsmitglieder behandelte. Die PUK Datensicherheit beschloss, in der Sachverhaltsermittlungs- und Beweiserhebungsphase folgende Personen als Auskunftspersonen zu befragen oder als Zeuginnen und Zeugen einzuvernehmen (Tabelle 7):[77]

Tabelle 7 Befragungen im Rahmen der Sachverhaltsermittlungsphase

Arioli	Kathrin	Staatsschreiberin, Leiterin der Staatskanzlei	als Auskunftsperson
Baeriswyl	Bruno	ehem. kantonaler Datenschutzbeauftragter	als Auskunftsperson
Billeter	Martin	Leiter der Finanzkontrolle	als Auskunftsperson
Bischof	Sarah	Autorin des Schlussberichts der Administrativuntersuchung	als Zeugin
Blonski	Dominika	Kantonale Datenschutzbeauftragte	als Auskunftsperson
Eckert	Andreas	ehem. Leitender Oberstaatsanwalt	als Auskunftsperson
Fehr	Jacqueline	Regierungsrätin, Vorsteherin der Direktion der Justiz und des Innern	als Auskunftsperson
Fehr	Mario	Regierungsrat, Vorsteher der Sicherheitsdirektion	als Auskunftsperson
Graf	Martin	alt Regierungsrat, ehem. Vorsteher der Direktion der Justiz und des Innern (2011–2015)	als Auskunftsperson
Gut-Winterberger	Ursula	alt Regierungsrätin, ehem. Vorsteherin der Finanzdirektion (2007–2015)	als Auskunftsperson
Habegger	Beat	Kantonsrat, ehem. GPK-Präsident	als Auskunftsperson
Husi	Beat	ehem. Staatsschreiber (1995–2018)	als Auskunftsperson
Kaderli	Urs	Leiter der Hauptabteilung Digital Solutions, Direktion der Justiz und des Innern	als Auskunftsperson
Mayer	Axel	ehem. Leiter Hauptabteilung Informatik, Direktion der Justiz und des Innern	als Auskunftsperson
Mühlebach	Renzo	ehem. kantonaler Informatik-Sicherheitsbeauftragter (I-SiBe)	als Auskunftsperson
Neukom	Martin	Regierungsrat, Vorsteher der Baudirektion	als Auskunftsperson
Notter	Markus	alt Regierungsrat, ehem. Vorsteher der Direktion der Justiz und des Innern (1996–2011)	als Auskunftsperson
Rickli	Natalie	Regierungsrätin, Vorsteherin der Gesundheitsdirektion	als Auskunftsperson
Romer	Jacqueline	Generalsekretärin, Direktion der Justiz und des Innern	als Auskunftsperson

[77] Den ersten Befragungsplan (Juni bis Juli 2024) legte die PUK Datensicherheit am 24. Mai 2024 definitiv fest und setzte die betroffenen Personen am 5. Juni 2024 darüber in Kenntnis. Den zweiten Befragungsplan (August bis Dezember 2024) legte die PUK Datensicherheit am 23. August 2024 definitiv fest und setzte die betroffenen Personen am 28. August 2024 darüber in Kenntnis. Schliesslich informierte sie mit Schreiben vom 13. März 2025 über die Befragung des ehemaligen Leitenden Oberstaatsanwalts vom 28. Februar 2025.

Stähelin	Susanna	Stv. Generalsekretärin, Direktion der Justiz und des Innern	als Auskunftsperson
Steiner	Fredi [Alfred]	Leiter Operation Management und ehem. Leiter Abteilung Informatik, Direktion der Justiz und des Innern	als Auskunftsperson
Steiner	Silvia	Regierungsrätin, Vorsteherin der Bildungsdirektion	als Auskunftsperson
Stocker	Ernst	Regierungsrat, Vorsteher der Finanzdirektion	als Auskunftsperson
Strebel	Daniel	Stv. Leiter, Finanzkontrolle	als Auskunftsperson
Tommer	Benjamin	Kommunikationsbeauftragter, Direktion der Justiz und des Innern	als Auskunftsperson
Walker Späh	Carmen	Regierungsrätin, Vorsteherin der Volkswirtschaftsdirektion	als Auskunftsperson
Widmer	Renato	ehem. Hauptabteilungsleiter Logistik, Finanzen und Controlling, Direktion der Justiz und des Innern	als Auskunftsperson
Winkler	Maria	Autorin des Schlussberichts der Administrativuntersuchung	als Zeugin
Zünd	Christian	ehem. Generalsekretär, Direktion der Justiz und des Innern	als Auskunftsperson

Für die Sachverhaltsermittlungs- und die Beweiserhebungphase wurden die Befragungen der Auskunftspersonen sowie die Einvernahmen der Zeuginnen und Zeugen zwischen Anfang Juni 2024 und Ende Januar 2025 durchgeführt. Des Weiteren wurde in Bezug auf das Vorgehen gleich verfahren wie in der Informationsbeschaffungsphase.

Aktenbeizug im Rahmen der Sachverhaltsermittlungsphase

Im Rahmen von Befragungen und Einvernahmen der Sachverhaltsermittlungsphase hat die PUK Datensicherheit Akten erhalten oder diese nachträglich bei den befragten Personen eingefordert. Zusätzlich wurden im Nachgang der Befragungen und Einvernahmen, auch unaufgefordert, Ergänzungen oder Dokumente eingereicht. Darüber hinaus liess die Finanzkontrolle der PUK Datensicherheit auf Nachfrage Unterlagen von früheren Prüfungen zukommen.[78] Auch vom Generalsekretariat der JI oder von der Staatskanzlei forderte die PUK Datensicherheit ergänzende Unterlagen ein.[79]

Bezeichnung der Betroffenen

Während der Sachverhaltsermittlungs- und Beweiserhebungsphase erlangte die PUK Datensicherheit zusätzliches Wissen und bezeichnete mit Beschluss vom 24. Mai 2024[80], 30. August 2024[81] und 28. Februar 2025[82] zusätzlich folgende Personen als durch die Untersuchung in ihren Interessen unmittelbar betroffen (Tabelle 8):

[78] Aktenbeizüge vom 5. Juli 2024 und vom 20. November 2024.

[79] Die PUK Datensicherheit forderte beim Generalsekretariat der JI Akten zu deren Geschäftsverwaltungssystem und bei der Staatskanzlei Unterlagen zu den Regierungsratssitzungen vom November 2020 sowie Dezember 2022 an.

[80] Protokoll der Sitzung der PUK Datensicherheit vom 24. Mai 2024.

[81] Protokoll der Sitzung der PUK Datensicherheit vom 30. August 2024.

[82] Protokoll der Sitzung der PUK Datensicherheit vom 28. Februar 2025.

Tabelle 8 Weitere als betroffen bezeichnete Personen

Graf	Martin	alt Regierungsrat, ehem. Vorsteher der Direktion der Justiz und des Innern (2011–2015)
Gut-Winterberger	Ursula	alt Regierungsrätin, ehem. Vorsteherin der Finanzdirektion (2007–2015)
Husi	Beat	ehem. Staatsschreiber (1995–2018)
Notter	Markus	alt Regierungsrat, ehem. Vorsteher der Direktion der Justiz und des Innern (1996–2011)
Steiner	Fredi [Alfred]	Leiter Operation Management und ehem. Leiter Abteilung Informatik, Direktion der Justiz und des Innern
Widmer	Renato	ehem. Hauptabteilungsleiter Logistik, Finanzen und Controlling, Direktion der Justiz und des Innern

Die bereits bezeichneten sowie die neu als betroffen bezeichneten Personen wurden über die jeweiligen Beschlüsse informiert. Zusätzlich wurden die neu bezeichneten betroffenen Personen auf ihre Rechte im Verfahren der PUK Datensicherheit hingewiesen. Gleichzeitig wurde allen betroffenen Personen eine Liste der im Rahmen der Sachverhaltsermittlungs- und Beweiserhebungsphase geplanten Befragungen und Einvernahmen mit Datum und Sitzungsort zugestellt. Bei Änderungen wurden die betroffenen Personen informiert.

Die PUK Datensicherheit machte im Übrigen von der Möglichkeit der Einschränkung der Verfahrensrechte der Betroffenen Gebrauch, indem sie den betroffenen Personen die Einsicht in die Strafverfahrensakten der Staatsanwaltschaft III sowie die Protokolle der Befragungen und Einvernahmen von Auskunftspersonen sowie Zeuginnen und Zeugen ab 30. August 2024 verweigerte.[83]

Einholung von Auskünften

Im Rahmen des Auftrags hatte die PUK Datensicherheit auch zu untersuchen, ob die Datensicherheit in der kantonalen Verwaltung gewährleistet und die Datenvernichtung ausreichend reglementiert und dokumentiert ist.[84] Die PUK Datensicherheit holte aus diesem Grund mittels Fragebogen Auskünfte von den Informationssicherheitsbeauftragten (ISID) der Direktionen ein. Der Fragebogen wurde den ISID am 22. Januar 2025 zugestellt. Bis zum 21. Februar 2025 retournierten alle ISID die ausgefüllten Fragebogen.

Zusätzlich hatte die PUK Datensicherheit zu untersuchen, ob die weiteren zuständigen kantonalen Stellen zeitnah die nötigen Schritte unternommen hatten, um den Datensicherheitsvorfall aufzuarbeiten und sicherzustellen, dass ähnliche Vorfälle verhindert werden konnten.[85] Die PUK Datensicherheit verwendete ebenfalls Fragebogen, um von den selbständigen öffentlich-rechtlichen Anstalten des Kantons Zürich Auskünfte zum Stand der Informationssicherheit und zu den diesbezüglichen Entwicklungen einzuholen. Den selbständigen öffentlich-rechtlichen Anstalten des Kantons Zürich wurde der Fragebogen am 23. Januar 2025 zugestellt. Bis März 2025 retournierten alle selbständigen öffentlich-rechtlichen Anstalten die ausgefüllten Fragebogen.

[83] Protokoll der Sitzung der PUK Datensicherheit vom 6. September 2024.

[84] Antrag der Geschäftsprüfungskommission vom 27. April 2023 (KR-Nr. 172/2023), S. 1.

[85] Antrag der Geschäftsprüfungskommission vom 27. April 2023 (KR-Nr. 172/2023), S. 1.

Schliesslich holte die PUK Datensicherheit am 21. Januar 2025 von der Staatskanzlei noch die Auskunft ein, wie viele Administrativuntersuchungen in den einzelnen Direktionen in den Jahren 2020–2024 durchgeführt worden waren.[86] Die Staatskanzlei übermittelte der PUK Datensicherheit hierzu am 23. März 2025 eine Übersicht.[87]

2.4.7 Akteneinsicht der Betroffenen

Nach Abschluss der Sachverhaltsermittlungs- und Beweiserhebungsphase beschloss die PUK Datensicherheit, sämtliche Untersuchungsakten, die keinen Bezug zum laufenden Strafverfahren aufweisen, per sofort zu öffnen und den betroffenen Personen Gelegenheit zur Einsichtnahme und zur schriftlichen Stellungnahme sowie zur schriftlichen Bezeichnung von Gegenbeweismitteln zu bieten.[88] Für die schriftliche Stellungnahme und die Bezeichnung von Gegenbeweismitteln wurde ihnen eine Frist bis am 12. Mai 2025 gesetzt. Innert Frist bezeichnete Regierungsrätin Jacqueline Fehr Gegenbeweismittel. Der kantonale Informationssicherheitsbeauftragte (ISIK), Philipp Grabher, reichte Akten zu gesamtkantonalen Aktivitäten im Bereich Informationssicherheit ein.

Soweit erforderlich, wurde bei der Diskussion des ersten Berichtsentwurfs auf die eingegangenen Stellungnahmen reagiert.

2.4.8 Erster Entwurf des Schlussberichts der PUK Datensicherheit

Anlässlich einer Rückschau auf die durchgeführten Befragungen beriet die PUK Datensicherheit im Januar 2025 ihre Feststellungen und Schlussfolgerungen aus der durchgeführten Untersuchung und befasste sich mit einer möglichen inhaltlichen Gliederung des Schlussberichts. Im Rahmen eines ganztägigen Workshops legte die PUK Datensicherheit Mitte März 2025 die Berichtsstruktur fest und beschloss, die zeitlich und thematisch gegliederten Inhalte jeweils als Teilberichte zu beraten. In enger Zusammenarbeit von Präsidium, Sekretariat und Rechtskonsulentin wurden in den folgenden Monaten die einzelnen Entwürfe zu den Teilberichten erarbeitet. In mehreren Sitzungen von Mai bis Juli 2025 wurden die Teilberichte als Entwürfe beraten und Änderungen und Ergänzungen beschlossen, die jeweils in die Überarbeitungen der Teilberichte einflossen. Im August 2025 nahm die Kommission in mehreren Sitzungen eine Gesamtsicht vor und befasste sich eingehend mit ihren Schlussfolgerungen und Empfehlungen. Im September 2025 beriet die PUK Datensicherheit den Entwurf des Schlussberichts integral und verabschiedete ihn vorläufig.[89]

2.4.9 Stellungnahmen der Betroffenen

Nach Abschluss der Ermittlungen und vor der Berichterstattung an den Kantonsrat ist den Personen, die Gegenstand des Verfahrens der PUK Datensicherheit bilden, Gelegenheit zu geben, sich zu den Teilen des Berichtsentwurfs zu äussern, die sie betreffen.[90] Der von der PUK Datensicherheit vorläufig genehmigte Bericht wurde in diesem Sinn den Betroffenen zur schriftlichen Stellungnahme zugestellt: Alle Mitglieder des Regierungsrates, die Staatsschreiberin und die kantonale Datenschutz- sowie der kantonale Informationssicherheitsbeauftragte erhielten den gesamten Bericht zur Stellungnahme. Folgende Personen erhielten nur den sie betreffenden Auszug

---

[86] Schreiben der PUK Datensicherheit vom 21. Januar 2025 an die Staatskanzlei.

[87] Schreiben der Staatsschreiberin vom 23. März 2025 mit einer Übersicht über die Anzahl angeordneter Administrativuntersuchungen als Beilage.

[88] Beschluss der PUK Datensicherheit vom 14. März 2025.

[89] Protokoll der Sitzung der PUK Datensicherheit vom 26. September 2025.

[90] § 122 Abs. 2 KRG.

zur Gewährung des rechtlichen Gehörs: Bruno Baeriswyl; Martin Graf; Ursula Gut-Winterberger; Beat Husi; Axel Mayer; Markus Notter; Jacqueline Romer; Fredi Steiner; Renato Widmer sowie Christian Zünd.[91]

Es gingen von folgenden Personen fristgerecht Stellungnahmen ein: Kathrin Arioli, Bruno Baeriswyl, Dominika Blonski, Jacqueline Fehr, Philipp Grabher, Martin Graf, Beat Husi, Axel Mayer, Jacqueline Romer, Fredi Steiner, Renato Widmer sowie Christian Zünd. Die Stellungnahme von Markus Notter ging nach Ablauf der gesetzten Frist ein. Ursula Gut-Winterberger und Natalie Rickli verzichteten ausdrücklich auf eine Stellungnahme.

Die PUK Datensicherheit hat die aus ihrer Sicht begründeten und objektivierbaren Kritikpunkte in ihrem weiteren Vorgehen berücksichtigt und in den Schlussbericht übernommen.

2.4.10 Schlussbericht der PUK Datensicherheit

Nach der Überarbeitung des Berichts aufgrund der eingegangenen Stellungnahmen führte die PUK Datensicherheit die Schlussabstimmung durch. Der Schlussbericht der PUK Datensicherheit wurde mit 11 zu 0 Stimmen zuhanden des Kantonsrates genehmigt.[92]

---

[91] Beschluss der PUK Datensicherheit vom 26. September 2025.

[92] Protokoll der Sitzung der PUK Datensicherheit vom 21. November 2025.

3. Kosten

3.1 Kostenschätzung

Die Geschäftsleitung des Kantonsrates beantragte auf der Basis einer Schätzung die Kosten, die für die Arbeit der PUK Datensicherheit anfallen, und ergänzte das Budget des Kantonsrates entsprechend. Für die PUK Datensicherheit wurde insgesamt mit einem Aufwand von 800000 bis 1100000 Franken gerechnet.[93]

Da die PUK Datensicherheit erst im dritten Quartal eingesetzt wurde, konnten die Kosten für das Jahr 2023 nicht mehr ins Budget aufgenommen werden und es musste eine Budgetüberschreitung in Kauf genommen werden.

Für das Jahr 2024 wurde ein Betrag von 400000 Franken zur Verfügung gestellt und im Budget für das Jahr 2025 wurden ebenfalls 400000 Franken bewilligt. Das Gesamtbudget der PUK Datensicherheit betrug demnach 800000 Franken.

3.2 Kosten bis 21. November 2025

Im Zeitpunkt der Schlussabstimmung vom 21. November 2025 über den Bericht der PUK Datensicherheit beliefen sich die Kosten auf rund 550000 Franken.

Voraussichtlich fallen noch Kosten von rund 20000 Franken bis zum Abschluss der PUK Datensicherheit an. Insgesamt belaufen sich die Kosten demnach auf rund 570000 Franken.

[93] Antrag der Geschäftsprüfungskommission vom 27. April 2023 (KR-Nr. 172/2023), S. 7.

4. Kantonsrätliche Geschäfte und Vorstösse zum Datensicherheitsvorfall im Kanton Zürich

Tabelle 9 Kantonsrätliche Geschäfte und Vorstösse zum Datensicherheitsvorfall

456/2022	**Vorgehen und Verantwortlichkeiten in der Justizdirektion bei der Entsorgung von Datenträgern** Anfrage von Valentin Landmann (SVP, Zürich), Nina Fehr Düsel (SVP, Küsnacht), Yiea Wey Te (FDP, Unterengstringen), 28. November 2022
462/2022	**Verantwortlichkeiten bei der Justizdirektion verlangen Aufklärung** Dringliche Interpellation von Martin Hübscher (SVP, Wiesendangen), Yiea Wey Te (FDP, Unterengstringen), Jean-Philippe Pinto (Die Mitte, Volketswil), Andrea Gisler (GLP, Gossau), 5. Dezember 2022
172/2023	**Einsetzung einer Parlamentarischen Untersuchungskommission, Datensicherheitsvorfall** Antrag der Geschäftsprüfungskommission (GPK), 27. April 2023
274/2023	**Wahl Parlamentarische Untersuchungskommission (PUK) Datensicherheit** Antrag der Interfraktionellen Konferenz (IFK), 29. August 2023
364/2023	**Wahl Mitglied Parlamentarische Untersuchungskommission (PUK) Datensicherheit für Yvonne Bürgin** Antrag der Interfraktionellen Konferenz (IFK), 14. November 2023

5. Kantonale Entwicklung 1990–2005: Herausforderung Informationssicherheit in Zeiten des technologischen Wandels

5.1 Kantonale Organisation der Informatik in den 1990er-Jahren

In den 1990er-Jahren bestanden im Kanton Zürich drei wesentliche IT-Organisationen:
- Arbeitsgruppe Planung und Steuerung der Informatik und Kommunikation (AGIK; ab 1999 durch die Kommission für strategische Informatikführung [KOSIF] abgelöst)
- Abteilung für Informatikplanung (AIP)
- Amt für Informatikdienste (AID, früher Informatikzentrum der Abteilung für Organisation und Informatik [IZ-AOI])

Die 1992 vom Regierungsrat gewählte Arbeitsgruppe Planung und Steuerung der Informatik und Kommunikation (AGIK) unter dem Vorsitz des Finanzdirektors hatte in Zusammenarbeit mit einem externen Dienstleister eine Informatikstrategie sowie strategische Richtlinien und Weisungen zu erarbeiten. Sie wurde 1993 als strategisches und bereichsübergreifendes Gremium zur Ausrichtung der Informatik konzipiert.[94] Aus dieser Arbeitsgruppe entstand ab 1999 im Kontext der versuchten Neustrukturierung der Verwaltungsinformatik die Kommission für strategische Informatikführung (KOSIF) (siehe hierzu Kapitel 6.1.1). Sie sollte im Auftrag des Regierungsrates die strategischen Schwerpunkte des Informatikeinsatzes in der Verwaltung vorlegen und die Eckwerte, die Rahmenbedingungen und den Geltungsbereich der Verwaltungsstrategie festlegen. Mit der Entscheidungskompetenz über die Informatikarchitektur hatte sie auch die Minimalanforderungen an die Bereiche festzulegen.[95]

Mit der Abteilung für Informatikplanung (AIP) schuf der Regierungsrat 1994 im Kontext der ersten Informatikstrategie eine zentrale Instanz für die Planung und Steuerung der Informatik. Die AIP beriet die Direktionen.[96] Sie war in der Finanzdirektion angesiedelt und nicht in den operativen Betrieb der Informatikdienstleistungen involviert.[97] Die bereits bestehende Abteilung für Organisation und Informatik (AOI), das spätere Amt für Informatikdienste (AID), nahm hingegen die Rolle eines internen Informatikdienstleisters ein.

In der zweiten Hälfte der 1990er-Jahre kam es im IT-Bereich im Umfeld des New Public Management zu einer Dezentralisierung der IT-Budgets in die Direktionen und mit der Gründung der Abraxas 1998 schliesslich zur Auslagerung der operativen kantonalen Informatik. Im Sinne dieser dezentralen Leistungserbringung verabschiedete der Kantonsrat 1999 ein neues Gesetz, welches die Auslagerung von Informatikdienstleistungen regelte und festhielt, dass das öffentliche Organ für die Erfüllung seiner Leistungen verantwortlich bleibt und die Daten durch organisatorische und technische Massnahmen vor unbefugter Einsichtnahme zu schützen sind.[98] Das Amt für Informatikplanung blieb zwar vorerst bestehen, nahm nun aber nur noch eine marginale Rolle ein. Mit der Neuen Informatikstrategie (NIS) und dem Aufbau der Organisation des Kantonalen IT-Teams (KITT) hob man das zentrale Amt für Informatikplanung 2003 ganz auf.[99]

---

94 RRB Nr. 1639/1992 vom 3. Juni 1992, Informatikorganisation (Arbeitsgruppe) (StAZH MM 3.198, S. 646).

95 RRB Nr. 540/1999 vom 17. März 1999, Strukturreform der Verwaltungsinformatik (Projekt «Espresso»), Betriebskonzept.

96 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 11.

97 RRB Nr. 3275/1993 vom 27. Oktober 1993, Informatikstrategie (StAZH MM 3.202, S. 1435–1438).

98 Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999 (LS 172.71).

99 RRB Nr. 1700/2003 vom 19. November 2003, Neue Informatikstrategie: Eckwerte, Organisationsmodell, Einführungs- und Migrationsplanung.

5.2 Erste rechtliche Grundlagen zur Informationssicherheit

5.2.1 Gesetz über den Schutz von Personendaten vom 6. Juni 1993 (Datenschutzgesetz, DSG)

Mit dem Gesetz über den Schutz von Personendaten vom 6. Juni 1993 erhielt der Datenschutz seine erste gesetzliche Grundlage im Kanton Zürich.[100] Der Kantonsrat überarbeitete die Vorlage, die der Regierungsrat bereits im Jahr 1987 eingebracht hatte, im Sinne des modernen Datenschutzes.[101] Aus Sicht des damals an den Beratungen beteiligten Kantonsratsmitglieds und späteren Regierungsrates, Markus Notter, war wohl die vorherrschende Stimmung im damaligen Regierungsrat, dass dieser ein Datenschutzgesetz mache, weil er es machen müsse. Der Regierungsrat habe einen mageren ersten Entwurf vorgelegt und sich gegen griffige Bestimmungen im Datenschutzgesetz gewehrt.[102]

Grundidee des Datenschutzes ist es, die Grundrechte der Personen zu schützen, deren Daten durch die öffentlichen Organe bearbeitet werden, wobei unter dem Begriff «Bearbeitung von Daten» nicht nur die Veränderung, sondern auch die Speicherung und Löschung zu verstehen ist.[103] Nur unter bestimmten Voraussetzungen haben öffentliche Organe das Recht, Daten von Personen zu bearbeiten. Diese Voraussetzungen machten einen wesentlichen Teil des ersten Datenschutzgesetzes des Kantons Zürich aus.[104] Bei der Datenbearbeitung im öffentlichen Bereich gilt es folgende Prinzipien und Grundsätze zu beachten (Tabelle 10)[105], die sowohl dem Datenschutzgesetz vom 6. Juni 1993 als auch dem Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007 zugrunde liegen:

Tabelle 10 Prinzipien des Datenschutzes und der Informationssicherheit

Grundsatz	Beschreibung	DSG	IDG	rev. IDG[106]
Legalität	Es gibt eine rechtliche Grundlage, welche die Bearbeitung der Daten erlaubt und umschreibt.	§ 4	§ 8 Abs. 2	§ 24 lit. a
Verhältnismässigkeit	Die Bearbeitung der Daten ist für die Aufgabenerfüllung geeignet und erforderlich.	§ 4	§ 8	§ 27
Zweckbindung	Daten dürfen nur für jene Zwecke bearbeitet werden, für die sie erhoben wurden.	§ 4	§ 9	§ 26
Archivierungspflicht	Nach der Datenbearbeitung und dem Ablauf der Aufbewahrungsfristen ändert sich der Zweck der Daten. Sie werden archiviert und dienen nun dazu, das Verwaltungshandeln historisch nachvollziehen zu können.	§ 14	§ 5	§ 8
Transparenz	Betroffenen Personen muss bekannt sein, dass Daten bearbeitet werden.	§ 15	§ 4	§ 6

[100] Gesetz über den Schutz von Personendaten vom 6. Juni 1993 (Datenschutzgesetz, DSG; LS 236.1).

[101] Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 7.

[102] Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 26.

[103] Protokoll der Befragung von Dominika Blonski vom 26. Januar 2024, S. 8; siehe § 1 lit. f DSG: «Bearbeiten: jeder Umgang mit Daten, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten von Daten».

[104] Gesetz über den Schutz von Personendaten vom 6. Juni 1993 (Datenschutzgesetz, DSG; LS 236.1).

[105] Protokoll der Befragung von Dominika Blonski vom 26. Januar 2024, S. 6–7.

[106] Das Gesetz über die Information und den Datenschutz (IDG) befindet sich aktuell in Totalrevision (Vorlage 5923). Die zuständige Kommission für Staat und Gemeinden des Kantonsrates hat ihre Vorberatungen hierzu am 10. Juli 2025 abgeschlossen.

Grundsatz	Beschreibung	DSG	IDG	rev. IDG[106]
Informationssicherheit	Daten sind mit organisatorischen und technischen Massnahmen zu schützen.	§ 4 Abs. 5	§ 7	§ 10
Verantwortlichkeiten	Es ist und bleibt immer die Institution, welche die Daten aufgrund ihres Auftrags bearbeitet oder bearbeiten lässt, dafür verantwortlich, alle gesetzlichen Grundsätze einzuhalten.	§ 6	§ 6 Abs. 2	§ 9 Abs. 2
Kontrolle	Die Datenbearbeitung wird nachvollziehbar dokumentiert und betroffene Personen haben das Recht, in die Daten Einsicht zu nehmen.	§ 17	§ 20	§ 6 / § 17

Die Daten- respektive Informationssicherheit war von Beginn an Teil des Datenschutzgesetzes. Denn bei der Bearbeitung der Daten galt es mit angemessenen Massnahmen sicherzustellen, dass diese Daten nicht missbraucht werden konnten.[107] Das DSG enthielt Bestimmungen zur Datensicherheit[108] sowie zur Vernichtung nicht mehr benötigter Daten.[109] So war festgelegt, dass Daten mit angemessenen organisatorischen und technischen Massnahmen geschützt werden müssen und nicht mehr benötigte Personendaten zu vernichten sind. Weiter war mit § 6 DSG bereits klar festgehalten, dass die Verantwortung für den Datenschutz und damit für die Einhaltung dieser gesetzlichen Bestimmungen beim öffentlichen Organ liegt, welches die Personendaten zur Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt. Aus Sicht der heutigen Datenschutzbeauftragten, Dominika Blonski, waren die Grundsätze des Datenschutzes bereits im ersten kantonalen Datenschutzgesetz (DSG) gegeben und die Bestimmungen zur Informationssicherheit sind heute inhaltlich noch dieselben.[110]

Eine weitere Neuerung des Datenschutzgesetzes war die Schaffung der Datenschutzbehörde. Diese hatte und hat die öffentlichen Organe zu beraten, deren Datenbearbeitungen zu kontrollieren, zwischen Bürgerinnen und Bürgern und den verantwortlichen Organen zu vermitteln und allgemein für das Anliegen des Datenschutzes zu sensibilisieren.[111] Der Regierungsrat wählte Bruno Baeriswyl als ersten Datenschutzbeauftragten und siedelte ihn in der damaligen Direktion der Justiz an. Eine Minderheit des Kantonsrates hätte sich bereits damals die Wahl durch den Kantonsrat gewünscht.[112]

5.2.2 Datenschutzverordnung vom 7. Dezember 1994 (DSV)

Die Datenschutzverordnung vom 7. Dezember 1994[113] umschrieb und konkretisierte die organisatorischen und technischen Massnahmen gegen das unbefugte Bearbeiten von Personendaten. So mussten die ergriffenen Massnahmen dem Stand der Technik entsprechen und in angemessenen Zeitabständen überprüft werden. Die Verordnung nannte u. a. Kontrollen von Datenträgern als eine der möglichen Massnahmen.[114]

---

107 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 7.

108 § 4 Abs. 5 DSG: «Daten müssen durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.».

109 § 14 DSG: «Nicht mehr benötigte Personendaten sind zu vernichten. Das verantwortliche Organ legt für jede Datensammlung fest, wann die Personendaten zu vernichten sind. Vorbehalten bleiben die Bestimmungen über die öffentlichen Archive.».

110 Protokoll der Befragung von Dominika Blonski vom 26. Januar 2024, S. 10.

111 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 7; siehe § 23 DSG.

112 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 7.

113 Datenschutzverordnung vom 7. Dezember 1994 (DSV; LS 236.11).

114 § 2 DSV.

Gemäss dem ehemaligen Datenschutzbeauftragten, Bruno Baeriswyl, löste das Inkrafttreten des Datenschutzgesetzes (DSG) und der Verordnung (DSV) am 1. Januar 1995 punkto Informationssicherheit eine erste Phase aus.[115]

5.2.3 Weisung über die Weiterverwendung von Informatikmitteln vom 2. August 1995

Ergänzend zu den rechtlichen Rahmenbedingungen erliess der Regierungsrat auch konkrete Weisungen zum Umgang mit nicht mehr benötigten Informatikmitteln.

Die erste allgemeinverbindliche Weisung aus dem Jahr 1992[116] sah ein zentral koordiniertes Vorgehen vor, welches die Entsorgung von Hardware umfasste. Zur effizienteren Abwicklung des Verkaufs von Informatikmitteln entschied der Regierungsrat jedoch 1995, die diesbezüglichen Entscheidungskompetenzen in die Direktionen zu delegieren. Gleichzeitig setzte er klare Richtlinien für die Weitergabe von Informatikmitteln fest: «Vor der Weitergabe von Datenträgern ist sicherzustellen, dass gespeicherte Daten so gelöscht werden, dass sie vom Empfänger durch technische Massnahmen nicht mehr reaktiviert werden können.»[117]

Die rechtlichen Vorgaben sowie die Weisung zum Umgang mit Informatikmitteln, namentlich die Notwendigkeit einer korrekten Löschung von Datenträgern, waren dem ehemaligen Vorsteher der Direktion der Justiz und der Direktion des Innern[118], Markus Notter, sowie dem ehemaligen Leiter der Hauptabteilung Logistik, Finanzen und Controlling, Renato Widmer, und dem dort angesiedelten ehemaligen Leiter der Informatikabteilung, Fredi Steiner, sehr bewusst.[119] Dieses starke Bewusstsein fand Ausdruck in einer sehr frühen und umfassenden Verschlüsselung der Datenträger in der JI (siehe Kapitel 7.2). Dass entsprechende Kenntnisse in der Verwaltung vorhanden sein konnten, zeigt sich auch darin, dass der ehemalige Datenschutzbeauftragte, Bruno Baeriswyl, in seinem ersten Tätigkeitsbericht 1995 konkrete Ausführungen zur sicheren Papierentsorgung und zur Vernichtung elektronischer Daten machte.[120]

5.2.4 Informatiksicherheitsverordnung vom 17. Dezember 1997 (ISV) und deren Umsetzung

Vorgaben der Informatiksicherheitsverordnung (ISV)

Um den Begriff der «angemessenen technischen und organisatorischen Massnahmen» gemäss § 4 DSG weiter zu konkretisieren, entstand in der Folge im Auftrag der Arbeitsgruppe Planung und Steuerung der Informatik und Kommunikation (AGIK) in enger Zusammenarbeit mit dem Datenschutzbeauftragten, Bruno Baeriswyl, und weiteren Stellen die Informatiksicherheitsverordnung (ISV).[121] Diese Verordnung regelte, was die Amtsstellen für die Realisierung der Informatiksicherheit vorzukehren hatten. Die ebenfalls für verbindlich erklärten Ausführungsrichtlinien unterstützten die Amtsstel-

---

115 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 7.

116 RRB Nr. 2216/1992 vom 8. Juli 1992, Weisung über die Weiterverwendung nicht mehr benötigter Informatikmittel (StAZH MM 3.198, S. 835–836).

117 RRB Nr. 2381/1995 vom 2. August 1995, Weisung über die Weiterverwendung nicht mehr genügender oder nicht mehr benötigter Informatikmittel (StAZH MM 3.207, S. 1134).

118 Ab 1999 in der Direktion der Justiz und des Innern (JI) zusammengeführt.

119 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 10; Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 9; Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 9.

120 Tätigkeitsbericht des Datenschutzbeauftragten 1995, «Informationssicherheit – Anstrengungen notwendig», S. 28–31.

121 Informatiksicherheitsverordnung vom 17. Dezember 1997 (ISV; LS 170.8); Tätigkeitsbericht des Datenschutzbeauftragten 1997, S. 6.

len bei der Umsetzung. Sie umfassten Erläuterungen und einen Plan mit kurzfristig realisierbaren und vielfach kostenneutralen organisatorischen und technischen Massnahmen.[122] Der Geltungsbereich der Verordnung erstreckte sich bewusst auf den Kanton und alle Stellen, die mit diesem Daten austauschten.[123] Gemäss dem ehemaligen Datenschutzbeauftragten, Bruno Baeriswyl, zeigte diese frühere Verordnung den Prozess und die Methodik auf, welche es den verantwortlichen Stellen erlaubt hätten, die Informationssicherheit selbständig umzusetzen: Ausgehend von einer Risikobeurteilung und der Einschätzung der möglichen Folgen (Abschnitt I) waren Sicherheitsstufen und Schutzziele (Vertraulichkeit, Integrität und Authentizität, Verfügbarkeit) festzulegen (Abschnitt II). Zu deren Erreichung waren Massnahmen zu planen, umzusetzen (Abschnitt III) und regelmässig zu überprüfen (Abschnitt V). Auch bei Datenbearbeitungen ausserhalb der Amtsstellen war zu vereinbaren, welche Massnahmen der Beauftragte zu treffen hatte und wie diese kontrolliert wurden (Abschnitt IV).[124] Dieser regelmässige Kontrollmechanismus, den man in der Verwaltung etablieren wollte, war aus Sicht des damaligen Datenschutzbeauftragten, Bruno Baeriswyl, ein wesentliches Element der ISV. Für die Erarbeitung der Massnahmenpläne sah die Verordnung bei bestehenden Informatiksystemen dann eine Zweijahresfrist vor.[125] Dabei sollte ein Kernteam um den Datenschutzbeauftragten die Umsetzung unterstützend begleiten.[126]

In Ergänzung zur ISV erklärte der Regierungsrat 1999 die Richtlinien und Anforderungen an die papiergebundenen Informationen für verbindlich.[127]

Umsetzung der Sicherheitsmassnahmen nach Informatiksicherheitsverordnung (ISV)

Für den Datenschutzbeauftragten zeigte sich, dass die Sicherheitsmassnahmen in der Praxis unterschiedlich umgesetzt wurden. Laut seinem Tätigkeitsbericht 2001 lag dies am Mangel an Ressourcen und internen Schutzmassnahmen sowie daran, dass das Know-how und die Nachkontrollen fehlten.[128] Auch in späteren Jahren kamen die Direktionen der rechtlichen Vorgabe kaum nach, die eigenen Sicherheitsmassnahmen intern sowie extern, wie in § 17 und § 18 ISV vorgesehen, regelmässig zu überprüfen. Es gab jedoch vereinzelte Ausnahmen.[129]

Der damalige Vorsteher der federführenden Direktion der Justiz und des Innern, Markus Notter, hat die Umsetzungsphase der ISV in der Gesamtverwaltung ebenfalls als zäh in Erinnerung. Auch wenn eine Direktion die Umsetzung ernst genommen hatte, waren die vielfältigen Anforderungen aufwendig umzusetzen.[130]

Ein wesentlicher Grund für die mangelhafte Umsetzung der Informatiksicherheitsverordnung (ISV) war für den Datenschutzbeauftragten, Bruno Baeriswyl, das Fehlen einer direktionsübergreifenden IT-Sicherheitsorganisation. Deshalb beantragte eine Arbeitsgruppe, bestehend aus dem Datenschutzbeauftragten und Mitarbeitenden der Abteilung für Informatikplanung (AIP), bei der Kommission für strategische Infor-

---

122 RRB Nr. 2783/1997 vom 17. Dezember 1997, Informatiksicherheitsverordnung.

123 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 15.

124 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 16.

125 § 20 ISV.

126 Tätigkeitsbericht des Datenschutzbeauftragten 1997, S. 6.

127 RRB Nr. 673/1999 vom 7. April 1999, Sicherheitsrichtlinien und -anforderungen für papiergebundene Information.

128 Tätigkeitsbericht des Datenschutzbeauftragten 2001, S. 28.

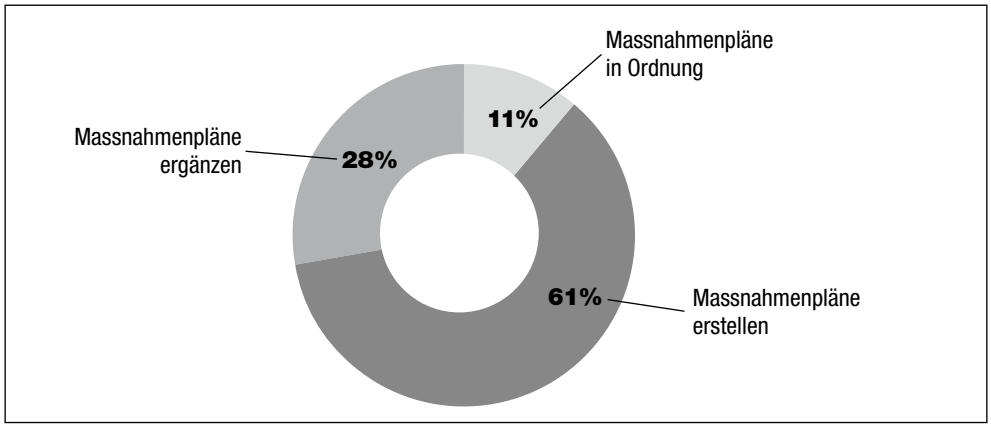
129 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 19.

130 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 9.

matikführung (KOSIF), eine Informatiksicherheitsstrategie auszuarbeiten: «Der unterschiedlichen Umsetzung der Sicherheitsmassnahmen gemäss Informatiksicherheitsverordnung müsste mit einer umfassenden Informatiksicherheitsstrategie begegnet werden.»[131] Aus Sicht der Arbeitsgruppe waren also zuerst direktionsübergreifende Zielsetzungen angezeigt, um die Mängel angehen zu können. Die KOSIF lehnte den Antrag mit der Begründung ab, dass die Zielsetzung mit mehr Datenschutzreviews und zusätzlichen Sensibilisierungsmassnahmen zu erreichen sei. Eine Freigabe der dafür benötigten Ressourcen erfolgte jedoch nicht.[132]

Die unterschiedliche Praxis bei der Umsetzung der Sicherheitsmassnahmen trat auch im Rahmen der Datenschutzreviews des Datenschutzbeauftragten zutage (Abbildung 3):

Abbildung 3 Umsetzung der Massnahmen der ISV



Quelle: Tätigkeitsbericht des Datenschutzbeauftragten 2003, S. 31.

In seinem Tätigkeitsbericht 2003 wies der Datenschutzbeauftragte, Bruno Baeriswyl, auf die mangelhafte Umsetzung respektive das Fehlen von Massnahmenplänen hin und empfahl, ein ganzheitliches IT-Sicherheitskonzept zu erarbeiten und einzuführen, um die mit der ISV angestrebten IT-Sicherheitsniveaus zu erreichen. Namentlich sollten in der kantonalen Verwaltung sicherheitsspezifische Rollen festgelegt werden, um dem übergreifenden Charakter des IT-Sicherheitsprozesses gerecht zu werden. Nur mit qualifizierten Mitarbeitenden mit entsprechenden Aufgaben könnten alle wichtigen Aspekte der Informationssicherheit berücksichtigt und die Aufgaben erledigt werden.[133]

Gemäss dem ehemaligen Vorsteher der JI, Markus Notter, in dessen Direktion der Datenschutzbeauftragte angesiedelt war, hatte der Datenschutzbeauftragte jedoch von Anfang an keinen einfachen Stand. Der Regierungsrat war der Meinung, dass es diese Position nicht brauche, und kritische Feststellungen in Berichten des Datenschutzbeauftragten führten innerhalb der Regierung zu Diskussionen.[134]

Auch aus der Sicht des ehemaligen Staatsschreibers, Beat Husi, hat man den Datenschutz nicht als etwas Wichtiges empfunden und ihn eher als hinderlich betrachtet. Der schwere Stand des Datenschutzes in jener Zeit zeigte sich in der Grundhaltung innerhalb des Regierungsrates: Er sah sich durch den Datenschutz in seinen Möglichkeiten eingeschränkt, zielführende Informatiklösungen zu realisieren. In den jährlichen Gesprächen versuchten die Mitglieder des Regierungsrates, den Datenschutzbeauf-

131 Tätigkeitsbericht des Datenschutzbeauftragten 2001, S. 28.

132 Tätigkeitsbericht des Datenschutzbeauftragten 2004, S. 12.

133 Tätigkeitsbericht des Datenschutzbeauftragten 2003, S. 27.

134 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 25.

tragten von der Notwendigkeit ihrer Projekte zu überzeugen. Zusammen mit dem Staatsschreiber rangen sie mit dem Datenschützer und überlegten sich bei den Projekten, wie man diese bei ihm durch- resp. an ihm vorbeibringen könnte.[135]

5.3 Sicherheitsinitiative 2004

Für eine Analyse des IT-Sicherheitsgrundschutzes und dessen Verbesserung mit Sofortmassnahmen beschloss der Regierungsrat 2004 die Sicherheitsinitiative und gab dem Datenschutzbeauftragten, Bruno Baeriswyl, den Auftrag, die Situation in der kantonalen Verwaltung zu analysieren, einen Bericht vorzulegen und Massnahmen zu empfehlen.[136] In seinem Schlussbericht empfahl der Datenschutzbeauftragte u. a., die Stelle eines kantonalen Chief Information Security Officer (CISO) zu schaffen. Mit der Schaffung angemessener Organisationsstrukturen im Bereich Sicherheit tat man sich aber allgemein schwer. Aus Sicht des ehemaligen Datenschutzbeauftragten, Bruno Baeriswyl, fehlte in den 2000er-Jahren die Sensitivität; die zunehmende Komplexität der Informatik und die Notwendigkeit zum Aufbau entsprechender Strukturen wurden unterschätzt.[137]

Gemäss dem ehemaligen Datenschutzbeauftragten, Bruno Baeriswyl, war der Kanton bemüht, im Bereich Sicherheit etwas zu machen, und war eigentlich auf gutem Weg, diesbezüglich ein Fundament zu schaffen, auch wenn die empfohlenen Massnahmen zum Grundschutz unterschiedlich umgesetzt wurden.[138]

5.4 Würdigung durch die PUK

In Bezug auf die rechtliche Situation kann die PUK Datensicherheit die Einschätzung des ehemaligen Vorstehers der JI, Markus Notter, teilen: «Also ich glaube, die rechtliche Situation – würde ich sagen – ist im Kanton Zürich nicht an der Spitze gewesen, aber recht fortschrittlich und gut organisiert.»[139] Die PUK Datensicherheit stützt die Aussage des ehemaligen Datenschutzbeauftragten, dass die gesetzlichen Grundlagen mit Datenschutzgesetz (DSG), Verordnung zum Datenschutzgesetz (DSV) und Informatiksicherheitsverordnung (ISV) eine gute Ausgangslage darstellten.[140] Die Informatiksicherheitsverordnung zeigte zudem konkret die Mechanismen auf, die man in der Verwaltung etablieren wollte. Weiter waren Regierungsratsbeschlüsse zum Umgang mit Informatikmitteln sowie papiergebundenen Informationen vorhanden und bekannt.

Kritisch zu sehen sind hingegen die in dieser Zeit abwehrende Grundhaltung des Regierungsrates gegenüber den Bestrebungen des Datenschutzes, die verzögerte Umsetzung der Sicherheitsmassnahmen in den Direktionen, die fehlende kantonale Sicherheitsorganisation und der Entscheid der Kommission für strategische Informatikführung (KOSIF), in diesem Zusammenhang auf die Erarbeitung einer Informatiksicherheitsstrategie zu verzichten. Mit der Umsetzung der Sicherheitsinitiative reagierte der Regierungsrat jedoch auf entsprechende Rückmeldungen des Datenschutzbeauftragten.

---

135 Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 6–7.

136 Tätigkeitsbericht des Datenschutzbeauftragten 2004, S. 35.

137 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 19.

138 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 9.

139 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 8.

140 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 14.

Erst mit der 2021 eingeleiteten und 2022 verabschiedeten Cybersicherheitsstrategie wird eine eigene strategische Grundlage für die Informationssicherheit vorliegen.[141]

Die PUK Datensicherheit stellt mit grossem Unverständnis fest, dass für die Informationssicherheit erst im Jahr 2022 eine eigene Strategie vorliegt, obwohl der ehemalige Datenschutzbeauftragte, Bruno Baeriswyl, eine solche bereits im Jahr 2004 gefordert hatte. Dieses lange Zuwarten ist nicht nachvollziehbar.

[141] RRB Nr. 676/2022, Cybersicherheitsstrategie (Festsetzung, Umsetzung, Stellenplan, Ausgabenbewilligung). Laut der Allgemeinen Informationssicherheitsrichtlinie vom 16. April 2025 ist künftig die Bezeichnung «Kantonale Informationssicherheitsstrategie» vorgesehen.

6. Kantonale Entwicklung 2006–2014: Das KITT-Umfeld und die gescheiterte Umsetzung der Informatikstrategie 2008

6.1 KITT-Umfeld

6.1.1 Vorgeschichte

Im Rahmen der Reformen hin zu einer wirkungsorientierten Verwaltungsführung (wif) versuchte der Regierungsrat ab 1997, auch die Informatik neu aufzustellen, und definierte die Kommission für strategische Informatikführung (KOSIF) unter der Leitung des Finanzdirektors als direktionsübergreifendes Planungsgremium. Die mit RRB Nr. 540/1999 beschlossene gesamtheitliche Neuausrichtung der IT scheiterte jedoch.[142] Die beabsichtigte Zentralisierung von IT-Basisdiensten stiess gemäss GPK-Tätigkeitsbericht 2002/2003 auf starken Widerstand und die damalige Verwaltungsstruktur und das politische Umfeld liessen eine Umsetzung der neuen Zusammenarbeitsformen nicht zu. Eine externe Evaluation stellte schliesslich fest, dass die direktionsübergreifende Zusammenarbeit zu wenig wirksam und die IT-Strategie im Bereich der Organisation zu verbessern sei.[143] Der Wunsch, die kantonale IT stärker zusammenzuführen, traf auf die gewachsene dezentrale IT-Infrastruktur mit quasi eigenständigen Informatikdiensten in den Direktionen. In seinem Grundsatzentscheid für eine Neue Informatikstrategie (NIS) schuf der Regierungsrat 2002 die Basis für das Kantonale IT-Team (KITT) und verzichtete vor dem Hintergrund der Erfahrungen mit vergangenen Dezentralisierungs- und Zentralisierungsbemühungen auf den Versuch, erneut eine zentrale Organisationseinheit zu schaffen.[144] Die KOSIF erhielt den Auftrag, zu den wichtigsten Problemfeldern der direktionsübergreifenden Informatik Lösungsvorschläge auszuarbeiten. Im direktionsübergreifend zusammengesetzten Projektteam fand ein Bewusstseinswandel statt und es reifte die Idee, dass direktionsübergreifende Probleme auch mit direktionsübergreifenden Lösungen angegangen werden sollten. Die Neue Informatikstrategie (NIS) konzentrierte sich auf die direktionsübergreifende Informatik und folgte dem Kernsatz «Für ein Problem gibt es eine Lösung». Die bisherige direktionsübergreifende Organisation, bestehend aus der KOSIF, der Abteilung für Informatikplanung (AIP) sowie den Foren der Informatikverantwortlichen und Informatikcontroller, wurde durch die KITT-Organisation ersetzt. Die Verantwortung für die direktionsübergreifenden Informatikbelange übertrug man dem direktional zusammengesetzten KITT-Gremium.[145]

6.1.2 KITT-Umfeld

Am 1. Januar 2006 trat die Verordnung über die direktionsübergreifende Informatik (KITT-Verordnung) in Kraft.[146] Sie regelte die gemeinsamen Informatiklösungen der kantonalen Verwaltung, einschliesslich der unselbständigen Anstalten.[147] Ziel der

---

142 RRB Nr. 1700/2003 vom 19. November 2003, Neue Informatikstrategie: Eckwerte, Organisationsmodell, Einführungs- und Migrationsplanung.

143 Bericht der Geschäftsprüfungskommission vom 18. September 2003 über ihre Tätigkeit vom Oktober 2002 bis September 2003 und über den Geschäftsbericht 2002 des Regierungsrates (KR-Nr. 240/2003), S. 39.

144 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 11.

145 RRB Nr. 1700/2003 vom 19. November 2003, Neue Informatikstrategie: Eckwerte, Organisationsmodell, Einführungs- und Migrationsplanung.

146 Verordnung über die direktionsübergreifende Informatik (KITT-Verordnung; LS 170.7).

147 § 1 Abs. 1 KITT-Verordnung.

KITT-Verordnung war es, eine koordinierte, wirtschaftliche und qualitativ hochwertige Umsetzung solcher Lösungen über verschiedene Direktionen hinweg sicherzustellen. Sie folgte dem Grundsatz «eine Anforderung – eine Lösung» und förderte die Standardisierung von direktionsübergreifenden Informatikprozessen, Anwendungssystemen und Infrastrukturen.[148] Zentrales Element war das Kantonale IT-Team (KITT), das sich aus Vertreterinnen und Vertretern aller Direktionen sowie der Staatskanzlei zusammensetzte.[149] Das KITT war für direktionsübergreifende IT-Belange zuständig und entschied, welche IT-Services, -Prozesse und -Standards eingeführt und in welcher Form umgesetzt wurden.[150] Zu den Aufgaben des KITT zählten unter anderem die Pflege und Weiterentwicklung der kantonalen Informatikstrategie, die Planung und Steuerung von IT-Vorhaben sowie die Festlegung globaler Standards.[151] Unterstützt wurde das KITT durch die KITT-Geschäftsstelle sowie die Kompetenz- und Servicezentren, die für die operative Umsetzung und den Betrieb verantwortlich waren.[152]

Das KITT hatte Beschlüsse über die Festlegung oder Aufhebung von direktionsübergreifenden IT-Services, -Prozessen und -Standards einstimmig zu fassen. Lag keine Einstimmigkeit vor, mussten die Beschlüsse dem Regierungsrat zur Genehmigung vorgelegt werden.[153] Bei Vorhaben von grösserer Tragweite oder bei solchen mit Genehmigungspflicht durch den Regierungsrat war die Leitung der KITT-Geschäftsstelle, die den KITT-Vorsitz innehatte, verpflichtet, im Vorfeld eine Stellungnahme der Generalsekretärenkonferenz einzuholen.[154] Kam es hierbei zu Meinungsverschiedenheiten, hatten das KITT und die Generalsekretärenkonferenz eine einvernehmliche Lösung anzustreben.[155]

Trotz kurzer Kommunikationswege, eines grundsätzlich vorhandenen Bewusstseins für Informationssicherheit[156] und einer als sinnvoll erachteten organisatorischen Verortung des KITT in der Finanzdirektion[157] wurde das Gremium von vielen Beteiligten als «schwaches» Organ wahrgenommen.[158] Es wurde als «Verhinderungskonstrukt»[159] bezeichnet oder als schwerfälliges Konstrukt gesehen, das den Anforderungen an eine einheitliche, direktionsübergreifende Informatik nur bedingt gerecht werden konnte.[160] Das Vorankommen des KITT wurde gemäss Beteiligten durch verschiedene Aspekte verhindert.

---

148 § 2 KITT-Verordnung.

149 § 4 Abs. 1 KITT-Verordnung.

150 § 8 Abs. 1 KITT-Verordnung.

151 § 8 Abs. 2 KITT-Verordnung.

152 §§ 12 ff. KITT-Verordnung.

153 § 9 Abs. 2 KITT-Verordnung.

154 § 10 Abs. 1 KITT-Verordnung.

155 § 10 Abs. 3 KITT-Verordnung.

156 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 6, 23.

157 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 16 (in Bezug auf die Verortung in der Finanzdirektion); Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 11 (in Bezug auf die Angliederung des Informatiksicherheitsbeauftragten an die KITT-Geschäftsstelle).

158 Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 11.

159 Protokoll der Befragung von Ursula Gut-Winterberger vom 20. September 2024, S. 8–9.

160 Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 7; Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 9; Protokoll der Befragung von Ursula Gut-Winterberger vom 20. September 2024, S. 8.

Interessen der Direktionen

Die zugrunde liegende Idee des KITT-Modells war es, alle Direktionen ins Boot zu holen und durch das Einstimmigkeitserfordernis zu gemeinsamer Verantwortung zu bewegen. Der dahinterliegende Gedanke war, dass sich die Direktionen unter einem gewissen Druck zusammenraufen sollten.[161] Wie die Beteiligten ausführten, erwies sich dies in der Praxis jedoch als schwierig. So wurde unter anderem kritisiert, dass die KITT-Mitglieder die eigenen Interessen ihrer Direktion verfolgten, anstatt eine einheitliche Regelung anzustreben,[162] und dass die Stellung eines KITT-Mitglieds teilweise davon abhing, wie dieses in der Direktion verortet war und welchen Zugang es zur Direktionsvorsteherin oder zum Direktionsvorsteher hatte.[163] Schliesslich war der Regierungsrat, der allfällige Beschlüsse des KITT zu genehmigen hatte, zu weit vom Thema entfernt und spürte den Druck der IT-Benutzerinnen und -Benutzern aus der eigenen Direktion.[164]

Einstimmigkeit

Die gesetzlich geforderte Einstimmigkeit für Beschlüsse wurde sodann als weiteres zentrales Hindernis erachtet.[165] Sie erschwerte die Entscheidungsfindung erheblich, zumal die Bedürfnisse und Ausgangslagen in den Direktionen sehr unterschiedlich waren, etwa durch bereits implementierte IT-Systeme[166] oder unterschiedliche Zielgruppen.[167] Eine Weisungsbefugnis anstelle dieses Entscheidungsmechanismus wäre aus Sicht vieler Beteiligter zielführender gewesen.[168] Das ursprünglich beabsichtigte Ziel, durch ein Einstimmigkeitserfordernis alle Beteiligten zu gemeinsamer Verantwortung zu bewegen, erwies sich schliesslich als kontraproduktiv. Die Folge war eine zunehmende Handlungsunfähigkeit des Gremiums.

6.1.3 Hemmende Wirkung der KITT-Organisation auf Zentralisierungsbemühungen

Die oben beschriebenen Herausforderungen führten dazu, dass das KITT regelmässig im Gesamtregierungsrat diskutiert wurde.[169] Das KITT war aber kein ständiges Traktandum in den Sitzungen des Regierungsrates.[170] Die KITT-Verordnung wurde schliesslich mit Beschluss des Regierungsrates vom 25. April 2018 aufgehoben und per 1. Juli 2018 ausser Kraft gesetzt.[171]

Rückblickend zeigt sich, dass das KITT-Konstrukt in der Praxis mit erheblichen strukturellen und organisatorischen Herausforderungen konfrontiert war. Besonders augenfällig waren die Spannungen zwischen dem KITT und der KITT-Geschäftsstelle. Während die KITT-Geschäftsstelle neue Ideen zur Vereinheitlichung der direktionsübergreifenden Informatik ausarbeitete, zeigten sich die KITT-Mitglieder und die

---

161 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 10–12.

162 Protokoll der Befragung von Ursula Gut-Winterberger vom 20. September 2024, S. 10.

163 Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 10–11.

164 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 12.

165 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 6 f.

166 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 27.

167 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 9, 12.

168 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S 16, 27; Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 7, 10–11.

169 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 9.

170 Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 7.

171 Verordnung über die direktionsübergreifende Informatik (KITT-Verordnung; LS 170.7) (Aufhebung vom 25. April 2018), OS Band 73, S. 192.

Regierungsmitglieder mit den jeweiligen IT-Lösungen in den eigenen Direktionen zufrieden und hatten meist kein Interesse an einer Zentralisierung der Informatik. Das mag auch daran gelegen haben, dass die Mitglieder des Regierungsrates oft von ihren eigenen KITT-Vertretern über die Entwicklungen im KITT ins Bild gesetzt wurden.[172] Die grundsätzliche Zufriedenheit mit den eigenen IT-Leitern stärkte den Status quo. Da dieser für die Mitglieder des Regierungsrates stimmte, liefen die Bemühungen der damaligen Finanzdirektorin, Ursula Gut-Winterberger, die KITT-Geschäftsstelle im Sinne einer zentraleren Lösung zu unterstützen, ins Leere.[173] Gesamtkantonale Lösungen brachten für die Direktionen je nachdem unterschiedliche Anpassungskosten. Deshalb kam es vor, dass Regierungsmitglieder, die eigentlich gesamtkantonalen Lösungen positiv gegenüberstanden, in konkreten Einzelfällen bremsten.[174] Gemäss Aussage eines damals direkt beteiligten Regierungsratsmitglieds gab es in den Jahren 2011–2015 im Regierungsrat, verglichen mit den folgenden Jahren, mehr Bedenken und Widerstand gegen eine Zentralisierung.[175] Vor dem Hintergrund der damals sehr vielfältigen IT-Landschaft und dem damit verbundenen Anpassungsaufwand war die Kooperationsbereitschaft im Regierungsrat diesbezüglich lediglich mittelgross.[176] Einer weiteren überlieferten Schilderung zufolge herrschte in jener Zeit noch stärker eine «Direktionslogik» und die IT wurde als «Direktionsgebiet» und nicht direktionsübergreifend verstanden. Je nach Direktion war sie auch noch wesentlich ausgeprägter in den Ämtern angesiedelt.[177]

6.1.4 Bericht der FIKO/GPK-Subkommission 2009

Bereits 2009 beurteilte die Subkommission der Geschäftsprüfungskommission (GPK) und der Finanzkommission (FIKO) in ihrem Bericht die Organisation der kantonalen Informatik kritisch, da sie die Gefahr berge, dass Einzelinteressen der Direktionen überwiegen, und damit die Vereinheitlichung und Standardisierung nicht im gewünschten Mass vorangetrieben werden könne. Sie empfahl, die Organisation der Informatik und die KITT-Verordnung zu überprüfen und der KITT-Geschäftsstelle klare Kompetenzen und Ressourcen für die operative Ebene der kantonalen Informatik zuzuweisen. Die Subkommission stellte auch fest, dass zwischen den Direktionen bezüglich IT-Sicherheit beträchtliche Unterschiede bestanden, und verlangte eine für alle Direktionen verbindliche und zentrale Regelung von IT-Sicherheitsfragen.[178]

6.2 Informatikleitbild 2006

In seinem Informatikleitbild 2006 hat das Kantonale IT-Team (KITT) die Ziele und Grundsätze für den Einsatz der Informatik in der Verwaltung und deren mittel- und langfristige Entwicklung festgelegt. Mit seinem Beschluss vom 20. Dezember 2006 hat der Regierungsrat das Informatikleitbild verabschiedet und die damit verbundene strategische Ausrichtung gutgeheissen.[179]

---

172 Protokoll der Befragung von Ursula Gut-Winterberger vom 20. September 2024, S. 8.

173 Protokoll der Befragung von Ursula Gut-Winterberger vom 20. September 2024, S. 12–13.

174 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 27.

175 Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 11.

176 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 12.

177 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 16–17.

178 Bericht der Finanzkommission und der Geschäftsprüfungskommission über ihre Abklärungen zur IT in der kantonalen Verwaltung und zur IT-Strategie des Regierungsrates vom 24. September 2009 und 1. Oktober 2009.

179 RRB Nr. 1835/2006 vom 20. Dezember 2006, Informatikstrategie, Festlegung Leitbild.

Das Informatikleitbild äussert sich kurz zu Datenschutz und Informatiksicherheit. Die geltenden gesetzlichen Vorgaben fanden Eingang in das Dokument, wurden jedoch nicht weiter konkretisiert.

Zielsetzung

– «Die Informatik stellt die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen und Informationssysteme sicher.»

Führungs- und Einsatzleitlinien

– «Beim Einsatz der Informatik werden die eidgenössischen und kantonalen Vorschriften betreffend Datenschutz und Datensicherheit erfüllt.»
– «Alle an den Informatikprozessen Beteiligten nehmen ihre Verantwortung wahr, die notwendigen Schutzmassnahmen für eine sichere Anwendung der Informatikmittel einzuführen bzw. anzuwenden.»
– «Die Risiken bei der Datenbearbeitung sind angemessen zu minimieren.»
– «Dabei werden die Aspekte des Datenschutzes sowie des Schutzes, der Praktikabilität und der Wirtschaftlichkeit der Datensicherheit berücksichtigt.»[180]

6.3 Vorgaben zur Informationssicherheit im Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007

Im Gesetz über die Information und den Datenschutz (IDG)[181] regelte der Kanton Zürich das Öffentlichkeitsprinzip, welches durch die neue kantonale Verfassung eingeführt worden war. Da das neue Grundrecht auf Zugang zu amtlichen Dokumenten[182] in einem Spannungsverhältnis zum Schutz der Privatsphäre der Einzelnen steht, verzahnte der Gesetzgeber das Öffentlichkeitsprinzip konsequent mit dem Datenschutz. Im Rahmen der Reform verzichtete der Regierungsrat bewusst darauf, den Datenschutzbeauftragten zu stärken, indem er ihm die Funktion des Öffentlichkeitsbeauftragten übertragen hätte.[183] Stattdessen schuf er in der Staatkanzlei eine Koordinationsstelle IDG und bezeichnete in allen Direktionen eine zentrale Ansprechperson (§ 28 IDV).[184] Die Umsetzung des Öffentlichkeitsprinzips war damit organisatorisch von der Umsetzung der übrigen Aspekte des IDG getrennt.

Allgemein stärkte jedoch das neue Gesetz die Datenschutzbehörde: Sie wurde administrativ aus der JI herausgelöst, und die Wahl der oder des Datenschutzbeauftragten unterlag neu der Genehmigung des Kantonsrates. Weiter erhielt die Datenschutzbehörde die Möglichkeit, Verfügungen der Verwaltung anzufechten. Im engeren Bereich der Informationssicherheit, als Element des Datenschutzes, änderte sich materiell nichts Wesentliches.[185] Die Informationssicherheit ist in § 7 IDG geregelt und nachfolgend tabellarisch zusammengefasst (Tabelle 11).[186]

---

[180] Informatikleitbild der Kantonalen Verwaltung Zürich. Vom KITT verabschiedet am 26. Oktober 2006, vom Regierungsrat genehmigt am 20. Dezember 2006. Die Abschnitte zu Datenschutz und Informatiksicherheit befinden sich auf den S. 4 und 6.

[181] Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (IDG; LS 170.4).

[182] Art. 17 der Verfassung des Kantons Zürich vom 27. Februar 2005 (KV; LS 101).

[183] Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 25.

[184] Verordnung über die Information und den Datenschutz vom 28. Mai 2008 (IDV; LS 170.41).

[185] Protokoll der Befragung von Dominika Blonski vom 26. Januar 2024, S. 10.

[186] Für die folgenden Ausführungen siehe auch § 7 Informationssicherheit, in: Baeriswyl/Rudin (2012): Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), S. 44–52.

Tabelle 11 IDG-Bestimmungen zur Informationssicherheit

§ 7 Abs. 1	Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.
§ 7 Abs. 2	Die Massnahmen richten sich nach den folgenden Schutzzielen:
§ 7 Abs. 2 lit. a	Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen,
§ 7 Abs. 2 lit. b	Informationen müssen richtig und vollständig sein,
§ 7 Abs. 2 lit. c	Informationen müssen bei Bedarf vorhanden sein,
§ 7 Abs. 2 lit. d	Informationsbearbeitungen müssen einer Person zugerechnet werden können,
§ 7 Abs. 2 lit. e	Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.
§ 7 Abs. 3	Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.

Informationen sind unabhängig vom Medium, auf dem sie sich befinden, angemessen zu schützen. Gemäss § 3 Abs. 2 IDG fallen darunter jegliche Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen. Angemessen sind die Massnahmen dann, wenn damit die folgenden Grundsätze der Informationssicherheit eingehalten werden können (Tabelle 12):

Tabelle 12 Grundsätze der Informationssicherheit

Grundsatz	Mögliche Massnahme
Vertraulichkeit (§ 7 Abs. 2 lit. a IDG)	Verschlüsselung/Zugriffskonzept
Integrität (§ 7 Abs. 2 lit. b IDG)	Zertifikate
Verfügbarkeit (§ 7 Abs. 2 lit. c IDG)	Backup-Systeme
Authentizität (§ 7 Abs. 2 lit. d IDG)	Passwort/Smartcard mit Zertifikat
Nachvollziehbarkeit (§ 7 Abs. 2 lit. e IDG)	Automatisierte Aufzeichnungen

Bei grösseren Informationsbearbeitungen ist folglich ein Informationssicherheitskonzept notwendig, welches auf die geltenden Vorgaben Bezug nimmt und darlegt, wie die technischen und organisatorischen Massnahmen sicherstellen, dass die Informationsbearbeitung gesetzmässig erfolgt. Die Angemessenheit der Massnahmen ist zudem regelmässig zu überprüfen, da sich der Verwendungszweck der Informationen ändern kann oder die Massnahmen mit der technologischen Entwicklung nicht Schritt halten können.[187]

6.4 Informatikstrategie 2008 und deren Umsetzung

Mit Beschluss vom 9. Dezember 2008 verabschiedete der Regierungsrat die «Informatikstrategie der Kantonalen Verwaltung Zürich», welche die Ausrichtung der kantonalen Informatik unter den neuen Rahmenbedingungen regelte.[188]

Im Bereich der Informationssicherheit enthielt die Strategie folgende Ziele: «Die bestehenden Sicherheitsvorgaben werden eingehalten und wenn notwendig zusätzliche Sicherheitsstandards definiert, umgesetzt und gepflegt. Das Sicherheitsbewusstsein aller Mitarbeitenden der kantonalen Verwaltung wird laufend gefördert.»[189]

---

[187] Baeriswyl, Bruno / Rudin, Beat (2012): Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), S. 44–52.

[188] RRB Nr. 1955/2008 vom 9. Dezember 2008, Informatikstrategie, Festlegung.

[189] Kantonales IT-Team (KITT), Informatik-Strategie der Kantonalen Verwaltung Zürich. Vom Kantonalen IT-Team (KITT) am 31. Oktober 2008 verabschiedet, S. 17–18.

Die Strategie hielt in ihren Prinzipien fest, dass die eidgenössischen und kantonalen Vorschriften betreffend Datenschutz, Sicherheit und Umgang mit Informationen und Personendaten in Bezug auf die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität erfüllt werden und dazu klare Rollen und Verantwortlichkeiten zugewiesen werden müssen.

Es war dem KITT bewusst, dass Informatiksicherheit ein übergreifendes Thema ist, welches vom Aufbau einer Informatiksicherheitsarchitektur abhängt, namentlich von der Entwicklung einheitlicher Sicherheitskonzepte sowie dem Aufbau eines kantonsweiten Informatiksicherheits-Managementsystems (ISMS). Um den notwendigen Sicherheitsstandard zu erreichen, sollten die benötigten Massnahmen im Bereich der Organisation getroffen sowie Rollen und Verantwortlichkeiten zugewiesen werden. Dazu wollte das KITT ein Kompetenzzentrum Informatiksicherheit bilden, welches entsprechende Grundlagen zu erarbeiten hatte.

Die Informationssicherheit war damit ein wesentlicher Teil der Umsetzung der kantonalen Informatikstrategie. Am 13. November 2011 verabschiedete das mit der Umsetzung betraute KITT das Organisationskonzept für die Informatiksicherheit.[190] Gemäss diesem Konzept war folgende kantonale Informatiksicherheitsorganisation vorgesehen:

– Es sollte ein Kompetenzzentrum Informatiksicherheit (CC I-Si) unter der Leitung des Informatik-Sicherheitsbeauftragten (I-SiBZH)[191] geschaffen werden. Diese Funktion sollte als zentrale Stelle für alle Aspekte der Informatiksicherheit fungieren und die Bestrebungen für eine angemessene Informatiksicherheit innerhalb der kantonalen Verwaltung unterstützen. Dazu konnte das KITT IT-Sicherheitsaufgaben an den Informatik-Sicherheitsbeauftragten delegieren.
– Weiter war eine Fachgruppe Informatiksicherheit (FG I-Si) vorgesehen. Neben anderen Spezialisten sollten auch die von den Direktionen zu bestimmenden Informatik-Sicherheitsbeauftragten der Direktion/Staatskanzlei darin Einsitz nehmen.

Im Bereich der Informatiksicherheit sollten mit der Umsetzung der Informatikstrategie drei Ziele erreicht werden:

– Auf Grundlage eines Informatiksicherheitskonzepts wird eine kantonale Informatiksicherheitsorganisation geschaffen, welche die Aufgaben, Kompetenzen und die Verantwortung der beteiligten Stellen und Personen klärt.
– Ein kantonales Managementsystem für Informatiksicherheit (ISMS) legt die Basis für die Umsetzung der Informationssicherheit in den Direktionen und der Staatskanzlei.
– Eine revidierte Informatiksicherheitsverordnung berücksichtigt die neuen gesetzlichen Grundlagen[192], klärt den Zuständigkeitsradius und regelt die Verantwortlichkeiten und Organisation der kantonalen Informatiksicherheit.[193]

---

[190] Kantonales IT-Team (KITT), Strategieumsetzungseinheit 2 Informatiksicherheit – Organisationskonzept für die Informatiksicherheit in der kantonalen Verwaltung Zürich. Version 2.4 vom 19. September 2014.

[191] Die PUK Datensicherheit verwendet für den Informatik-Sicherheitsbeauftragten des Kantons Zürich im Folgenden die einfachere Abkürzung I-SiBe. Mit der Abkürzung ISIK bezeichnen wir jeweils den aktuellen Informationssicherheitsbeauftragten des Kantons. Für die Fachgruppe Informatiksicherheit respektive Informationssicherheit verwenden wir die Abkürzung FAGIS.

[192] Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999 (LS 172.71); Verordnung über die Nutzung von Internet und E-Mail vom 17. September 2003 (LS 177.115); Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007 (IDG; LS 170.4).

[193] Kantonales IT-Team (KITT), Informatikstrategie Kanton Zürich (RRB Nr. 1955/2008): Stand der Umsetzung. 2014, S. 11–13.

6.5 Berichte der Finanzkontrolle zur Situation der kantonalen Informatik

6.5.1 IT-Prüfungstätigkeit der Finanzkontrolle

Vor 2010 nahm die Finanzkontrolle im IT-Bereich nur punktuelle Prüfungen vor. Im Jahr 2010 kam die Finanzkontrolle zum Schluss, dass es auch ihre Aufgabe sei, die gesamte IT-Situation einmal grundlegend zu betrachten, weil das IT-Umfeld sich natürlicherweise mit finanzrelevanten Zahlungsströmen, Beschaffungen sowie Fragen der Projektorganisation befasst. Dennoch war die Informations- und Datensicherheit im Sinne einer Aufgabenabgrenzung gegenüber der Datenschutzbehörde nicht primärer Fokus der Finanzkontrolle und ist es auch heute nicht.[194] Um die IT-Prüfungen voranzubringen, entschied die Finanzkontrolle, die damals noch kaum eigene diesbezüglichen Ressourcen aufwies, im Jahr 2010 mithilfe eines externen Partners die IT-Situation im Kanton Zürich zu beleuchten. Auf Basis von IT-Kurzchecks liess sie sich in den nächsten zwei Jahren von den verschiedenen Direktionen und Ämtern zur Maturität ihrer IT-Organisation informieren. Die Selbstbeurteilung der befragten Leitungsorgane im IT-Bereich fiel sehr positiv aus und war sicherlich überhöht und deshalb problematisch.[195]

6.5.2 Feststellungen der Finanzkontrolle zur IT-Situation des Kantons Zürich

Der Bericht der Finanzkontrolle lag im August 2013 vor. Darin machte die Finanzkontrolle im Bereich der kantonalen Informatiksicherheit verschiedene Lücken und erheblichen Nachholbedarf aus:

– Im Bereich des Zugriffsschutzes, der die Vertraulichkeit der Informationen sichern soll, waren Berechtigungskonzepte oftmals nicht vorhanden, obwohl die geltende Informatiksicherheitsverordnung die Klassifizierung von Informationen vorschrieb und damit die Basis für Zugriffskonzepte vorhanden gewesen wäre. Zudem fehlte es an der Sensibilisierung der Benutzer im Umgang mit Passwörtern.
– Weiter existierte kein verbindliches IT-Sicherheitsmanagement für den Kanton Zürich und auch kein mit entsprechenden Kompetenzen ausgestatteter IT-Sicherheitsbeauftragter.[196]

Die Finanzkontrolle empfahl, die Lücken rasch mit ergänzenden Vorgaben und konkreter Umsetzung der bestehenden strategischen Anforderungen zu reduzieren sowie der Führung und der Sicherheit im IT-Bereich eine erhöhte Aufmerksamkeit zu schenken, da sich hinter den Lücken erhebliche Risiken für den Kanton Zürich verbargen.[197] Die Finanzkontrolle wies in ihrem Bericht auch darauf hin, dass die festgestellten Lücken Ausdruck der mangelhaften Umsetzung der Informatikstrategie aus dem Jahr 2008 seien. So seien Vorgaben der kantonalen Informatikstrategie, wie die Ziele zur Informatiksicherheit, nicht oder nur unzureichend umgesetzt.

---

194 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 8.

195 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 10.

196 Bericht der Finanzkontrolle in Zusammenarbeit mit bprex group AG vom 30. August 2013: «Erkenntnisse zur IT-Situation des Kantons Zürich. Würdigung anhand der Resultate aus den IT-Kurzchecks unter Berücksichtigung der KITT-Aktivitäten», S. 25–26.

197 Bericht der Finanzkontrolle in Zusammenarbeit mit bprex group AG vom 30. August 2013: «Erkenntnisse zur IT-Situation des Kantons Zürich. Würdigung anhand der Resultate aus den IT-Kurzchecks unter Berücksichtigung der KITT-Aktivitäten», S. 5.

Kompetenzzentrum Informationssicherheit

Obwohl die damals Befragten die Notwendigkeit zum Erlass zentraler Vorgaben für ein Informationssicherheits-Managementsystem und die Schaffung einer entsprechenden Stelle allgemein anerkannten und unterstützten, war gemäss dem Bericht der Finanzkontrolle dennoch erst 2016 mit dem Aufbau des Managementsystems für Informatiksicherheit (ISMS) zu rechnen, denn die Ansiedlung des Kompetenzzentrums IT-Sicherheit war zwischen der Finanzdirektion und Direktion der Justiz und des Innern (JI) umstritten. Das KITT wünschte eine Ansiedlung in der JI, während die Finanzdirektion diese Verantwortung bei sich haben wollte. Die Beziehung zwischen dem Kantonalen IT-Team (KITT) und der Finanzdirektion wurde im Bericht als schwierig beschrieben.[198]

Aus Sicht der damaligen Finanzdirektorin, Ursula Gut-Winterberger, war auch das Verhältnis zwischen dem KITT-Gremium aus Vertretern der Direktionen und der Staatskanzlei sowie der KITT-Geschäftsstelle, die in der Finanzdirektion angesiedelt war, nicht einfach. Ihren Widerstand gegen den KITT-Entscheid begründete sie in der Befragung durch die PUK Datensicherheit mit dem Auftreten und der Dominanz des JI-Vertreters im KITT-Gremium sowie dessen Art, sich durchzusetzen. Renato Widmer, der damalige Leiter der Hauptabteilung Finanzen, Logistik und Controlling (LFC), fungierte bereits seit 1999 in den direktionsübergreifenden Gremien als Vertreter der Belange der Direktion der Justiz (und des Innern).[199] Die Finanzdirektorin wollte vermeiden, dass mit der Ansiedlung des Kompetenzzentrums in der JI die bereits starke Rolle des Leiters LFC noch weiter gestärkt würde.[200] Auch wenn das Thema Datensicherheit traditionellerweise in der JI verortet war, war für den ehemaligen Vorsteher der JI, Martin Graf, gut nachvollziehbar, dass die damalige Finanzdirektorin, Ursula Gut-Winterberger, mit der Zuständigkeit für die KITT-Geschäftsstelle die Datensicherheit in der Finanzdirektion ansiedeln wollte.[201] In der Folge legte die Finanzdirektion den Antrag des KITT, der eine Verortung des Informatiksicherheitsbeauftragten in der JI vorsah, dem Regierungsrat nicht zur Beschlussfassung vor.[202]

Rückblickend nahm die GPK in ihrem Bericht aus dem Jahr 2017 auf die damals fehlende Einigung zwischen den KITT-Verantwortlichen und der damaligen Finanzdirektorin Bezug und kritisierte den mangelhaften Informationsfluss zwischen KITT und Regierungsrat. Der Umstand, dass dem Regierungsrat und dem KITT die Finanzdirektion und die Generalsekretärenkonferenz zwischengeschaltet waren, habe erschwerend gewirkt.[203]

Reaktion auf den Bericht der Finanzkontrolle

Gemäss der ehemaligen Finanzdirektorin, Ursula Gut-Winterberger, haben die Mitglieder des Regierungsrates aufgrund anderer Verpflichtungen diesem ersten Bericht der Finanzkontrolle zur IT vielleicht nicht die nötige Priorität gegeben.[204] Anderen Re-

---

198 Bericht der Finanzkontrolle in Zusammenarbeit mit bprex group AG vom 30. August 2013: «Erkenntnisse zur IT-Situation des Kantons Zürich. Würdigung anhand der Resultate aus den IT-Kurzchecks unter Berücksichtigung der KITT-Aktivitäten», S. 29–30.

199 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 7.

200 Protokoll der Befragung von Ursula Gut-Winterberger vom 20. September 2024, S. 12–13, 21.

201 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 14.

202 Kantonales IT-Team (KITT), Bericht vom 15. Juli 2014. Umsetzungsbericht 2014 «Informatikstrategie Kanton Zürich (RRB Nr. 1955/2008): Stand der Umsetzung».

203 Bericht der Geschäftsprüfungskommission über die vertiefte Untersuchung zur IT in der kantonalen Verwaltung vom 13. Juli 2017 (KR-Nr. 2003/2017), S. 20.

204 Protokoll der Befragung von Ursula Gut-Winterberger vom 20. September 2024, S. 19.

gierungsmitgliedern war dieser Bericht in der Befragung gar nicht mehr präsent.[205] Auch der ehemalige Staatsschreiber, Beat Husi, gab gegenüber der PUK Datensicherheit zu Protokoll, dass die Empfehlungen der Finanzkontrolle «in der Tendenz eher zu wenig ernst genommen wurden».[206]

6.5.3 Feststellungen im Tätigkeitsbericht 2013 der Finanzkontrolle

Nach den Feststellungen im internen Bericht vom August 2013 wies die Finanzkontrolle in ihrem Tätigkeitsbericht 2013 darauf hin, dass die damalige IT-Organisation bei der Etablierung von Sicherheitsstandards an ihre Grenzen stosse, und wollte damit in der Politik, namentlich beim Regierungsrat, eine Verbesserung anstossen. Sie hielt Folgendes fest:

– «Die dezentrale Organisation der IT im Kanton Zürich führt dazu, dass übergreifende (Sicherheits-)Standards schwer zu verwirklichen sind und daher verschiedene Risiken bei Querschnittfunktionen bestehen, die weder in einem IKS [Internes Kontrollsystem] noch einem übergeordneten ganzheitlichen Risikomanagement berücksichtigt werden. Verantwortlich für das Management dieser Risiken ist das Kantonale IT-Team (KITT), wobei die Prioritäten und Vorgaben für das Risikomanagement sowie einen definierten IT-Grundschutz vom Regierungsrat beschlossen werden sollten.» [207]

6.6 Stand der Umsetzung der Informatiksicherheit im Jahr 2014

Fünf Jahre nach dem Erlass der Informatikstrategie im Dezember 2008 befassten sich das KITT-Gremium und die KITT-Geschäftsstelle in einem Strategieworkshop mit dem Stand der Umsetzung der Informatikstrategie und legten dazu im Juli 2014 einen Bericht vor.[208] Darin wurde auch über den Stand der Umsetzung der drei Elemente «Informationssicherheitsorganisation», «Informatiksicherheitsverordnung» sowie «Managementsystem für Informatiksicherheit (ISMS)» der Umsetzungseinheit «Informatiksicherheit» berichtet.

Weitere Verzögerung bei der Informatiksicherheitsorganisation

Im Juli 2014 war das Geschäft «Informatiksicherheitsorganisation» noch nicht abgeschlossen. Die Verortung des Informatik-Sicherheitsbeauftragten war weiterhin nicht geklärt. Im Rahmen der Generalsekretärenkonferenz vom 19. Mai 2014 brachte die Finanzkontrolle weitergehende Ansprüche zur Organisation der Informatiksicherheit ein. Aufgrund dieser Rückmeldung beschloss man, das Geschäft nochmals zu überarbeiten. Erst am 19. September 2014 konnte das KITT das Organisationskonzept, nach welchem das Competence Center IT-Sicherheit der Finanzdirektion zugewiesen wurde, genehmigen.[209]

---

[205] Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024; S. 11; Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 15.

[206] Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 16.

[207] Bericht der Finanzkontrolle vom 8. Mai 2014 über ihre Tätigkeiten 2013, S. 16.

[208] Kantonales IT-Team (KITT), Bericht vom 15. Juli 2014. Umsetzungsbericht 2014 «Informatikstrategie Kanton Zürich (RRB Nr. 1955/2008): Stand der Umsetzung», S. 12–13.

[209] Die Genehmigung durch den Regierungsrat erfolgte schliesslich im Februar 2015: RRB Nr. 129/2015 vom 11. Februar 2015, Organisationskonzept für die Informatiksicherheit in der kantonalen Verwaltung (Genehmigung).

Totalrevision der Informatiksicherheitsverordnung (ISV)

Der Regierungsrat verabschiedete, nach Vorarbeiten des KITT, am 26. Februar 2014 das Konzept der Finanzdirektion für die Totalrevision der Informatiksicherheitsverordnung, welche namentlich die Organisation der Informatiksicherheit festlegen sollte.[210] Die Festlegung auf Verordnungsstufe wurde jedoch nie realisiert, da die ISV nicht in dieser Form umgesetzt wurde (siehe dazu Kapitel 10.2).

Managementsystem für Informatiksicherheit (ISMS)

Das ISMS lag im Juli 2014 noch nicht vor. Es existierte zwar ein Entwurf des KITT, aber eine definitive Ausarbeitung des Regelwerks wäre erst nach der Festlegung der neuen ISV möglich gewesen.

6.7 Einschätzung der Geschäftsprüfungskommission (GPK) im Rückblick

Die GPK hat sich in den Jahren 2015–2017 eingehend mit der aus ihrer Sicht über weite Strecken gescheiterten Umsetzung der Informatikstrategie 2008 befasst und dazu einen Bericht vorgelegt. Mögliche Gründe für dieses Scheitern waren aus ihrer Sicht das Führungsdefizit auf Ebene des Regierungsrates und dessen mangelndes Bewusstsein für die strategische Bedeutung der IT-Führung, die Kultur des direktionalen statt gesamtkantonalen Denkens sowie das Organisationsmodell, das den direktionsübergreifenden Organen und Interessen eine ungenügende Stellung gab und in dem insbesondere Weisungs- und Überwachungskompetenzen gegenüber den dezentralen Einheiten fehlten.[211] Zu den verschiedenen Problemfeldern äusserte sich die GPK in ihrem Bericht konkret wie folgt:

Keine ausreichende Führung durch den Regierungsrat

- *«An der Umsetzung der von ihm selbst beschlossenen IT-Strategie, seines zentralen Steuerungsinstruments für diesen Bereich, hat er kein grosses Interesse erkennen lassen. Dies ist umso schwerer nachvollziehbar, als die Finanzkontrolle und die Geschäftsprüfungskommission spätestens ab März 2013 kommunizierten, dass für eine koordinierte Verwaltungstätigkeit und eine erfolgreiche Umsetzung der kantonalen Informatikstrategie eine Reform der Organisationsstrukturen nötig sei.»*
- *«Erstens hat teilweise das Bewusstsein gefehlt, dass eine wirksame Zusammenarbeit im IT-Bereich primär eine Frage von Strategie und Organisation ist, die für den Kanton wichtig ist und ein klares Bekenntnis der politischen Führungsverantwortlichen erfordert.»*
- *«Zweitens hat teilweise – sei es bewusst oder unbewusst – wohl die Perspektive als Direktionsvorstehende gegenüber jener als Regierungsmitglied überwogen.»*
- *«Drittens herrschte offenbar lange die Haltung vor, dass kein Handlungsbedarf bestehe, solange die IT im operativen Tagesgeschäft passabel funktioniere.»* [212]

Mangelhafte Verknüpfung von politischer und strategischer Führungsebene

- *«Dem Regierungsrat fehlte bis mindestens 2014 ein Überblick über den Umsetzungsstand der 2008 von ihm erlassenen und eigentlich bis 2013 umzusetzenden Strategie. Er verpasste es aber, beim KITT die entsprechenden Informationen einzufordern – obwohl eigentlich ein periodisches Reporting vorgesehen war.»*

---

[210] RRB Nr. 231/2014 vom 26. Februar 2014, Informatiksicherheitsverordnung, Totalrevision, Konzept.

[211] Bericht der Geschäftsprüfungskommission über die vertiefte Untersuchung zur IT in der kantonalen Verwaltung vom 13. Juli 2017 (KR-Nr. 203/2017), S. 25.

[212] Bericht der Geschäftsprüfungskommission über die vertiefte Untersuchung zur IT in der kantonalen Verwaltung vom 13. Juli 2017 (KR-Nr. 203/2017), S. 18.

Vorherrschen direktionaler Interessen sogar in den überdirektionalen Gremien

– *«Die einzelnen Direktionen und IT-Abteilungen haben naturgemäss nicht immer die gleichen Perspektiven und Interessen, wie sie ein übergeordneter Akteur im Interesse des Gesamtkantons hätte. Dies ist nachvollziehbar und an sich nicht problematisch. Problematisch ist jedoch, dass die bestehende Organisationsstruktur keine starken Akteure schafft, die das IT-Management primär aus einer gesamtkantonalen Perspektive betrachten, die gesamtkantonalen Interessen vertreten und auf einen ausgewogenen Interessenausgleich hinwirken könnten.»*

Kein direktionsübergreifendes Organ mit ausreichenden Kompetenzen

– *«Die Geschäftsprüfungskommission empfiehlt schon seit Längerem die Übertragung eines Weisungsrechts in IT-Fragen an ein übergeordnetes Organ (siehe etwa KR-Nr. 86/2015), bisher aber vergeblich. Ein Weisungsrecht fehlt nicht nur dem KITT als Organ, sondern weitgehend auch den einzelnen KITT-Mitgliedern.»*

Ungenügendes direktionsübergreifendes IT-Controlling und Portfoliomanagement

– *«Es ist heute gut möglich, dass verschiedene Direktionen parallel ähnliche Lösungen entwickeln, ohne voneinander zu erfahren und ohne dass irgendjemand ihre direktionsübergreifende Relevanz erkennen kann.»*[213]

6.8 Würdigung durch die PUK

Die Eindrücke, welche die PUK Datensicherheit im Rahmen ihrer Befragungen und Einvernahmen über diese Zeit gewonnen hat, decken sich mit den Feststellungen der GPK. Das damals fehlende Bewusstsein oder das mangelnde Interesse des gesamten Regierungsrates sowie die grundsätzliche Zufriedenheit der Regierungsmitglieder mit der direktional organisierten Informatik und nicht zuletzt die vorherrschend direktionale Sicht zeigten sich auch in den Befragungen der PUK Datensicherheit.

Hindernde Wirkung der KITT-Organisation

Im Weiteren stellt die PUK Datensicherheit fest, dass dem KITT-Konstrukt sowohl die strukturellen Voraussetzungen als auch die politische Unterstützung und der Wille fehlten, um eine direktionsübergreifende Informatik langfristig und wirksam zu etablieren. Vor diesem Hintergrund ist die spätere vollständige Ablösung des KITT 2018 sogar nachvollziehbar. Die grundsätzliche Schwierigkeit, im Rahmen der KITT-Organisation direktionsübergreifende Prozesse und Standards zu schaffen, hatte auch Auswirkungen auf die Umsetzung der Informationssicherheit. Obwohl die Finanzkontrolle und auch die GPK darauf hingewiesen hatten, dass für die Umsetzung der kantonalen Informatikstrategie eine Reform der bestehenden Organisationsstrukturen nötig wäre, blieb das «Verhinderungskonstrukt» der KITT-Organisation lange unverändert.

Schleppende Umsetzung der Informatiksicherheit

Die PUK Datensicherheit anerkennt, dass die vom KITT geschaffenen strategischen Grundlagen bereits früh den Weg aufzeigten. Die kantonale Informatikstrategie erwähnte den Bedarf für ein Kompetenzzentrum Informatiksicherheit und den Aufbau eines ISMS. Mit dem Organisationskonzept konkretisierte das KITT dann ab 2011 die Umsetzung der Informationssicherheit mit der beabsichtigten Schaffung einer kantonalen Informatiksicherheitsorganisation in Form eines Kompetenzzentrums Informatiksicherheit, dem Aufbau eines ISMS und der Revision der ISV. Die Umsetzung der

[213] Bericht der Geschäftsprüfungskommission über die vertiefte Untersuchung zur IT in der kantonalen Verwaltung vom 13. Juli 2017 (KR-Nr. 203/2017), S. 20–23.

Informationssicherheit scheiterte jedoch – wie die Umsetzung der gesamten Informatikstrategie – an diversen Faktoren, insbesondere der mangelnden Unterstützung durch den Gesamtregierungsrat.

Die PUK Datensicherheit hält in aller Deutlichkeit fest, dass es dem Gesamtregierungsrat trotz mehrfacher, klarer Kritik der Finanzkontrolle und der GPK am Bewusstsein für die Bedeutung der Informationssicherheit fehlte, obwohl die Regierungsmitglieder in den Befragungen der PUK Datensicherheit jeweils von hoher «Awareness» sprachen. Die mangelhafte Verknüpfung der politischen mit der strategischen Ebene, welche die GPK kritisiert hatte, zeigte sich auch beim Thema Informationssicherheit. Der damalige Regierungsrat hatte auch hier die Umsetzung der Informatikstrategie zu wenig begleitet. Sechs Jahre nach der Verabschiedung der Informatikstrategie waren alle drei Projekte zur Informationssicherheit – Informatiksicherheitsorganisation (Kompetenzzentrum Informatiksicherheit), Revision der ISV und Aufbau eines ISMS – noch lange nicht abgeschlossen.

Die fehlende Führung durch den Regierungsrat lässt sich beim Teilprojekt Informatiksicherheitsorganisation aufzeigen. Die ausbleibende Einigung über die Verortung des Kompetenzzentrums verzögerte die Umsetzung und führte dazu, dass dem Regierungsrat kein Antrag vorgelegt wurde. Inwieweit sich der Regierungsrat damals mit dieser Angelegenheit befasste, lässt sich heute nicht mehr sagen. Auf jeden Fall war die Thematik noch im Juli 2014, fast ein Jahr nach der diesbezüglichen Feststellung der Finanzkontrolle (August 2013), nicht gelöst.

Die Verzögerung bei einem wesentlichen Element der Informationssicherheit ist insofern erstaunlich, als die Notwendigkeit des Aufbaus einer Sicherheitsorganisation bereits länger bekannt war. Der Datenschutzbeauftragte, Bruno Baeriswyl, hatte bereits 2001 eine Sicherheitsorganisation gefordert und 2003 verlangt, dass die sicherheitsspezifischen Rollen innerhalb der Verwaltung festgelegt werden, da sonst die Sicherheitsmassnahmen aus der ISV kaum realisiert werden könnten. In seinem Bericht zur Sicherheitsinitiative zuhanden des Regierungsrates empfahl er 2004 explizit, die Stelle eines kantonalen Chief Information Security Officer (CISO) zu schaffen. Auch die Finanzkontrolle hatte in ihrem Bericht vom 30. August 2013 zur IT-Situation des Kantons Zürich darauf hingewiesen, dass weiterhin kein IT-Sicherheitsmanagement und kein mit entsprechenden Kompetenzen ausgestatteter Informatik-Sicherheitsbeauftragter existiere.

Weil das Kompetenzzentrum fehlte, konnte auch der Aufbau des ISMS nicht weiterverfolgt werden. Das dritte Teilprojekt, die Totalrevision der ISV, wurde zwar früher angestossen, liess sich aber in den folgenden Jahren auch nicht in der ursprünglichen Form realisieren. An die Stelle der ISV trat später die Verordnung über die Informationsverwaltung und -sicherheit (IVSV) (siehe dazu Kapitel 10.2).

Dass der Regierungsrat als Gremium die Umsetzung der Informatiksicherheit nur ungenügend beachtete, zeigt sich für die PUK Datensicherheit besonders darin, dass die Finanzkontrolle 2013 klar und deutlich empfahl, der Sicherheit im IT-Bereich eine erhöhte Aufmerksamkeit zu schenken. Für die PUK Datensicherheit ist nicht nachvollziehbar, weshalb der Regierungsrat bis 2015 keine konkreten Massnahmen ergriff. Damit kam er seiner Verantwortung nicht nach.

7. Informationssicherheit in der Direktion der Justiz und des Innern (JI) mit Fokus auf die Beschaffungs- und Entsorgungsprozesse von 2000–2014

IT-Organisation in der Direktion der Justiz und des Innern (JI)

In den 1990er-Jahren bestanden noch zwei separate Direktionen für die Justiz und für das Innere. Deren Informatikabteilungen waren getrennt, unterschiedlich organisiert und nutzten nicht die gleichen Systeme. Die IT der Direktion der Justiz war bereits zentral aufgestellt, während die IT der Direktion des Innern dezentral funktionierte. Das Sicherheitsbewusstsein war, auch aufgrund der unterschiedlichen Aufgaben, nicht in beiden Direktionen gleich ausgeprägt. Mit der Zusammenführung der beiden Direktionen im Rahmen des Projektes «Direktion 99» galt es, diese Kulturen im Jahr 1998 zu vereinigen und auch das Generalsekretariat neu zu organisieren.

Die neugeschaffene Hauptabteilung Logistik, Finanzen und Controlling (LFC) umfasste mit Ausnahme des HR-Bereichs alle nicht-juristischen Aufgaben des Generalsekretariats.[214] Renato Widmer, welcher ab 1988 die Informatik der Direktion der Justiz aufgebaut und die wachsende Informatikgruppe geführt hatte, leitete ab 1999 die Hauptabteilung LFC und fungierte für die Direktion als Mitglied der Kommission für strategische Informatikführung (KOSIF) respektive Mitglied des Kantonalen IT-Teams (KITT).[215] Parallel dazu wurde die Stelle des Abteilungsleiters der JI-Informatik geschaffen, die ab 1998 der Vorgänger von Fredi Steiner innehatte.[216]

Von Mai 2001 bis Ende 2014 war Fredi Steiner in der Funktion des Abteilungsleiters der JI-Informatik tätig und Renato Widmer, dem Leiter LFC, unterstellt. Die JI-Informatik war zwar im Bezirksgebäude Zürich, der Leiter LFC aber beim Generalsekretariat im Kaspar-Escher-Haus untergebracht. Nach dem Abgang von Renato Widmer übernahm Fredi Steiner dessen Rolle in der IT-Leitung. Die Bereiche Finanzen, Controlling und Logistik übergab der Generalsekretär an den Direktionscontroller. 2016 wurde schliesslich im Rahmen einer Reorganisation die JI-Informatik als eigene Hauptabteilung geschaffen.[217]

Gemäss dem Organigramm vom März 2014 bestand die JI-Informatik aus den Bereichen Systeme und Rechenzentren (Data-Center), Support & Engineering (mit dem Help- respektive Servicedesk), Applikationen, IT-Spezialisten sowie externen Mitarbeitenden. In die letzte Kategorie fiel auch der namentlich genannte André Gisler, der bei der Entsorgung von Datenträgern der JI mitwirkte. In dieser Funktion spielte er im Zusammenhang mit dem Datensicherheitsvorfall eine wesentliche Rolle.[218]

7.1 Rechtliche Rahmenbedingungen und interne Regelwerke

7.1.1 Regelungen vor 2010

Der damalige Direktionsvorsteher der JI, Markus Notter, erliess am 4. Januar 1999, gestützt auf die Informatiksicherheitsverordnung (ISV), eine Verfügung zu Massnahmen zum Schutz von Daten innerhalb und ausserhalb der Amtsräume mit Vorgaben zum

[214] Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 6–7, 15.

[215] Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 6–7.

[216] Staatsanwaltschaft III, Delegierte Einvernahme des Leiters der JI-Informatik (1996–2000) vom 19. Juli 2023.

[217] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 6; Stellungnahme von Fredi Steiner vom 5. November 2025.

[218] Direktion der Justiz und des Innern, Logistik, Finanzen und Controlling, Abteilung Informatik, Präsentation «Vorstellung IT JI» vom 31. Januar 2012. Version vom 24. April 2014 mit Organigramm vom 10. März 2014.

Zugangs- und Zugriffsschutz, zum Umgang mit der persönlichen Chipkarte und zur Verwendung und Speicherung von Daten. Überdies erinnerte die Verfügung die Vorgesetzten an ihre Pflicht zur periodischen Überprüfung der Einhaltung der ISV und Schulung der Mitarbeitenden. Die Mitarbeitenden hatten diese Nutzungsvorschriften zu unterzeichnen. 2003 wurden die Vorschriften um die Bestimmung zur Benutzung von Internet und E-Mail ergänzt. Der PUK Datensicherheit liegt ein solches Formular aus dem Jahr 2010 vor.[219]

7.1.2 Informatikstrategie vom 14. Februar 2011

Als erste Direktion überhaupt erliess die JI am 14. Februar 2011 eine eigene Informatikstrategie, wie sie gemäss der geltenden kantonalen Informatikstrategie 2008 gefordert war.[220] Die Informatikstrategie der JI wies grundsätzlich alle Ämter, Bereiche und Anstalten in der Direktion der Stufe 3 der ISV zu, also der Stufe mit hohem Schutzbedarf. Sie definierte die Rollen und Aufgaben in Bezug auf die direktionsweit zentralisierte Informatik. Dabei unterschied sie u. a. zwischen der Verantwortung des Direktionsvorstehers, der leitenden Verantwortung des Leiters der Hauptabteilung LFC sowie der operativen Verantwortung der Informatik (siehe Tabelle 13).

Tabelle 13 Zuständigkeiten gemäss Informatikstrategie der JI vom 14. Februar 2011

Rolle	Verantwortung	Ausgewählte Aufgaben
Direktionsvorsteher	Oberste Verantwortung für die Ausgestaltung der IT-JI	– Festlegung/Genehmigung Strategie, Leitbild, Betriebskonzept, Budget, Projekte
Leiter Hauptabteilung Logistik, Finanzen und Controlling (LFC)	Leitung und Lenkung aller IT-Aktivitäten	– Strategien, Analysen, Konzeptionen – Auswahl und Entwicklung von Hard- und Software – Planung, Budget, Mittelverwendung – Verantwortlich für Führung, Aufbau und Organisation der IT-JI sowie für interne und externe Leistungs-Verbringung [sic]
Informatikabteilung JI	Zentraler Dienstleister für JI	– Sicherstellung operativer Betrieb – Bereitstellung, Inventarisierung und Betrieb der gesamten IT-Infrastruktur

Die Informatikstrategie der JI enthielt auch einen Abschnitt zur Sicherheit. Dieser hielt fest, dass der Einsatz der Informatiksysteme die eidgenössischen und kantonalen Vorschriften betreffend Datenschutz und Datensicherheit erfüllen müsse und die Direktion für die Handhabung ihrer Systeme notwendige, ergänzende Vorschriften zu erlassen habe. Die Sicherheitsanforderungen und -vorschriften hatten für alle betroffenen Systemkategorien, Personen und Sachmittel Gültigkeit.

Die Direktionsstrategie hielt zudem fest, dass die Informatikabteilung die Informatikdienstleistungen allein erbringt, aber externe Partner unter der Kontrolle der JI-Informatik ergänzend bestimmte Dienstleistungen ausführen können. Für diese Partner waren der Leiter LFC und die JI-Informatik Verhandlungs- und Arbeitspartner.

---

[219] Direktion der Justiz und des Innern, Erklärung zur Informatiksicherheitsverordnung (ISV) vom 17. Dezember 1997 und zur Verordnung über die Nutzung von Internet und E-Mail vom 17. September 2003, Stand Juni 2010.

[220] Direktion der Justiz und des Innern, Generalsekretariat, Logistik, Finanzen und Controlling, Informatik-Strategie und Reglement der Direktion der Justiz und des Innern (JI) des Kantons Zürich. Erlassen am 14. Februar 2011.

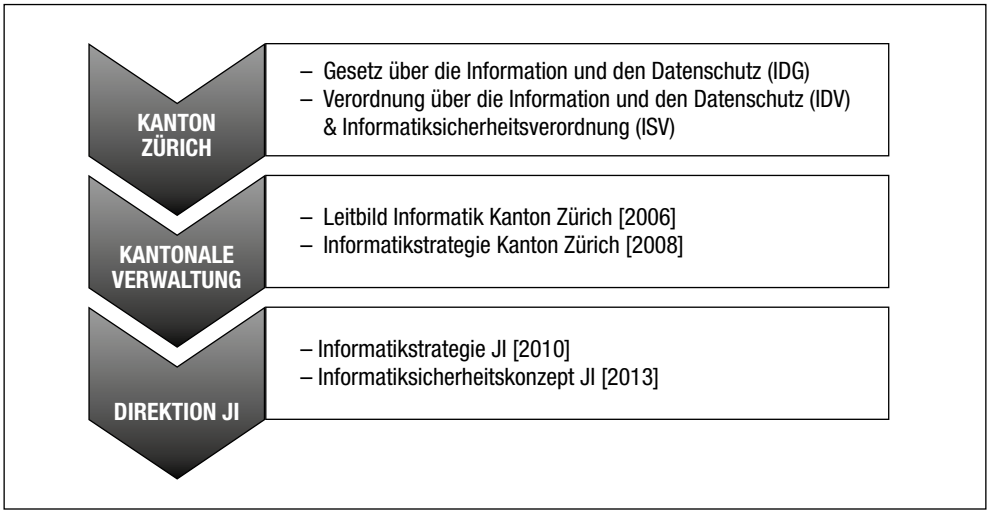
7.1.3 Qualitätsmanagement-System der JI-Informatik

Zur konkreten Umsetzung der direktionalen Informatikstrategie hatte die JI-Informatik ein Qualitätsmanagement-System nach ISO 9001 zu führen.[221] Die erste Zertifizierung erfolgte im Jahr 2009. Die damals erarbeiteten Dokumente hatten mit kleineren Anpassungen bezüglich Layouts und Benennungen noch bis ins Jahr 2022 Gültigkeit. Die Dokumente zu «Qualitätsmanagement», «Beschaffungswesen» und «Leitbild und Strategie» enthielten jedoch keine spezifischen Ausführungen zur Entsorgung oder Vernichtung von Datenträgern. Auch wenn die Informationssicherheit allgemein einen hohen Stellenwert hatte, räumten sowohl der ehemalige Leiter der Hauptabteilung LFC, Renato Widmer, als auch der damalige Leiter der JI-Informatik, Fredi Steiner, rückblickend ein, dass ihnen der Aspekt der Datenträgerentsorgung damals wohl zu wenig bewusst gewesen sei.[222]

7.1.4 Informatiksicherheitskonzept vom 4. November 2013[223]

Mit ihrem Informatiksicherheitskonzept berücksichtigte die JI die bestehenden Informatiksicherheitsanforderungen, formulierte eigene Informatiksicherheitsziele und schaffte die Basis für konkrete Massnahmen. Hier waren alle Festlegungen zur Informatiksicherheit der JI zusammengefasst. Das Konzept umfasste alle Mitarbeitenden und Räumlichkeiten der Direktion, war aber auf den Bereich der Informatiksicherheit beschränkt. Das Dokument bildete damit den weiteren logischen Schritt in der Kaskade von den kantonalen Vorgaben bis zur konkreten Umsetzung in den Direktionen (siehe Abbildung 4).

Abbildung 4 Kaskade zu den Grundlagen der Informationssicherheit



[221] Direktion der Justiz und des Innern, Generalsekretariat, Logistik, Finanzen und Controlling, Informatik-Strategie und Reglement der Direktion der Justiz und des Innern (JI) des Kantons Zürich. Erlassen am 14. Februar 2011, S. 4–7.

[222] Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 11; Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 11.

[223] Direktion der Justiz und des Innern, Generalsekretariat, Informatiksicherheitskonzept vom 4. November 2013. In Kraft getreten am 1. Januar 2014.

Die Erarbeitung des ersten Informatiksicherheitskonzepts der JI wurde durch den Leiter LFC, Renato Widmer, in Auftrag gegeben.[224] Das rund 70-seitige Dokument betonte, ausgehend von den Prinzipien der Informatiksicherheit, die Bedeutung der Informatiksicherheit für die Direktion und klärte die Verantwortlichkeiten zwischen Direktionsvorstand, Leitung LFC, JI-Informatik und Mitarbeitenden in den Amtsstellen. Der Leiter LFC hatte die Aufsicht zu führen und die JI-Informatik trug die Verantwortung für die Infrastruktur (Geräte, Netzwerke, Basissoftware). Alle Mitarbeitenden waren für den verantwortungsvollen Umgang mit Daten zuständig und hatten die diesbezüglichen Massnahmen und Weisungen zu beachten.

Vorgaben zur sicheren Entsorgung oder Wiederverwendung von Geräten

Gemäss dem Informatiksicherheitskonzept war die JI-Informatik für das Verfahren zum sicheren Löschen von Informationen, die sich allenfalls noch auf zurückgegebenen Geräten befanden, verantwortlich.[225] Auch die nicht mehr benötigten Datenträger mussten gemäss Informatiksicherheitskonzept durch Zerstörung unlesbar gemacht werden, wobei für die zwingenden Entsorgungsvorschriften auf die QM-Vorgaben verwiesen wurde.[226] Gemäss dem QM-Dokument «Auftragsabwicklung Standard-Dienstleistungen» fielen das Einrichten eines Standard-Arbeitsplatzes sowie das Installieren von zusätzlicher Hard- und Software in die Kategorie der Standard-Dienstleistungen. Die Erbringung einer solchen Dienstleistung war beim Leiter LFC zu beantragen, der dann die Freigabe erteilte, den Auftrag zur Abwicklung an den Helpdesk weitergab und gleichzeitig den Leiter der JI-Informatik informierte. Die Aufgabe als Helpdesk-Mitarbeiterin übernahm während vieler Jahre die inzwischen verstorbene Erika W. Die konkreten Einsätze sollten dann vom Helpdesk geplant und die Leistungen von Mitarbeitenden der JI-Informatik erbracht werden. Die Rücknahme einzelner PC-Arbeitsplätze oder Komponenten davon konnte selbständig über den Helpdesk ausgelöst werden. Nach der Leistungserbringung war dem Helpdesk eine unterschriebene Auslieferungsbestätigung abzugeben und der Leiter LFC zu informieren.[227] Im Rahmen von internen Audits hatte die zuständige Mitarbeiterin des Helpdesks jeweils den Nachweis über die unterschriebenen Auslieferungsbestätigungen zu erbringen (siehe Kapitel 8.3.2).

Umzüge von PCs oder Rollouts waren gemäss dem QM-Dokument hierzu[228] planbare Aktionen, die durch Antrag beim Leiter LFC ausgelöst werden konnten. Die Grobplanung zu den eingesetzten Mitarbeitenden wurde jedoch zwischen der Administration, was wohl dem Helpdesk entsprach, und der Gruppenleitung erstellt. Für grössere Rollouts konnten externe Mitarbeitende beigezogen werden, wozu aber vorgängig eine Absprache mit dem Leiter der Informatikabteilung und ein Antrag beim Leiter LFC zu erfolgen hatten.

---

[224] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 12.

[225] Abschnitt «9.2.6. Sichere Entsorgung oder Wiederverwendung von Geräten» im Informatiksicherheitskonzept vom 4. November 2013.

[226] Abschnitt «10.7.2. Entsorgung von Datenträgern» im Informatiksicherheitskonzept der JI vom 4. November 2013.

[227] Direktion der Justiz und des Innern, Generalsekretariat, Informatik, Auftragsabwicklung Standard-Dienstleistungen Service Deployment & Delivery vom 8. April 2009, Version 2.0 vom 28. Oktober 2009, S. 2–3.

[228] Direktion der Justiz und des Innern, Generalsekretariat, Informatik, Personal-Management, Einsatz- und Verfügbarkeitsplanung vom 8. April 2009, Version 2.0 vom 28. Oktober 2009, S. 2.

Vorgaben zur Sicherheitsüberprüfung

Mitarbeitende hatten nach dem Informatiksicherheitskonzept der JI eine Sicherheitsüberprüfung gemäss Weisung vom 1. April 2011 zu durchlaufen. Neben einem aktuellen Strafregisterauszug sowie der Meldung allfälliger gelöschter oder eingestellter Strafverfahren mussten je ein Auszug aus dem Betreibungs- und dem Handelsregister eingefordert und Referenzauskünfte eingeholt werden. Der PUK Datensicherheit liegt ein Formular des Personaldienstes der Direktion zur Einwilligung in eine Sicherheitsüberprüfung, datiert von April 2011, vor. Diese Formulare fanden jeweils Eingang in die Personalakte.[229]

Vorgaben im Umgang mit externen Leistungserbringern

Die Verpflichtung zur Sicherheitsüberprüfung galt auch für Dritte, bevor sie elektronischen Zugang zu Systemen oder physischen Zugang zu Computern, Computerräumen oder ähnlichen Einrichtungen erhielten. Schliesslich waren Externe und Hilfspersonen verpflichtet, eine Vertraulichkeitserklärung zu unterschreiben. Mandatsverträge mussten immer die Allgemeinen Geschäftsbedingungen Sicherheit des Kantons Zürich (AGB Sicherheit)[230] beinhalten. Diese AGB verlangen vom kantonalen Leistungsbezüger explizit die Erstellung von Vorgaben und vom Leistungserbringer die Dokumentation der Methoden und Prozesse, die Abgabe eines Datensicherheitskonzepts sowie die Verpflichtung zur Einhaltung der Sicherheitsbestimmungen durch das eigene Personal.

Das strategische QM-Dokument zur Risikoanalyse der Systeme und Applikationen sah vor, dass alle Informatik-Dienste, die von externen Dienstleistern erbracht wurden, durch Verträge abgesichert werden mussten, wobei Datenschutzmassnahmen Teil dieser Verträge sein mussten. Man erkannte also allgemein das Risiko durch unvorsichtiges oder böswilliges Verhalten von Mitarbeitenden oder Dritten. Das Risiko nicht sachgemässer Entsorgungen wurde aber nicht explizit genannt.[231]

Am 18. November 2013 erliess der damalige Direktionsvorsteher der JI, Martin Graf, eine Weisung betreffend Zugriff durch externe Mitarbeitende auf die Informatikinfrastruktur. Dabei waren die Auftraggebenden verpflichtet, bei den Mandatierten eine Vertraulichkeitserklärung und die Zustimmung zu den Richtlinien der JI-Informatik einzuholen. Der Zugriff durch externe Personen auf die Informatik-Ressourcen war analog zu den Eintrittsprozessen für interne Mitarbeitende vorzunehmen und die Berechtigungen per vorgängig definiertem Auftragsende sofort wieder zu entziehen. Weiter war der Zugriff auf den benötigten Umfang zu begrenzen und die Umsetzung der Arbeiten durch die Auftraggebenden zu kontrollieren. Ausdrücklich waren mit der Weisung auch die laufenden Mandatsverhältnisse erfasst.[232]

---

[229] Direktion der Justiz und des Innern, Generalsekretariat, Personaldienst, Formular «Einwilligung zur Sicherheitsüberprüfung», Version 1.0 vom April 2011.

[230] Kanton Zürich, Allgemeine Geschäftsbedingungen über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit bei der Erbringung von Informatikdienstleistungen «AGB Sicherheit» vom September 2001.

[231] Direktion der Justiz und des Innern, Generalsekretariat, Informatik, Leitbild und Strategie Risikoanalyse Systeme / Applikationen vom 15. Dezember 2008. S. 5.

[232] Direktion der Justiz und des Innern, Generalsekretariat, Logistik, Finanzen & Controlling, Weisung bezüglich Zugriffe zur Informatikinfrastruktur für Mandatierte (Externe Mitarbeitende) vom 18. November 2013. In Kraft ab 1. Januar 2014.

7.2 Technische Informationssicherheit und Bewusstsein

7.2.1 Verschlüsselungslösung der JI

Gemäss dem damaligen Direktionsvorsteher, Markus Notter, war man sich in der früheren Direktion der Justiz sehr bewusst, dass man besonders im Bereich der Strafverfolgung und des Strafvollzugs mit sensitiven Daten arbeitete, weshalb man auf sichere Programme setzte und die Möglichkeiten der Mitarbeitenden technisch beschränkte.[233]

Dieses starke Bewusstsein für die Datensicherheit reflektiert sich auch darin, dass die Direktion bereits 1996 Verschlüsselungslösungen einführte.[234] Die Sicherheitslösung sah für alle JI-Mitarbeitenden Chipkarten und eine zertifikatsbasierte 2-Faktoren-Authentifizierung (2FA) vor. Der Zugriff auf die Geräte war folglich nur mit der Chipkarte und dem dazugehörigen Passwort möglich. Weiter waren die Dateien auf den Geräten und Datenträgern lokal verschlüsselt. Die Mail-Zustellung erfolgte sicher und auch der Netzwerkverkehr lief via VPN (virtual private network) verschlüsselt ab. Das Arbeiten war zudem nur mit zugelassenen Geräten erlaubt.[235]

Aus den Einvernahmen durch die Staatsanwaltschaft III des langjährigen ICT-Security-Architekten der JI-Informatik geht hervor, dass die Verschlüsselung bei den Geräten speicherortbasiert erfolgte. So konnten Mitarbeitende erstmals lediglich jenen Bereich des Laufwerks sehen, auf dem sich ihre Benutzerdaten befanden. Alle anderen Bereiche waren mit dem JI-Schlüssel geschützt und konnten ohne Chipkarte nicht eingesehen werden. Temporäre Verzeichnisse sowie das Downloadverzeichnis blieben aber unverschlüsselt. Die Verifizierung des Schlüssels erfolgte über die User-ID, wobei die Anmeldung immer über die Chipkarte erfolgte.[236]

Die JI leistete auch im Bereich der kantonalen Informationssicherheit ihren Beitrag. Das in der JI aufgebaute Service-Center PKI (Public Key Infrastructure), welches die Chipkarten herausgab, erbrachte diese Dienstleistung später auch für die Sicherheitsdirektion.[237] Im Jahr 2012 waren für die JI 2100 und für die Sicherheitsdirektion 4000 Chipkarten im Einsatz.[238] Daneben war ab 2008 das kantonale Service Center «Messaging-Services» bei der JI-Informatik angesiedelt, die somit das kantonale System für die Datenbanken und den E-Mail-Verkehr betrieb.[239]

Der ehemalige Datenschutzbeauftragte, Bruno Baeriswyl, äusserte sich in seinem Tätigkeitsbericht 1995 positiv zum Verschlüsselungsprojekt, welches dem Stand der Technik entsprach, sich mit verhältnismässigem Aufwand umsetzen liess und die Anforderungen des Datenschutzgesetzes erfüllte.[240] Der damals zuständige Regierungsrat, Markus Notter, liess die IT-Sicherheitsarchitektur 2003 extern überprüfen, und das diesbezügliche Gutachten kam zum Schluss, dass die gewählte Lösung über dem «State of the Art» in vergleichbaren, sicherheitskritischen Umgebungen von Verwal-

---

233 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 7.

234 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 8.

235 Direktion der Justiz und des Innern, Technologieentwicklung JI-Client: Timeline 1996–2016; Direktion der Justiz und des Innern, Verschlüsselungslösung der JI, 5. Dezember 2022.

236 Staatsanwaltschaft III, Dritte delegierte Einvernahme des ICT-Security-Architekten vom 24. Juli 2023, S. 4–8.

237 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 8.

238 Direktion der Justiz und des Innern, Logistik, Finanzen & Controlling, Abteilung Informatik, Präsentation Vorstellung IT-JI vom 3. Januar 2012.

239 Bericht der Geschäftsprüfungskommission über ihre Tätigkeit vom April 2012 bis März 2013, Direktion der Justiz und des Innern: Themenschwerpunkt «IT in der Direktion der Justiz und des Innern» (KR-Nr. 81/2013), S. 8–11.

240 Tätigkeitsbericht des Datenschutzbeauftragten 1995, S. 28.

tungen liege. In Bezug auf die lokale Verschlüsselung erinnerte es daran, dass Mitarbeiter dafür aber alle sensitiven Daten in den dafür vorgesehenen Bereichen speichern müssten.[241]

In ihrem Kurzcheck zur Informatik in der JI stellte die Finanzkontrolle 2012 fest, dass die konsequente Ausrichtung der Informatik an den hohen Sicherheitsanforderungen zu Einschränkungen bei der Prozessgestaltung führe, weshalb die Geschäftsplanung sorgfältig mit den Sicherheitsanforderungen abzustimmen sei.[242] Auch die GPK stellte in ihrem Tätigkeitsbericht 2013 fest, dass die Informatiksicherheit in der JI ein grosses Gewicht habe, hielt ergänzend aber fest, dass trotz strenger Vorschriften die Einhaltung durch die Mitarbeitenden und die damit verbundene Kontrolle entscheidend sei.[243] Der erste Informatik-Sicherheitsbeauftragte (I-SiBe), Renzo Mühlebach, erhielt von der Lösung, die in der JI für die Datenverschlüsselung auf den lokalen Geräten genutzt wurde, ebenfalls einen positiven Eindruck. Die in der JI bereits realisierte Möglichkeit, Daten verschlüsselt auf Datenträgern wie USB-Sticks abzulegen, war gemäss seiner Aussage etwas, das auch für die übrige kantonale Verwaltung angestrebt werden sollte.[244]

Dieses technisch hohe Sicherheitslevel war ein Verdienst des Leiters LFC, Renato Widmer, der als Autor hinter den diesbezüglichen Vorgaben stand und sie gemäss verschiedener Aussagen auch gegenüber den Mitarbeitenden mit Nachdruck vertrat.[245] Dagegen war gemäss seiner Aussage die eigentlich alle zwei Jahre vorgesehene Überprüfung der Informatikstrategie der JI schwierig zu erreichen, da bei Anpassungen die Amtsleitungen mit ihren unterschiedlichen Bedürfnissen einbezogen werden mussten.[246]

Verschiedene durch die PUK Datensicherheit befragte Personen betonten, dass die sehr frühe Einführung der Verschlüsselung mit Chipkarte und PIN-Codes Pioniercharakter hatte und die Direktion hier federführend und fortschrittlich gewesen sei.[247] Auch der Leiter der JI-Informatik, Axel Mayer, der 2018 seine Stelle antrat, hatte noch den Eindruck, dass die JI, technisch gesehen, einen zeitgemässen Sicherheitsstandard aufwies.[248]

Das hohe Sicherheitsniveau und die Bedeutung, die man diesem Aspekt beimass, waren neben den damit verbundenen Einschränkungen auch für die späteren Direktionsvorsteherinnen und -vorsteher, Generalsekretärinnen und -sekretäre sowie Mitarbeitenden deutlich spürbar.[249] Beispielsweise waren USB-Sticks zentral zu beziehen. Für Präsentationen ausser Haus mussten die Daten auf den Datenträgern vorgängig entschlüsselt werden, damit sie überhaupt ausgelesen werden konnten.[250] Die Infor-

---

241 Bewertung der IT-Sicherheitsarchitektur der DJI 2003, Erstellt im Auftrag der Direktion der Justiz und des Innern des Kantons Zürich, Prof. Dr. Ueli Maurer, ETH Zürich.

242 Finanzkontrolle Kanton Zürich, IT-Kurzcheck in Zusammenarbeit mit bprex, Justiz und Inneres (JI), Protokollarische Zusammenfassung der Arbeitsschritte und Erkenntnisse, 23. Januar 2012, S. 6.

243 Bericht der Geschäftsprüfungskommission über ihre Tätigkeit vom April 2012 bis März 2013, Direktion der Justiz und des Innern: Themenschwerpunkt «IT in der Direktion der Justiz und des Innern».

244 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 8, 20.

245 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 12; Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 7–8; Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 9.

246 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 12.

247 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 8; Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 8; Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 8.

248 Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 6.

249 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 7; Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 7; Protokoll der Befragung von Benjamin Tommer vom 27. September 2024, S. 8; Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 9.

250 Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 8.

matikstrategie der JI hielt für diese Ausnahmefälle, bei denen die Speichermedien nicht mehr verschlüsselt waren, explizit fest, dass die Mitarbeitenden für die Sicherheit der unverschlüsselten Daten verantwortlich sind.[251]

Angesichts der Verschlüsselung der Datenträger machte man sich gemäss dem ehemaligen Leiter LFC, Renato Widmer, keine Sorgen, dass etwas nach aussen dringen könnte.[252] Auch der ehemalige Leiter der JI-Informatik, Fredi Steiner, hielt gegenüber der PUK Datensicherheit fest, dass er beim internen Bekanntwerden des Datensicherheitsvorfalls 2020 «aus allen Wolken gefallen» sei, da die JI-Informatik 2014 einen solchen Datenvorfall faktisch ausgeschlossen hatte und davon ausging, dass die Prozesse sicher seien.[253] Auch die heutige Direktionsvorsteherin, Jacqueline Fehr, vermutet, dass die zuständigen Personen nicht fahrlässig gehandelt hätten, sondern einfach überzeugt waren, dass die Geräte und Festplatten sicher seien. Diesen könne, da sie ja nicht geknackt werden können, ohnehin nichts passieren.[254]

Gemäss dem ehemaligen Leiter der JI-Informatik, Fredi Steiner, wurde auch die Verschlüsselung der Server in den Rechenzentren diskutiert. Angesichts der Schwierigkeiten, die verschlüsselte Serverdaten für die Archivierung mit sich bringen, verzichtete man aber darauf.[255] Die Abklärungen der Kantonspolizei Zürich haben allerdings gezeigt, dass in den Rechenzentren mehrere Speicherlaufwerke zu einem logischen Laufwerk kombiniert worden waren. Solche RAID-Systeme (Redundant Array of Independent Disks) liessen sich für einen Datenzugriff praktisch unmöglich wiederaufbauen, da hierzu alle zugehörigen Festplatten kombiniert und konfiguriert werden müssten.[256]

7.2.2 Ablauf der Löschprozesse in der Direktion

Umgang mit Client-Geräten

Bis ins Jahr 1998 stand die JI-Informatik unter der Leitung des späteren Leiters LFC, Renato Widmer. Damals wurden die noch tauglichen Geräte formatiert und verkauft und die nicht mehr tauglichen Geräte geschreddert.[257] Gemäss dem ehemaligen Leiter der JI-Informatik, Fredi Steiner, gewann nach der Jahrtausendwende das Wipen, also die mehrfache Überschreibung, an Bedeutung. Mit Hilfe einer Diskette und einem entsprechenden Programm konnten die Daten sauber von den Geräten gelöscht werden, sodass sie forensisch nicht wiederherstellbar waren.

Prozesse für die Server der Rechenzentren

Gemäss der Aussage des ehemaligen Leiters der JI-Informatik, Fredi Steiner, war die Entsorgung der Serverdisks in einem eigenen Prozess geregelt. Dieser sah vor, dass Serverdisks das Rechenzentrum nur in Behältern für die Zerstörung verlassen.[258] Gemäss dem diesbezüglichen QM-Dokument war der Zutritt zu den Rechenzentren nur mit Schlüssel, Badge und Sicherheitscode möglich.[259]

---

[251] Direktion der Justiz und des Innern, Generalsekretariat, Logistik, Finanzen und Controlling, Informatik-Strategie und Reglement der Direktion der Justiz und des Innern (JI) des Kantons Zürich. Erlassen am 14. Februar 2011, S. 16.

[252] Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 15.

[253] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 33.

[254] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 29.

[255] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 13.

[256] Kantonspolizei, Schlussbericht zum Ermittlungsverfahren Memory vom 19. Dezember 2024, S. 8–9.

[257] Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 15.

[258] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 21.

[259] Direktion der Justiz und des Innern, Generalsekretariat, Abteilung Informatik, Infrastructure Management, Betrieb der erweiterten RZ-Infrastruktur vom 24. Juni 2008.

Gemäss den Abklärungen der Staatsanwaltschaft kam es in den Jahren 2002–2005 zu einer Modernisierung der Serverinfrastruktur sowie mutmasslich in den Jahren 2007 und 2012 zu einem weiteren Austausch der Server.[260]

Gemäss dem Memo zur Entsorgung der Datenträger in der JI wird seit 2005 die Entsorgung der alten Hardware beim Ersatz der gesamten Serverinfrastruktur im Rahmen des Beschaffungsprozesses eingefordert. Einzelne defekte Serverdisks oder defekte Bänder werden laut Memo intern im Rechenzentrum gesammelt und dann unter Begleitung von Mitarbeitenden der JI-Informatik der mechanischen Vernichtung zugeführt.[261] Ein Dokument vom 16. April 2007 zeigt, dass der zuständige JI-Mitarbeiter bestätigt, Daten aus den Systemen formatiert, aus dem RAID ausgebaut und wieder neu aufgesetzt zu haben.[262] Weiter liegt der PUK Datensicherheit ein Zertifikat vom 30. April 2013 vor, das die Entsorgung von 220 Kilogramm Tapes bei einem zertifizierten Entsorgungsunternehmen bestätigt.[263] Vor diesem Hintergrund ist es für den ehemaligen Leiter der JI-Informatik, Fredi Steiner, nicht nachvollziehbar, wie Serverdisks in falsche Hände gelangt sein sollen.[264]

Die Finanzkontrolle hatte 2014 im Rahmen ihrer Prüfung Inventarnachweise zur Entsorgung von Servern verlangt (siehe dazu Kapitel 8.6). Die in diesem Zusammenhang beigebrachte Liste über die entsorgten und aktiven Geräte war aus ihrer Sicht in Ordnung. Die gelieferten Angaben waren glaubhaft, auch wenn der Umgang damit gemäss Prüfnotiz der Finanzkontrolle fahrlässig war.[265] Auch gemäss dem Leiter der JI-Informatik (2018–2020), Axel Mayer, gab es serverseitig einen klaren Lösch- und Vernichtungsprozess.[266]

Die Staatsanwaltschaft III kommt in ihrem Bericht hingegen zum Schluss, dass der externe Dienstleister, André Gisler, punktuell auch für die Entsorgung von Servern eingesetzt wurde. Diese waren als Elektroschrott in einem Palettenrahmen deponiert, den er abzuholen hatte. Dort befanden sich auch USB-Sticks, die Mitarbeitende weggeworfen hatten.[267] Die Entsorgung von Servern stand jedoch nicht im Vordergrund, und die Staatsanwaltschaft III konnte trotz gewisser Anhaltspunkte nicht abschliessend feststellen, ob die 39 sichergestellten Festplatten, die als Serverplatten verifiziert werden konnten, wirklich aus der JI stammten.[268]

7.2.3 Rechtsinformationssystem (RIS1 und RIS2)

In den 1990er-Jahren war als Teillösung für verschiedene Bereiche der späteren JI ein Rechtsinformationssystem in Anwendung.[269] Um das System weiter betreiben zu können, führte es die JI-Informatik mit internen Programmierern als Eigenentwicklung weiter und erweiterte es. Der erfolgreiche Aufbau des Rechtsinformationssystems (RIS1), einer Geschäftsverwaltungs-Applikation für den Justizbereich der Direktion,

---

260 Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 22.

261 Direktion der Justiz und des Innern, Generalsekretariat, Digital Solutions, Memo PdP Datenleck – Entsorgung Datenträger bei der JI vom 5. Dezember 2022.

262 Direktion der Justiz und des Innern, Logistik, Finanzen & Controlling, Abteilung Informatik, Memo vom 16. April 2007 «Bestätigung Datenlöschung».

263 Immark, Vernichtungs-Zertifikat vom 30. April 2013.

264 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 21.

265 Finanzkontrolle Kanton Zürich, Prüfnotiz 2014 Fragestellungen IT / Zusammenfassung der Erkenntnisse, 12. Dezember 2014, S. 15–16.

266 Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 15.

267 Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 18–19.

268 Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 24.

269 RRB Nr. 461/2010 vom 30. März 2010, Rechtsinformationssystem der Direktion der Justiz und des Innern (Technologischer Um- und Ausbau).

erfolgte unter der Führung des Leiters LFC, Renato Widmer.[270] Nach Aussage eines ehemaligen Mitglieds des RIS-Teams wurde RIS1 im Jahr 2000 erstmals in der Justizvollzugsanstalt Pöschwies eingeführt. Die Staatsanwaltschaften begannen etwa 2004 damit zu arbeiten.[271]

Bezüglich eines möglichen Zugriffs auf Daten aus dem RIS kam die Staatsanwaltschaft Zürich-Sihl nach ihren Abklärungen zum Schluss, dass aufgrund der Verschlüsselungslösung mit Chipkarten und Zugriffspassworten kein direkter Zugriff auf die verschlüsselten RIS-Daten der JI bestanden hatte.[272] Innerhalb des RIS waren die Berechtigungen und Einsichtsrechte abgestuft. Zugriffe konnten im Verlauf der Zeit auch nachvollzogen werden, was gemäss dem ehemaligen Generalsekretär, Christian Zünd, zum relativ hohen Sicherheitsstandard beigetragen hatte.[273] Beispielsweise konnte eine Abteilung der Staatsanwaltschaft nicht auf die Akten einer anderen Staatsanwaltschaft zugreifen. [274]

Gemäss der Einvernahme des ehemaligen Leiters des Data-Centers der JI-Informatik (2007–2018) gab es immer wieder Probleme mit der Leistung bzw. der Stabilität von RIS1. Aus diesem und weiteren Gründen hätten Mitarbeitende der Staatsanwaltschaften wissentlich Daten auf den Festplatten ihrer Geräte gespeichert.[275] Aus weiteren Protokollen der Staatsanwaltschaft III geht hervor, dass Einvernahmen lokal abgespeichert wurden.[276]

Im Jahr 2008 stiess der damalige Direktionsvorsteher, Markus Notter, die Gesamterneuerung des Rechtsinformationssystems RIS1 an, welches zu diesem Zeitpunkt die einzige Applikation war, die alle Untersuchungs- und Vollzugsabläufe sowie die Geschäftskontrollfunktionen für die wichtigsten Bereiche und Ämter elektronisch ermöglichte.[277] Die Modernisierung der Applikation von RIS1 zu RIS2 begann unter der übergeordneten Verantwortung des Leiters LFC, Renato Widmer. Nach Aussagen eines Mitglieds der damaligen Projektleitung und eines beteiligten Mitarbeiters gehörten etwa 20 Personen zum Entwicklungsteam.[278]

Mit RIS2 lassen sich für bestimmte Verfahrensschritte Vorlagen erstellen, welche die hinterlegten Informationen aus dem System berücksichtigen und einbauen. Für die Entwicklung dieser Funktion haben die RIS-Entwickler mit elektronischem und physischem Vorlagenmaterial gearbeitet. Gemäss der Aussage des früheren Leitenden Oberstaatsanwalts, Andreas Eckert, übergaben die Staatsanwaltschaften dem Entwicklungsteam dazu verschiedene Beispiele, wie etwa das Format für Haftlisten auszusehen hatte. Dabei gingen sie selbstverständlich von einer fachgerechten Entsorgung des übermittelten Vorlagenmaterials aus.[279]

---

[270] Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 18.

[271] Staatsanwaltschaft III, Delegierte Einvernahme des RIS-Teammitglieds vom 31. Januar 2024, Fragen 30–37.

[272] Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 2.

[273] Protokoll der Befragung von Christian Zünd vom 30. August 2024, S. 11.

[274] Staatsanwaltschaft III, Dritte delegierte Einvernahme des ICT-Security-Architekten vom 24. Juli 2023, Frage 27.

[275] Staatsanwaltschaft III, Delegierte Einvernahme des ehemaligen Leiters des Data-Centers vom 14. August 2023, Frage 116.

[276] Staatsanwaltschaft III, Dritte delegierte Einvernahme des ICT-Security-Architekten vom 24. Juli 2023, Frage 62 sowie Anhang 7 zum Schlussbericht der Administrativuntersuchung vom 30. März 2023. Protokoll des Interviews vom 14. Dezember 2020 mit dem ICT-Security-Architekten.

[277] RRB Nr. 461/2010 vom 30. März 2010, Rechtsinformationssystem der Direktion der Justiz und des Innern (Technologischer Um- und Ausbau).

[278] Staatsanwaltschaft III, Delegierte Einvernahme des Projektleiters der Digital Solutions vom 20. März 2024, Frage 35; Staatsanwaltschaft III, Delegierte Einvernahme des RIS-Teammitglieds vom 31. Januar 2024, Frage 44.

[279] Protokoll der Befragung von Andreas Eckert vom 28. Februar 2025, S. 22.

Nachdem bereits die erste Entwicklungsphase bei den Staatsanwaltschaften stark verzögert und wesentlich schwieriger und kostspieliger war als geplant, liessen sich auch für die folgenden Phasen zur Einführung von RIS2 in weiteren Amtsstellen massive Kostenüberschreitungen erahnen. Vor diesen Hintergrund entschied die Direktionsvorsteherin, Jacqueline Fehr, im September 2015, das Projekt zu überprüfen. In der Folge verzichtete der Regierungsrat angesichts der damit verbundenen Risiken auf die Weiterführung der Eigenentwicklung von RIS2.[280]

7.2.4 Netboxen zur Entlastung des Hauptnetzes

Da das kantonale Netzwerk sehr schwach war, wurden laut Aussage des ehemaligen Leiters der JI-Informatik, Fredi Steiner, Rechner in den Amtsstellen installiert. Diese enthielten die Programmdaten des Rechtsinformationssystems (RIS) und des Buchhaltungssystems und dienten zur Software-Verteilung bei Updates. Das QM-Dokument definiert Netboxen folgendermassen: «Als Netboxen werden dezentrale Server-Einheiten bezeichnet, welche an verschiedenen Aussenstellen zur Entlastung der zentralen RZ-Infrastruktur im Einsatz stehen (z. B. für die Software-Verteilung oder als Print-Server). Auf Netboxen werden keine Nutzdaten gehalten.»[281]

Der polizeiliche Schlussbericht im Auftrag der Staatsanwaltschaft III kam betreffend Netboxen zu folgenden Erkenntnissen: «Bei den sogenannten Netboxen handle es sich um Server, welche zur Entlastung von Hauptdatenleitungen eingesetzt werden. Diese Entlastungsserver würden über keine Verschlüsselung verfügen. Grundsätzlich seien nur Applikations- und Installationssoftware (RIS, Office, Lotus Notes) auf diesen Servern bzw. deren Festplatten gespeichert. Anlässlich von Clients-Rollouts oder deren Austausch hätte man Benutzerdaten vom Endgerät auf Netboxen zwischengespeichert und diese anschliessend auf das neu installierte Endgerät zurückgespielt. Aus diesem Grund könne nicht ausgeschlossen werden, dass sich unverschlüsselte (nicht gelöschte) Daten auf Netboxen befinden könnten.»[282]

Auch wenn es gemäss Aussage des ehemaligen Leiters der JI-Informatik, Fredi Steiner, regelwidrig war, Daten auf diese sogenannten Netboxen zu laden, wäre es technisch grundsätzlich möglich gewesen und somit auch nicht auszuschliessen.[283] Damit zeigt sich hier eine potenzielle Sicherheitslücke. Es kann somit nicht ausgeschlossen werden, dass auf diesem Weg Daten abgeflossen sind.

7.3 Aufbau einer IT-Sicherheitsorganisation

Nach der Erarbeitung des Informatiksicherheitskonzepts im Jahr 2013 schuf man in der JI-Informatik 2014 die Stelle einer Informatiksicherheitsbeauftragten.[284] Im Rahmen einer Präsentation stellte sie ihre neue Rolle vor und lieferte eine Übersicht zur IT-Sicherheit im Kanton und in der JI.[285] Sie hob die fehlende Kompetenz hervor, Sicherheitsvorkehrungen direkt anzuordnen, sowie den Umstand, dass nicht sie für die Einhaltung der Minimalanforderung verantwortlich sei. In Anlehnung an die be-

---

[280] RRB Nr. 1116/2016 vom 23. November 2016, RIS2-Überprüfung (Ergebnisse und weiteres Vorgehen); Direktion der Justiz und des Innern, Medienmitteilung vom 31. August 2016 «Direktion der Justiz und des Innern baut Rechtsinformationssystem RIS2 nicht weiter aus».

[281] Direktion der Justiz und des Innern, Generalsekretariat, DigiSol, Infrastructure Management, Aufsetzen Server vom 8. April 2009, Version 4.0 vom 1. April 2016, S.4.

[282] Kantonspolizei, Schlussbericht zum Ermittlungsverfahren Memory vom 19. Dezember 2024, S. 8–9.

[283] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 12.

[284] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 12.

[285] Direktion der Justiz und des Innern, Logistik, Finanzen & Controlling, IT-Sicherheitsbeauftragte JI, Präsentation «IT-Sicherheit JI» für das IT-Team vom 9. Juli 2014.

stehende Sicherheitsorganisation der Baudirektion wurde die Gründung eines IT-Sicherheitsausschusses und die Etablierung eines Informatiksicherheits-Managementsystems (ISMS) beabsichtigt, wobei die Informatik-Sicherheitsbeauftragte zur Risikobeurteilung explizit auf den ISO-Standard 27001 Bezug nahm. Der Sicherheitsausschuss wurde am 17. September 2014 gegründet und auch die Massnahmen und Ziele der folgenden Jahre lagen bereits fest: Schutzbedarfsfeststellungen und Risikoanalysen, Konzepte für die Schulung und Sensibilisierung sowie ein Reporting.[286]

Die Funktion der Informatik-Sicherheitsbeauftragten hatte jedoch scheinbar keine grosse Auswirkung und die Stelle blieb offenbar auch nicht lange bestehen, denn sowohl der frühere Generalsekretär, Christian Zünd, als auch die heutige Generalsekretärin, Jacqueline Romer, sowie die heutige Regierungsrätin, Jacqueline Fehr, gaben an, die entsprechende Person nicht zu kennen.[287] Jacqueline Fehr lernte in dieser Funktion den heutigen ICT-Security-Architekten der Digital Solutions kennen, welcher der Sicherheit eine hohe Bedeutung beimass und diesbezüglich zur Vorsicht mahnte.[288] Erst im Zusammenhang mit dem Regierungsratsbeschluss RRB Nr. 1193/2020 schuf man innerhalb der JI erneut eine dezidierte Stelle für diesen Bereich.

7.4 Würdigung durch die PUK

Die PUK Datensicherheit hat festgestellt, dass im von ihr untersuchten Zeitraum die technische Informationssicherheit in der JI einen grossen Stellenwert genoss und mit der frühen Verschlüsselung und der internen Eigenentwicklung des RIS in diesem Bereich grosse Anstrengungen unternommen wurden. Der ehemalige Leiter LFC, Renato Widmer, hat der Informationssicherheit auch gegen Widerstände die nötige Nachachtung verschafft. Dieses Vertrauen in die eigenen technischen Sicherheitsbemühungen hat allenfalls dazu geführt, dass andere Aspekte der Informationssicherheit, insbesondere die Entsorgungsprozesse, weniger Bedeutung erlangten.

Die JI-Informatik hat sich auf strategischer und konzeptioneller Ebene früh grundsätzlich gut aufgestellt. Mit dem Aufbau eines Qualitätsmanagement-Systems wurde versucht, die Prozesse abzubilden. Weiter liessen sich Ansätze zum Aufbau einer direktionsinternen Sicherheitsorganisation feststellen, die dann allerdings nicht weiterverfolgt wurden.

---

[286] Direktion der Justiz und des Innern, Logistik, Finanzen & Controlling, IT-Sicherheitsbeauftragte JI, Präsentation «Gründung IT-Sicherheitsausschuss JI vom 17. September 2014».

[287] Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 16; Protokoll der Befragung von Christian Zünd vom 30. August 2024, S. 14.

[288] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 11.

8. Ausmass und Hintergründe des Datensicherheitsvorfalls

8.1 Ausmass des Datensicherheitsvorfalls

Als die PUK Datensicherheit ihre Arbeiten aufnahm, waren sowohl der Zeitraum als auch das Ausmass des Datensicherheitsvorfalls noch nicht abschliessend geklärt. Für die Bearbeitung dieses Untersuchungsauftrags musste und konnte sich die PUK Datensicherheit weitgehend auf die Untersuchungen der Staatsanwaltschaften III und Zürich-Sihl abstützen, die hierzu umfassende Untersuchungen durchgeführt hatten. Die nachfolgenden Ausführungen stützen sich auf die Einstellungsverfügung der Staatsanwaltschaft III vom 8. September 2025.

Zeitraum

Der Zeitraum, in dem durch eine unsachgemässe Entsorgung von Datenträgern Daten der JI abgeflossen sein könnten, ist auf die Jahre 2002–2014 begrenzt, in denen der externe Dienstleister, André Gisler, für die JI Entsorgungen durchführte.

Im Rahmen der Untersuchung der Staatsanwaltschaft Zürich-Sihl blieb das konkrete Ausmass des potenziellen Datenabflusses noch weitgehend unbekannt. Es war nicht bekannt, wie viele Datenträger der Dienstleister, André Gisler, von der JI erhalten hatte und inwieweit diese verschlüsselt waren.[289]

Mögliches Ausmass des Datensicherheitsvorfalls

Aus der Untersuchung der Staatsanwaltschaft III geht hervor, dass der Dienstleister, André Gisler, im Zeitraum von 2002–2014 maximal gegen 2700 Personal Computer der JI zur Löschung/Wiederverwendung und/oder Entsorgung erhalten haben könnte. Hinzu kommen noch 60 bis 70 Geräte, die von den Statthalterämtern stammten, sowie die JI-Papierakten und Datenträger aus dem RIS-Entwicklungsbüro; wobei hier eher von einem Einzelfall ausgegangen werden kann.[290]

Erkenntnisse zu den sichergestellten Datenträgern

Die Staatsanwaltschaft Zürich-Sihl und die Staatsanwaltschaft III haben an zehn verschiedenen Orten 202 Datenträger oder Gehäuse sicherstellen können. Es handelte sich um vier private Geräte (Mobiltelefone, Tablets und Notebooks), 39 Serverplatten, 150 Datenträger, also Festplatten oder USB-Datensticks, sowie neun Computergehäuse ohne Datenträger.[291]

– Die zwei privaten Geräte von Roland Gisler, dem Bruder von André Gisler, waren insofern von Interesse, als auf diesen Geräten jene Liste gefunden werden konnte, die am Anfang des Datensicherheitsvorfalls gestanden hatte. Es handelte sich um eine Datei, auf welcher die privaten Adressen von Staatsanwältinnen und Staatsanwälten, teilweise mit Bildern der Betroffenen, enthalten waren.[292] Wie die weiteren Ermittlungen zeigten, stammten die in dieser Liste zusammengestellten Informationen aus öffentlichen Quellen und kamen nicht, wie ursprünglich befürchtet, von Datensätzen aus der JI. Durch die Nutzung von Adressverzeichnissen oder Datenbanken mit Wirtschaftsinformationen sowie eigene Abklärungen hatte Roland Gisler diese Informationen zusammengetragen. Über eine solche Abfrage war er auch an die Informationen gelangt, die es seiner Bekannten erlaubten, den Staats-

[289] Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 16.

[290] Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 21–24.

[291] Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 24–27.

[292] Kantonspolizei, Visionierungsbericht Mobiltelefon und Tablet vom 7. Februar 2024 mit Beilagen.

anwalt am 8. November 2020 zu Hause aufzusuchen. Auf den privaten Geräten befanden sich aber auch interne JI-Dokumente, wie beispielsweise Telefonlisten von Ämtern.[293]
– Die sichergestellten 39 Serverplatten, für die eine Herkunft von der JI lediglich vermutet werden kann, waren aus dem RAID-Verbund[294] mit anderen Platten gelöst und somit für Dritte nicht mehr lesbar.
– Bei den neun sichergestellten Gehäusen handelte es sich wohl um Geräte des Verwaltungsgerichts, dessen IT damals noch durch die JI ausgeführt wurde.
– Die Staatsanwaltschaft III und die Kantonspolizei haben grosse Anstrengungen unternommen, um die Herkunft der 150 Datenträger, darunter ca. 40 USB-Datensticks, zu klären. Etwa die Hälfte der sichergestellten Datenträger weisen einen JI-Bezug auf (siehe Tabelle 14).

Tabelle 14 Übersicht zu den sichergestellten Datenträgern

150 sichergestellte Datenträger	davon mit JI-Bezug
97 interne Festplatten	54
37 USB-Sticks	19
6 Speicherkarten	–
5 externe Datenträger	–
5 Desktop-Computer mit Datenträgern	–

Sofern die Benutzer der obengenannten Geräte der JI angehörten und eine Benutzerkennung vorhanden war, konnten die Datenträger durch diese der JI zugewiesen werden. Die Datenträger ohne Benutzerkennung mussten inhaltlich durch die Staatsanwaltschaft III bzw. die Kantonspolizei visioniert werden. Auf Basis des gesichteten Inhaltes konnte dann eine Zuordnung erfolgen. Auf diese Weise konnte die Kantonspolizei weiter eruieren, dass sich insgesamt 73 Datenträger der JI und 43 Datenträger Dritten zuordnen liessen. Bei weiteren 34 Datenträgern war keine Zuordnung möglich. Da auch auf sichergestellten Datenträgern von Privaten JI-Daten gefunden wurden, die vermutlich darauf kopiert worden waren, geht die Staatsanwaltschaft III insgesamt von etwa 80 bis 90 Datenträgern mit JI-Relevanz aus.[295]

Sensitivität der Daten

Als besonders schützenswerte Personendaten gelten Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht.[296]

Die Daten verschiedener Ämter waren vom Datensicherheitsvorfall betroffen, was in einigen Fällen auch Auswirkungen auf die in den Unterlagen genannten Personen und deren besonders schützenswerte Personendaten hatte. Besonders betroffen waren das Statistische Amt und das Amt für Justizvollzug und Wiedereingliederung. Mehr-

[293] Protokoll der Befragung von Mathias Eberli vom 31. Januar 2025, S. 3–8 mit Hinweis auf die diesbezüglichen Aussagen im Rahmen der Delegierten Einvernahme von Roland Gisler vom 23. Februar 2022.

[294] In einem RAID (Redundant Array of Independent Disks) werden mehrere physische Datenträger zu einem logischen System verbunden. Dabei werden die Daten auf die verschiedenen Datenträger verteilt. Ein Zugriff auf die Daten ist nur bei einer korrekten Anordnung der redundanten, unabhängigen Festplatten möglich.

[295] Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 25–27.

[296] Dazu gehören gemäss § 3 Abs. 4 IDG Informationen über: (a) die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten; (b) die Gesundheit, die Intimsphäre, die ethnische Herkunft sowie genetische oder biometrische Daten; (c) Massnahmen der sozialen Hilfe; oder (d) administrative oder strafrechtliche Verfolgungen oder Sanktionen.

fach betroffen waren aber auch die Regionalen und die Besonderen Staatsanwaltschaften des Kantons Zürich, das Gemeindeamt, das Staatsarchiv und die Statthalterämter. Punktuell flossen zudem Daten aus den Bezirksratskanzleien und dem Verwaltungsgericht ab, deren IT damals durch die JI betreut wurde.

Durch die Auswertung der sichergestellten Datenträger konnte die Staatsanwaltschaft III ermitteln, dass die Daten von lokal und unverschlüsselt gespeicherten Informationen und nicht direkt aus dem RIS-System stammen. Die Staatsanwaltschaft III kommt dennoch zum Schluss, dass der Datensicherheitsvorfall durch die Offenlegung der teils sensitiven Inhalte dieser Datenträger die persönlichen Rechte der betroffenen Personen erheblich beschnitten hat. So liessen sich anhand der Daten Rückschlüsse auf die Beteiligung von Personen in Strafverfahren oder Strafvollzugsmassnahmen ziehen.[297] Welche konkreten Auswirkungen der zuvor geschilderte Besuch bei einem Staatsanwalt hatte, ist nicht bekannt. Zurück bleiben jedoch ein Vertrauensverlust und eine Unsicherheit – auch aufgrund der aktiven Drohung, die Daten zu verwenden, als das Ausmass des Vorfalls noch unklar war. Auch die Direktionsvorsteherin der JI, Jacqueline Fehr, kam angesichts des Umstands, dass man das Schadenspotenzial nie abschliessend beurteilen konnte, zum Schluss: Auch wenn bis heute nichts Schlimmes passiert sei, wisse man nie, ob das so bleibe. Die Frage, wie gravierend der Vorfall wirklich gewesen sei, beschäftige sie bis heute.[298]

8.2 Umstände der Auftragsvergabe an den externen Dienstleister

8.2.1 Die Anstellung des externen Dienstleisters André Gisler

Bis ins Jahr 2000 arbeitete André Gisler als Angestellter eines Unternehmens für Bürobedarf und Büromöbel, das auch die JI regelmässig belieferte. In dieser Funktion war André Gisler gemäss der Aussage des späteren Leiters der JI-Informatik, Fredi Steiner, bereits für die JI tätig, als Letzterer am 1. Oktober 1997 seine Stelle als Leiter PC-Support antrat.[299] Im Jahr 2000 endete die Anstellung von André Gisler bei diesem Unternehmen. Gemäss den Abklärungen der Staatsanwaltschaft Zürich-Sihl arbeitete André Gisler in den Jahren 2002–2014 in unregelmässigen Abständen für die JI und gründete 2002 mit seinem damaligen Geschäftspartner sein eigenes Unternehmen «AG Transporte».[300] In den Jahren 2007–2012 war er gemäss den Abklärungen der Staatsanwaltschaft III als Selbständiger für ein weiteres Unternehmen mit Sitz im Kanton Zug tätig, das der JI verschiedene Druckermodelle lieferte. Lediglich für diese spezifische Tätigkeit bestand ab dem Jahr 2013 zwischen André Gisler und diesem Unternehmen ein Arbeitsvertrag auf Abruf.[301]

Gemäss der Aussage des damaligen Leiters der JI-Informatik, Fredi Steiner, tauchte André Gisler nach der Beendigung seiner Anstellung beim Unternehmen für Bürobedarf und Büromöbel mit seinem eigenen Lastwagen bei der JI-Informatik auf und bot seine Unterstützung an. Da die JI-Informatik damals niemanden für Transporte hatte und André Gisler bereits bekannt war, griff sie auf ihn zurück. In der Wahrneh-

---

297 Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 26–27.

298 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 30.

299 Staatsanwaltschaft III, Delegierte Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023; Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 16. Auch der frühere Leiter der JI-Informatik (1996–2000) gab an, das vom Leiter LFC, Renato Widmer, ausgesuchte Unternehmen übernommen zu haben. Siehe Staatsanwaltschaft III, Delegierte Einvernahme des Leiters der JI-Informatik (1996–2000) vom 19. Juli 2023.

300 Staatsanwaltschaft Zürich-Sihl, Einvernahme von André Gisler vom 23. Februar 2021.

301 Kantonspolizei, Schlussbericht zum Ermittlungsverfahren Memory vom 19. Dezember 2024, S. 24.

mung von Fredi Steiner war André Gisler ein Transporteur, der Dinge austauschte und von A nach B brachte.[302] Laut dem von ihm 2020 rückblickend erstellten Memo war André Gisler sporadisch zur Unterstützung des PC-Supports im Einsatz:

«Zu seinen Aufgaben zählten vornehmlich Installationen und Umzugsaktionen von PC-Arbeitsplätzen und Druckern. Er erledigte diverse kleine, aber auch grössere Transportarbeiten für die IT und unterstützte das PC-Support-Team vor allem bei Ferienengpässen oder bei grösseren Umzügen in den Amtsstellen. Ebenso wurden immer wieder Entsorgungsaktionen von Elektroschrott durch ihn durchgeführt, wobei hier festgehalten werden muss, dass die IT-JI nie Server-Hardware zusammen mit den Harddisks zur Entsorgung freigegeben hatte.»[303]

Der ehemalige Leiter LFC, Renato Widmer, war gemäss eigener Aussage vom Leiter der JI-Informatik, Fredi Steiner, darüber informiert, dass der Transporteur André Gisler im Zusammenhang mit der Verteilung von Geräten im ganzen Kanton Transportdienstleistungen ausführte.[304] Um die Projekte innerhalb eines gewissen Zeitrahmens umsetzen zu können, habe es im Rahmen von Rollout-Projekten externe Unterstützung gebraucht. Weiter betonte der Leiter LFC in der Befragung, dass André Gisler auch für das Unternehmen, von dem die JI ihre Drucker leaste, Drucker transportierte.[305]

Grössere Aufträge betrafen gemäss den Aussagen der direkt beteiligten JI-Mitarbeiterin, Erika W., die Entsorgung von Druckern, aber auch PC-Geräte seien durch ihn gebracht oder abgeholt worden. Bereits zu Beginn seiner Geschäftstätigkeit sei er auch mit Entsorgungsaufgaben beauftragt worden, wobei aber unklar sei, ob er auch Endgeräte entsorgt habe.[306] Laut dem ehemaligen Leiter der JI-Informatik, Fredi Steiner, hat André Gisler respektive sein Unternehmen für die JI-Informatik auch Löschaktionen vorgenommen.[307] André Gisler gab bei seiner Einvernahme an, er habe um das Jahr 2002 von der Staatsanwaltschaft des Kantons Zürich, wohl allgemein von der JI, im Rahmen der Ablösung von alten Geräten etwa 1500 Geräte, also Monitore, Clients und Drucker, erhalten. Die ausgebauten Harddisks seien durch ihn respektive seine Mitarbeiter entweder gelöscht und weiterverkauft oder zerbohrt worden.[308] Mit einer Löschdiskette der Staatsanwaltschaft habe er die Harddisks in einer Löschstrasse in den Räumlichkeiten der AG Transporte gelöscht, aufbereitet und in seinem Laden oder über Plattformen verkauft. André Gisler erhielt in der Folge jeweils Anrufe, wenn es Material gab, das bei der JI abgeholt werden sollte. Die korrekte Löschung der Daten lag in seinem Interesse, da ihm gesagt wurde, dass er bei einem Datenverlust keine Geräte mehr erhalte.[309]

Der freischaffende Mitarbeiter von André Gisler (etwa 2010–2013) gab an, dass er für die vollständige Überschreibung der Festplatten von der Mitarbeiterin des Helpdesks der JI, Erika W., eine Spezialdiskette erhalten habe.[310] Der ehemalige Leiter der JI-Informatik, Fredi Steiner, kann sich nicht mehr erinnern, ob diese Löschungen nur innerhalb oder auch ausserhalb der Räumlichkeiten der JI stattgefunden haben.[311]

---

302 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 16, 25.

303 Direktion der Justiz und des Innern, Generalsekretariat, DigiSol, Memo von Fredi Steiner vom 10. November 2020 «Mögliches Datenleck IT JI».

304 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 17.

305 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 20.

306 Staatsanwaltschaft Zürich-Sihl, Delegierte Einvernahme von Erika W. vom 23. November 2020.

307 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 9.

308 Staatsanwaltschaft Zürich-Sihl, Einvernahme von André Gisler vom 23. Februar 2021, Fragen 64, 81.

309 Staatsanwaltschaft III, Einvernahme von André Gisler vom 24. Januar 2023, Fragen 41–64.

310 Staatsanwaltschaft III, Einvernahme des ehemaligen Mitarbeiters vom 22. März 2023.

311 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 29.

8.2.2 Fehlende vertragliche Basis

Der ehemalige Leiter LFC, Renato Widmer, gab an, mit André Gisler keinen Vertrag als Dienstleister abgeschlossen zu haben.[312] Gemäss seinen Aussagen hätte die JI-Informatik diesen Vertrag, der innerhalb der Finanzkompetenz von 100 000 Franken[313] der Abteilung gelegen hätte, abschliessen können und sollen.[314]

Der ehemalige Leiter der JI-Informatik, Fredi Steiner, sagte hingegen aus, dass er angesichts der finanziellen Rahmenbedingungen auch bei kleineren Aufträgen jeweils beim Leiter LFC, Renato Widmer, nachgefragt habe, ob die Ausgabe in Ordnung sei.[315] Im Bereich Personal, Finanzen und Verträge habe der Leiter LFC das letzte Wort gehabt.[316] Auch die Anwendung der kantonalen Allgemeinen Geschäftsbedingungen (AGB) betreffend Umgang mit externen Dienstleistern und die Umsetzung im Rahmen des Vertragswesens lag gemäss dem ehemaligen Leiter der JI-Informatik beim Leiter LFC.[317] Zudem habe der ehemalige Leiter LFC, Renato Widmer, die Verträge physisch bei sich im Kaspar-Escher-Haus gehabt. Diese Aussage wird durch das QM-Dokument zum Beschaffungswesen[318] gestützt, wonach mit Lieferanten oder Dienstleistern abgeschlossene Verträge zentral durch den Leiter LFC verwaltet werden. Verträge waren folglich, anders als die Inventarblätter, welche die einzelnen Gerätewechsel dokumentierten, nicht bei der JI-Informatik abgelegt.[319] Es entzieht sich der Kenntnis des ehemaligen Leiters der JI-Informatik, Fredi Steiner, ob mit der AG Transporte oder André Gisler jemals ein Vertrag bestanden hat.[320] Auch die Staatsanwaltschaft III konnte im Rahmen ihrer Untersuchung keinen Arbeitsvertrag ausfindig machen. Darüber, ob dieser jemals in schriftlicher Form vorgelegen habe, lasse sich nur spekulieren.[321]

Der PUK Datensicherheit liegt einerseits die Stellenbeschreibung des ehemaligen Leiters der JI-Informatik vor, aus der hervorgeht, dass die Ausarbeitung von grossen Dienstleistungsverträgen (Service-Level-Agreements) zu seinem Aufgabenbereich gehörte und er für den Beizug und den Einsatz externer Spezialisten in den Bereichen Rekrutierung, Vertragsabschluss sowie Tarifverhandlung im Umfeld der JI-Informatik, aber auch generell für die korrekte Umsetzung der Sicherheitsvorgaben verantwortlich war.[322] Andererseits wies die Informatikstrategie die Verantwortlichkeit für die interne und externe Leistungs-Verbringung [sic] klar dem Leiter LFC zu.[323]

Damit liegen widersprüchliche Grundlagen vor. Es bleibt somit unklar, in wessen Zuständigkeit Abmachungen mit dem externen Dienstleister André Gisler oder seiner AG Transporte gefallen wären.

---

312 Staatsanwaltschaft III, Delegierte Einvernahme von Renato Widmer vom 28. Juni 2023, Frage 69.

313 Der Abteilungsleiter der JI-Informatik verfügte gemäss Anhang zum Organisationsreglement des Generalsekretariats der JI (ORGS) vom 23. Dezember 2010 über die Kompetenz für einmalige Ausgaben von 100 000 Franken, der Hauptabteilungsleiter LFC über die Kompetenz für einmalige Ausgaben bis 200 000 Franken.

314 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 13, 17.

315 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 18.

316 Staatsanwaltschaft III, Delegierte Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023, Frage 20.

317 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 10.

318 Direktion der Justiz und des Innern, Logistik, Finanzen & Controlling, Abteilung Informatik, Beschaffung vom 24. Juni 2008.

319 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 20–22.

320 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 26.

321 Kantonspolizei, Schlussbericht zum Ermittlungsverfahren Memory vom 19. Dezember 2024, S. 39.

322 Direktion der Justiz und des Innern, Personaldienst, Stellenbeschreibung Abteilungsleiter IT-JI vom 3. November 2010.

323 Direktion der Justiz und des Innern, Generalsekretariat, Logistik, Finanzen und Controlling, Informatik-Strategie und Reglement der Direktion der Justiz und des Innern (JI) des Kantons Zürich. Erlassen am 14. Februar 2011, S. 8.

8.2.3 Das Entschädigungsmodell

Gemäss der Aussage der direkt beteiligten Helpdesk-Mitarbeiterin, Erika W., erhielt André Gisler für seine geleisteten Arbeitsstunden im Gegenzug Druckergeräte oder Bildschirme.[324] André Gisler und weitere Personen aus seinem damaligen Umfeld sagten gegenüber der Staatsanwaltschaft Zürich-Sihl und gegenüber der Staatsanwaltschaft III aus, dass er für seine geleistete Arbeit alte PC-Geräte erhielt respektive für den Erhalt von Geräten im Gegenzug im entsprechenden Umfang bei der JI arbeiten musste.[325]

Gemäss seinen eigenen Angaben schloss André Gisler mit der JI Geschäfte über die Entsorgung von PC-Geräten ab. Dabei habe es sich um Geräte gehandelt, welche turnusgemäss ausgetauscht werden mussten. Für den Erhalt dieser ersten Geräte der JI musste er im Gegenzug arbeiten.[326] Wie dieser Auftrag, wohl um das Jahr 2002, genau zustande gekommen war, lässt sich nicht mehr eruieren. Manche Aussagen deuten darauf hin, dass André Gisler aufgrund seiner früheren Lieferantentätigkeit, auch nach der Beendigung seiner Anstellung bei dem Unternehmen für Bürobedarf, in der JI weiter Beschäftigung fand.[327]

Der ehemalige Leiter der JI-Informatik, Fredi Steiner, sagte aus, dass er den Austausch von Hardware gegen Leistung nie veranlasst habe und auch nicht legitimiert hätte. Es sei ihm nicht bewusst gewesen, dass André Gisler mit Ware bezahlt worden sei, weshalb er nach dem Bekanntwerden des Datensicherheitsvorfalls auch entsprechende Rechnungen gesucht habe.[328]

Der ehemalige Leiter LFC, Renato Widmer, gab hingegen an, der ehemalige Leiter der JI-Informatik, Fredi Steiner, habe ihn einmal informiert, dass mit dem Dienstleister so etwas vereinbart worden sei. Er betonte, dass er diese Vereinbarung nicht getroffen habe, über den Einsatz von André Gisler sei in der JI-Informatik entschieden worden.[329] Dem ehemaligen Leiter LFC war gemäss eigenen Angaben bewusst, dass Geräte verkauft wurden. Er sei aber davon ausgegangen, dass dies regelkonform abgelaufen sei.[330] Sowohl der ehemalige Leiter LFC als auch der ehemalige Leiter der JI-Informatik schildern, dass Ersterer intervenierte, als André Gisler nicht nur bei Rollouts, sondern auch unterjährig für kleinere Arbeiten eingesetzt wurde. Denn diese Arbeiten sollten mit internen Ressourcen realisiert werden.[331]

Die mit der Abwicklung betraute Helpdesk-Mitarbeiterin, Erika W., sagte gegenüber der Staatsanwaltschaft Zürich-Sihl aus, die Vereinbarungen nicht selbst abgeschlossen zu haben.[332] Als Verwaltungsmitarbeiterin hatte sie gemäss dem ehemaligen Leiter LFC, Renato Widmer, auch nicht die Kompetenz dazu.[333] Da sie keine Kaderangestellte war, ging der ehemalige Mitarbeiter von André Gisler gemäss seiner

---

[324] Staatsanwaltschaft Zürich-Sihl, Delegierte Einvernahme von Erika W. vom 23. November 2020, Anhang 3 der Administrativuntersuchung.

[325] Staatsanwaltschaft Zürich-Sihl, Einvernahme von André Gisler vom 23. Februar 2021, Frage 14; Staatsanwaltschaft III, Einvernahme des ehemaligen Mitarbeiters vom 22. März 2023, Frage 5; Staatsanwaltschaft III, Delegierte Einvernahme der früheren Partnerin vom 30. März 2023, Frage 67.

[326] Staatsanwaltschaft Zürich-Sihl, Einvernahme von André Gisler vom 23. Februar 2021.

[327] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 16; Staatsanwaltschaft III, Delegierte Einvernahme der früheren Partnerin vom 30. März 2023.

[328] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 24.

[329] Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 18–19.

[330] Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 9.

[331] Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 18–19; Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 25.

[332] Staatsanwaltschaft Zürich-Sihl, Delegierte Einvernahme von Erika W. vom 23. November 2020, Frage 47.

[333] Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 18.

Aussage davon aus, dass ihre Vorgesetzten über den Wiederverkauf der Geräte im Bild waren.[334] Der ehemalige Leiter der JI-Informatik, Fredi Steiner, sagte aus, bei Einsätzen von André Gisler, die länger als einen Tag dauerten, jeweils per E-Mail oder Anruf die Legitimation des Leiters LFC, Renato Widmer, abgeholt und erst nach Rücksprache mit diesem den Entscheid für Einsätze des Dienstleisters André Gisler gefällt zu haben. Da er davon ausging, dass dieser eine Rechnung stellen würde, nahm der ehemalige Leiter der JI-Informatik gemäss eigenen Angaben jeweils hinsichtlich der finanziellen Konsequenzen Rücksprache mit dem Leiter LFC.[335]

8.2.4 Budgetäre Rahmenbedingungen und ausbleibende Rechnungsstellung

Wenn die internen Ressourcen beispielsweise für den Austausch von Druckern in einer Aussenstation nicht ausreichten, bat die für die JI-Arbeitsplätze zuständige Helpdesk-Mitarbeiterin, Erika W., jeweils darum, den externen Mitarbeitenden André Gisler als Helfer für eine gewisse Zeit beiziehen zu können.[336] In jedem Fall musste sie nach einer bestimmten Zeit mit dem Leiter der JI-Informatik, Fredi Steiner, oder dem Leiter LFC, Renato Widmer, Rücksprache nehmen. Man wollte wohl angesichts des engen Budgets vermeiden, dass André Gisler seine Arbeit in Rechnung stellte. Der ehemalige Leiter LFC führte aus, dass es auch politisch schwierig war, immer genügend Mittel für die Informatik budgetieren zu können, und dass manchmal weniger Mittel als benötigt zur Verfügung standen.[337] Gemäss den ehemaligen Direktionsvorstehern, Markus Notter und Martin Graf, sowie weiteren Mitarbeitenden des Generalsekretariats der JI war der ehemalige Leiter LFC um einen wirtschaftlichen und sparsamen Umgang mit den Mitteln bemüht und suchte im Sinne des New Public Managements auch eigenständige unternehmerische Lösungen.[338]

Der ehemalige Leiter der JI-Informatik, Fredi Steiner, gab an, mit Ausnahme von Rechnungen zu Drucker-Rollouts keine Rechnungen von André Gisler oder seinem Unternehmen AG Transporte gesehen zu haben.[339] Auch der ehemalige Leiter LFC, Renato Widmer, räumte ein, dass es sich bei den Rechnungen, die er diesbezüglich gesehen habe, um keine grossen Beträge gehandelt habe.[340] Da der Direktionscontroller der JI in den Buchhaltungsbelegen «fast nichts» finden konnte, ist es aus seiner Sicht plausibel, dass die Entlöhnung mit Geräten erfolgte.[341] Auch die Finanzkontrolle konnte kaum finanzielle Spuren von André Gisler nachweisen.[342] Sie fand lediglich vier Belege aus dem Zeitraum 2011–2017 mit Bezug zu Drucker-Rollouts. Weiter war der Name André Gislers in einer Dokumentation der KITT-Geschäftsstelle vom 17. November 2014 zur Erhebung der Basisarbeitsplatzkosten aufgeführt. Darin war er unter den Personalkosten als externes Personal geführt und es wurden diesbezüg-

---

334 Staatsanwaltschaft Zürich-Sihl, Delegierte Einvernahme des ehemaligen Mitarbeiters vom 5. Februar 2021, Frage 58.

335 Staatsanwaltschaft Zürich-Sihl, Einvernahme von Fredi Steiner vom 13. November 2020, Frage 51; Staatsanwaltschaft III, Delegierte Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023, Frage 40.

336 Staatsanwaltschaft III, Delegierte Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023, Fragen 40–41.

337 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 20.

338 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 21; Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 18; Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 12; Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 8.

339 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 22.

340 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 19.

341 Staatsanwaltschaft III, Delegierte Einvernahme des Direktionscontrollers vom 18. August 2023, Frage 83.

342 Finanzkontrolle Kanton Zürich, Aktennotiz «Datenleck Justizdirektion» vom 7. Dezember 2022.

liche Kosten ausgewiesen, auch dort mit einem Bezug zum Drucker-Unternehmen.[343] Auf Nachfrage der PUK Datensicherheit präzisierte die Finanzkontrolle zudem, dass die letztgenannte Information keine Rückschlüsse auf tatsächliche Transaktionen oder Auftragsvolumina zulasse.[344] Da die Budgetierung und Rechnungsführung zentralisiert waren, wären allfällige Rechnungen zentral bei der Hauptabteilung LFC verbucht worden.[345]

8.3 Abläufe innerhalb der Direktion in der Praxis

8.3.1 Ablauf und Auftragserteilung

Gemäss eigenen Angaben koordinierte die Mitarbeiterin des Helpdesks, Erika W., im Bereich PC-Support die PC-Arbeitsplätze und führte in diesem Zusammenhang auch das Geräteinventar nach. Dabei koordinierte sie den Austausch defekter Einzelgeräte. Bei Rollouts ganzer Flotten entschieden hingegen Projektzuständige, wie der Austausch zu erfolgen hatte.[346] Erika W. hatte gemäss dem ehemaligen Leiter der JI-Informatik, Fredi Steiner, die einzelnen Austauschaktionen zu planen und erteilte dem externen Dienstleister André Gisler die konkreten Aufträge.[347] Dieser und seine ehemaligen Mitarbeitenden bestätigen, dass der direkte Kontakt jeweils über diese Helpdesk-Mitarbeiterin ablief und sie die wichtigste Ansprechperson war.[348] Gemäss dem ehemaligen Leiter des Data-Centers hatte sie die Entsorgung organisiert, die Termine abgesprochen und war intern die Ansprechperson für den Austausch von Hardware.[349] Der Kontakt mit den Hardwarelieferanten, die Organisation von Reparaturen sowie die Inventarisierung von IT-Geräten sind auch in ihrer Stellenbeschreibung enthalten.[350] Für jede Gerätemutation existierte ein Inventarblatt, aus dem hervorging, welches Gerät durch welches Gerät ersetzt worden war und an welchen Standorten diese Geräte ausgewechselt wurden. Auf Basis dieser Inventarblätter führte die Helpdesk-Mitarbeiterin das Inventar sorgfältig nach. Das Inventar widerspiegelte dann jeweils den aktuellen Stand, es liess sich demzufolge kein Bild mehr über die historischen Zu- und Abgänge gewinnen. Wohl um die Veränderungen weiterhin nachvollziehen zu können, wurden die Inventarblätter jahrelang aufbewahrt.[351]

Die obigen Ausführungen widerspiegeln die Prozesse zur Rücknahme einzelner PC-Arbeitsplätze, wie sie in der QM-Dokumentation beschrieben sind (siehe dazu Kapitel 7.1.4 zu den Vorgaben): Die Rücknahme einzelner PC-Arbeitsplätze konnte direkt über den Helpdesk abgewickelt werden. Nach erfolgter Dienstleistung war eine unterschriebene Auslieferungsbestätigung (Inventarblatt) abzugeben, und der Personaleinsatz wurde zwischen der Administration und dem Abteilungsleiter geplant. In

---

343 Finanzkontrolle Kanton Zürich, Revisionsakten zur IT-Beschaffungsprüfung 2014: Dokumentation vom 17. November 2014 zu Basisarbeitsplatzkosten.

344 Finanzkontrolle Kanton Zürich, E-Mail von Martin Billeter vom 13. September 2024.

345 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 16.

346 Staatsanwaltschaft Zürich-Sihl, Einvernahme von Erika W. vom 23. November 2021, Frage 16.

347 Staatsanwaltschaft III, Delegierte Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023, Fragen 40–43.

348 Staatsanwaltschaft Zürich-Sihl, Einvernahme von André Gisler vom 23. Februar 2021, Fragen 14, 31, 60; Staatsanwaltschaft Zürich-Sihl, Delegierte Einvernahme des ehemaligen Mitarbeiters vom 5. März 2021, Fragen 48, 110; Staatsanwaltschaft III, Einvernahme des ehemaligen Mitarbeiters vom 22. März 2023, Frage 48.

349 Staatsanwaltschaft III, Einvernahme des ehemaligen Leiters des Data-Centers vom 14. August 2023, Fragen 22–23.

350 Direktion der Justiz und des Innern, Logistik, Controlling & Finanzen, Stellenbeschreibung Administrative Aufgaben in der IT-Abteilung und Hotline vom 10. November 2010.

351 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 21.

Widerspruch zur Vorgabe wurde der externe Dienstleister jedoch nicht nur im Rahmen von grösseren Rollouts, sondern eben auch bei einzelnen Rücknahmeprozessen beigezogen.

Auf wessen konkrete Order und in welchem Ausmass die Aufträge an die Helpdesk-Mitarbeiterin bzw. in der Folge an André Gisler und sein Unternehmen AG Transporte vergeben wurden, konnte die Staatsanwaltschaft III im Rahmen ihrer Untersuchung nicht klären. Sie konnte trotz umfangreicher Ermittlungen nicht belastbar rekonstruieren, welche effektive Rolle der Leiter LFC, Renato Widmer, der ehemalige Leiter der JI-Informatik, Fredi Steiner, und die Helpdesk-Mitarbeiterin, Erika W., gespielt hatten.[352] Gemäss den Aussagen des ehemaligen Leiters des Data-Centers müsste es sich bei der Person, welche den Auftrag erteilt hatte, grundsätzlich um den Leiter der JI-Informatik, Fredi Steiner, gehandelt haben. Da der Leiter LFC, Renato Widmer, aber auch direkt Aufträge an die Mitarbeitenden erteilte, gehe er davon aus, dass der Dienstweg nicht eingehalten worden sei und die Helpdesk-Mitarbeiterin, Erika W., vom Leiter LFC direkt Aufträge erhalten habe.[353] Im Organigramm der JI-Informatik vom März 2014 waren die externen Mitarbeitenden, darunter auch André Gisler, der IT-Leitung seitlich beigeordnet.[354] Gemäss dem ehemaligen Leiter der JI-Informatik, Fredi Steiner, lag die Entscheidung darüber, welche Geräte wie ausgewechselt wurden, in erster Linie beim Leiter LFC, Renato Widmer.[355] Die QM-Prozesse aus dem Jahr 2009 zeigen, dass im Rahmen der planbaren Aktionen, wie Umzügen von Geräten oder Rollouts, die Freigabe durch den Leiter LFC zu erfolgen hatte. Dieser erteilte dann den Auftrag zur Abwicklung an die Disposition (Helpdesk). Der Leiter der JI-Informatik musste im Rahmen dieser Prozesse nur informiert werden. In den Prozessen ist also eine direkte Auftragsweitergabe vom Leiter LFC an die Helpdesk-Mitarbeiterin abgebildet. Es scheint somit plausibel, dass in diesem Bereich die Prozesse auch so umgesetzt wurden, ein direkter Kontakt zwischen dem Leiter LFC, Renato Widmer, und der Helpdesk-Mitarbeiterin, Erika W., bestand und diese wiederum mit dem externen Mitarbeiter, André Gisler, im Austausch stand.

Umgang mit Arbeitsrapporten

Die Schwierigkeiten, die Verantwortlichkeiten zu klären, sind auch darin begründet, dass zu den konkreten Aufträgen kaum schriftliche Dokumente vorliegen. Die PUK Datensicherheit konnte verschiedene Stundenrapporte von André Gisler aus den Jahren 2005–2014 einsehen (siehe Abbildung 5). Gemäss den Rapporten war André Gisler am 21. Januar 2014 letztmals für die JI tätig. Eine vereinbarte Arbeitsleistung am 24. März 2014 habe er nicht mehr erbracht.[356] Damit lässt sich festhalten, dass André Gisler von 2002–2014 für die JI tätig war.

---

[352] Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 42.

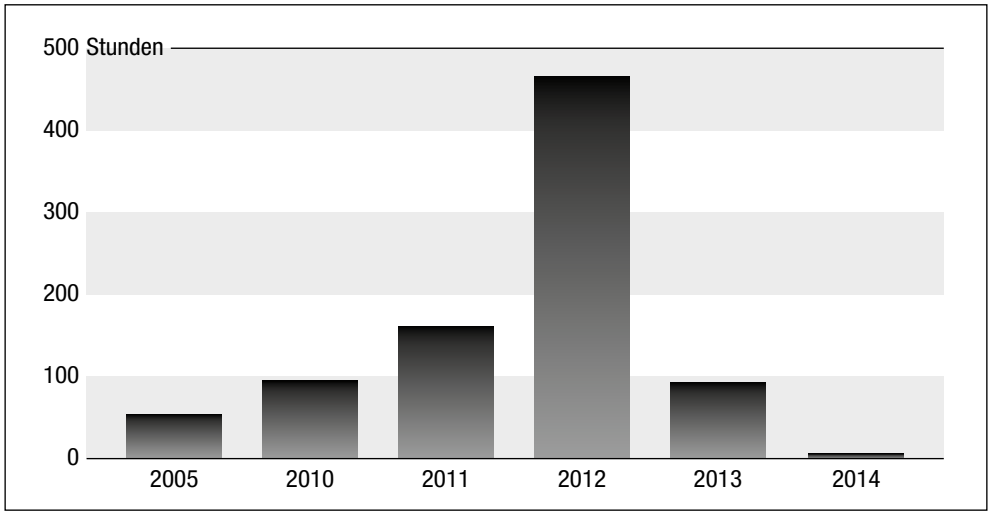
[353] Staatsanwaltschaft III, Delegierte Einvernahme des ehemaligen Leiters des Data-Centers vom 14. August 2023.

[354] Direktion der Justiz und des Innern, Logistik, Finanzen & Controlling, Abteilung Informatik, Präsentation Vorstellung IT-JI vom 3. Januar 2012 mit Organigramm IT-JI vom 10. März 2014.

[355] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 24.

[356] Staatsanwaltschaft Zürich-Sihl, Delegierte Einvernahme von Erika W. vom 23. November 2020, Frage 70.

Abbildung 5 Geleistete Stunden gemäss den vorliegenden Arbeitsrapporten



Gemäss dem heutigen Leiter des Data-Centers, der damals als Mitarbeiter des Service-Teams tätig war, hat André Gisler in den Jahren 2012–2014 etwa alle drei bis vier Monate Elektroschrott abgeholt, der in einem Palettenrahmen im Untergeschoss des Bezirksgebäudes gesammelt worden war. Im Hof hätten er und André Gisler die zu entsorgende Hardware auf den Lastwagen geladen.[357]

Die Befragten machten jedoch unterschiedliche Aussagen darüber, wer mit den Arbeitsrapporten zu tun gehabt hatte. Die direkt beteiligte Helpdesk-Mitarbeiterin, Erika W., gab an, die Arbeitsrapporte jeweils visiert und an die Hauptabteilung LFC weitergeleitet zu haben.[358] Laut dem ehemaligen Leiter der JI-Informatik, Fredi Steiner, sei dies wohl so gewesen.[359] Auch sein Vorgänger hielt das für möglich, wobei der Leiter LFC, Renato Widmer, üblicherweise die Arbeitsrapporte mitgenommen habe.[360] Der ehemalige Leiter LFC selbst sagte hingegen aus, nie einen Rapport von André Gisler erhalten oder gesehen zu haben.[361] Gemäss dem ehemaligen Leiter der JI-Informatik, Fredi Steiner, war André Gisler verpflichtet, die Rapporte einzureichen, und eine Visierung der Rapporte durch die direkt beteiligte Helpdesk-Mitarbeiterin war insofern passend, da sie die Leistungserfüllung kontrollieren konnte. Er selbst habe nur einen visierten und einen nicht visierten Rapport gesehen.[362] Er konnte weiter keine Angaben dazu machen, wie die Rapporte konkret abgelegt wurden, die Helpdesk-Mitarbeiterin habe ihm gegenüber aber geäussert, dass sie im gleichen Schrank wie die Inventarblätter deponiert worden seien. Infolge der Aufräumaktion im Jahr 2019 (siehe Kapitel 11.2) seien sie nun nicht mehr vorhanden.

---

[357] Kantonspolizei, Ermittlungsbericht IT-Infrastruktur der Digital Solution (DigiSol) mit Schwerpunkt Entsorgung Hardware vom 10. Juni 2024, S. 18.

[358] Staatsanwaltschaft Zürich-Sihl, Delegierte Einvernahme von Erika W. vom 23. November 2020, Frage 16.

[359] Staatsanwaltschaft III, Delegierte Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023, Frage 60.

[360] Staatsanwaltschaft III, Delegierte Einvernahme des Leiters der JI-Informatik (1996–2000) vom 19. Juli 2023, Frage 81.

[361] Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 19.

[362] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 30.

Ungenügende Sicherheitsüberprüfungen

Bezüglich der Sicherheitsüberprüfung vertraute die Helpdesk-Mitarbeiterin, Erika W., den Personen, von denen sie den Auftrag erhalten hatte, und ging bei langjährigen externen Mitarbeitenden davon aus, dass diese sicherheitsüberprüft waren. Nach ihrer Aussage waren die Hilfspersonen von André Gisler nicht sicherheitsüberprüft.[363] Der ehemalige Leiter der JI-Informatik, Fredi Steiner, vermutete, dass früher lediglich ein Strafregisterauszug eingefordert worden sei.[364] Auf jeden Fall seien Personen, welche die Justizvollzugsanstalt Pöschwies betreten wollten, sicherheitsüberprüft worden. Dies konnte André Gisler bestätigen.[365] Aufgrund einer solchen Überprüfung wurde seinem Mitarbeiter der Zutritt zur Justizvollzugsanstalt in Regensdorf verwehrt.[366]

Der ehemalige Leiter der JI-Informatik, Fredi Steiner, konnte nichts zu einer Sicherheitsüberprüfung von André Gisler sagen, da er ihn nicht eingestellt habe. Er räumte aber ein, dass er auch später Personen, die bereits für die kantonale Verwaltung tätig waren, anfänglich nicht sicherheitsüberprüft habe.[367] Auch laut dem Leiter LFC, Renato Widmer, war allen bewusst, dass grundsätzlich Sicherheitsüberprüfungen nötig waren.[368] Schliesslich wies der ehemalige Generalsekretär, Christian Zünd, darauf hin, dass man in der JI bei Anstellungen Sicherheitsüberprüfungen machen liess, die über die Einforderung des Strafregisterauszuges hinausgingen. Er äusserte die Vermutung, dass dieser konkrete Fall als unproblematisch eingestuft worden sei, da André Gisler als Lieferant bereits bekannt war, und deshalb keine weiteren Sicherheitsüberprüfungen veranlasst wurden.[369]

Die Weisung bezüglich Zugriffe externer Mitarbeitender[370] verlangte ab 2014 eine gleich sorgfältige Prüfung bei externen wie internen Personen und bezog alle laufenden Mandatsverhältnisse mit ein. Es scheint, als wäre die Notwendigkeit, Sicherheitsüberprüfungen auch bei laufenden Vertragsverhältnissen vorzunehmen, früher nicht auf dem Radar gewesen.

Auch für die Staatsanwaltschaft III scheinen André Gisler und dessen Mitarbeitenden nicht einer umfassenden Personenprüfung unterzogen worden zu sein.[371] Der polizeiliche Bericht kommt hierzu ergänzend zum Schluss, dass eine solche nie stattgefunden habe, da man sonst wohl auch unweigerlich auf den Bruder von André Gisler und dessen Nähe zum kriminellen Umfeld gestossen wäre.[372]

---

363 Staatsanwaltschaft Zürich-Sihl, Delegierte Einvernahme des ehemaligen Mitarbeiters vom 5. März 2021, Fragen 47, 80.

364 Staatsanwaltschaft III, Delegierte Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023, Frage 30.

365 Staatsanwaltschaft Zürich, Sihl, Einvernahme von André Gisler vom 23. Februar 2021, Frage 32.

366 Staatsanwaltschaft III, Delegierte Einvernahme eines weiteren ehemaligen Mitarbeiters vom 25. März 2023, Fragen 49–52.

367 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 10.

368 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 13.

369 Protokoll der Befragung von Christian Zünd vom 30. August 2024, S. 15–16.

370 Direktion der Justiz und des Innern, Generalsekretariat, Logistik, Finanzen & Controlling, Weisung bezüglich Zugriffe zur Informatikinfrastruktur für Mandatierte (Externe Mitarbeitende) vom 18. November 2013. In Kraft ab 1. Januar 2014.

371 Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 40.

372 Kantonspolizei, Schlussbericht zum Ermittlungsverfahren Memory vom 19. Dezember 2024, S. 39.

Kein Zugang zu Chipkarten

Gemäss dem ehemaligen Leiter der JI-Informatik, Fredi Steiner, hat André Gisler nie eine Chip- oder eine PIN-Karte und somit auch keinen Zugang zu verschlüsselten Daten erhalten.[373] Er habe aber im Jahr 2007 im Zusammenhang mit Drucker-Rollouts eine Rollouter-Karte erhalten.[374] Bis heute haben sich gemäss dem Schlussbericht der Kantonspolizei an die Staatsanwaltschaft Zürich-Sihl keine Hinweise ergeben, dass André Gisler im Besitz von Zugriffs-Smartkarten gewesen wäre.[375]

8.3.2 Kontrollmechanismen

Verpflichtung zur fachgerechten Löschung

Das vom ehemaligen Leiter der JI-Informatik, Fredi Steiner, 2020 zum Datensicherheitsvorfall verfasste Memo enthält die Ausführungen, dass André Gisler die korrekte Entsorgung der Festplatten jeweils unterzeichnen musste.[376] Diese Auskunft kann durch die PUK Datensicherheit aber nicht erhärtet werden. Gemäss seiner Aussage wies man André Gisler mündlich auf die fachgerechte Löschung hin, ohne ihm ein entsprechendes Schriftstück vorzulegen.[377] In der Befragung durch die PUK Datensicherheit meinte der Leiter der JI-Informatik, Fredi Steiner, dies habe zumindest auf dem Lieferschein oder Inventarblatt visiert werden müssen, er konnte sich jedoch nicht mehr konkret erinnern.[378]

Stichprobenkontrolle

Übereinstimmende Aussagen des ehemaligen Leiters der JI-Informatik, Fredi Steiner, sowie eines Mitarbeiters von André Gisler bestätigen, dass in Stichproben geprüft wurde, ob die Daten korrekt gelöscht worden waren.[379] Letzterer spricht jedoch von vereinzelten Kontrollen. Fredi Steiner räumte ein, dass angesichts des zeitlichen Aufwands, den ein solcher Kontrollprozess mit sich brachte, damals weder Zertifikate eingefordert noch ausreichend Kontrollen gemacht wurden. Man habe hier der Person, die schon lange für den Kanton Zürich tätig war, stark vertraut.[380]

Kontrolle der internen Prozesse

Die Einforderung der unterschriebenen Inventarblätter und deren korrekte Ablage beim Helpdesk waren gemäss dem QM-Dokument Teil des internen Audits zu den Prozessen der «Standard-Dienstleistungen». Die Helpdesk-Mitarbeiterin hatte dazu den Nachweis über die Liste der Auslieferungsbestätigungen zu erbringen.[381] Der ehemalige Leiter der JI-Informatik, Fredi Steiner, betonte in der Befragung durch die PUK Datensicherheit, dass die diesbezüglichen Anweisungen sehr ernst genommen wurden und das Inventar gewissenhaft nachgeführt worden sei.[382]

---

373 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 16.

374 Staatsanwaltschaft III, Delegierte Einvernahme eines PC-Support-Mitarbeiters vom 26. Februar 2024, Fragen 53–54.

375 Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 2.

376 Direktion der Justiz und des Innern, Generalsekretariat, DigiSol, Memo von Fredi Steiner vom 10. November 2020 «Mögliches Datenleck IT JI».

377 Staatsanwaltschaft Zürich-Sihl, Einvernahme von André Gisler vom 23. Februar 2021, Frage 85.

378 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 28.

379 Staatsanwaltschaft III, Einvernahme des ehemaligen Mitarbeiters vom 22. März 2023, Fragen 35–37.

380 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 9, 14–15.

381 Direktion der Justiz und des Innern, Generalsekretariat, Informatik, Qualitätsmanagement Einhaltung der Prozesse vom 8. April 2009, Version 4.0 vom 1. April 2016.

382 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 19.

8.3.3 Führungsstil und Persönlichkeiten

Der ehemalige Leiter LFC, Renato Widmer, wurde von verschiedenen befragten Personen als ein «Patron alter Schule» beschrieben. Gemäss dem vormaligen Leiter der JI-Informatik (1996–2000) war die Hauptabteilung mit den Bereichen Finanzen, Controlling und Logistik sehr mächtig und deren Leiter hielt die Schlüsselfaktoren in der Hand.[383]

Auf Grundlage der beigezogenen Protokolle der Staatsanwaltschaften, aber auch im Rahmen der eigenen Befragungen konnte sich die PUK Datensicherheit zum Führungsstil des Leiters LFC, Renato Widmer, ein Bild machen. Er wird als durchsetzungsstarke, unabhängige Person mit einem sehr dominanten Führungsstil und klaren Direktiven beschrieben. Er habe einerseits durch ernsthafte, gewissenhafte und qualitativ hochstehende Arbeit im Bereich der Informatik für den Kanton Zürich massgebliche Fortschritte erzielt. Andererseits galt er als intransparent. Er achtete stark auf seine Kompetenzen, schirmte den eigenen Bereich ab und duldete auch keinen Widerspruch. Es gab wenig Raum für ergebnisoffene Diskussionen und eine aktive Kommunikation.[384]

Aus den verschiedenen Befragungen geht hervor, dass der Leiter der JI-Informatik, Fredi Steiner, als loyaler Mitarbeiter dem Leiter LFC zugedient und dessen Vorgaben pflichtbewusst umgesetzt habe.[385] Gemäss der langjährigen stv. Generalsekretärin der JI, Susanna Stähelin, sei auch im Bereich der Informatik letztlich der Leiter LFC, Renato Widmer, die Person gewesen, die das Sagen gehabt habe. Auch gemäss dem Direktionscontroller lag die Führung der Informatik de facto bei Renato Widmer. Denn im Bereich der Grundausstattung habe zwar Fredi Steiner die Bedürfnisse der Benutzer abgeholt, darüber entschieden habe aber der Leiter LFC.[386] Fredi Steiner gab an, er habe trotz der ihm zugewiesenen Pflichten die operative Leitung und Verantwortung angesichts der starken Position und Einmischung von Renato Widmer gar nicht wahrnehmen können und mit seinem Team stark ausführend funktioniert. Über diese Situation seien zumindest die Mitarbeitenden des Generalsekretariats im Bild gewesen.[387] Auch der frühere Direktionsvorsteher, Martin Graf, räumte ein, dass er und der Generalsekretär erst relativ spät gemerkt hätten, dass sich der damalige Leiter der JI-Informatik, Fredi Steiner, gegenüber dem Leiter LFC, Renato Widmer, zu wenig durchsetzen konnte und zuweilen «etwas unter die Räder geriet».[388]

---

[383] Staatsanwaltschaft III, Delegierte Einvernahme des Leiters der JI-Informatik (1996–2000) vom 19. Juli 2023.

[384] Staatsanwaltschaft Zürich-Sihl, Delegierte Einvernahme von Erika W. vom 23. November 2020, Frage 26; Staatsanwaltschaft III, Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023, Fragen 20, 61; Staatsanwaltschaft III, Delegierte Einvernahme des ehemaligen Leiters des Data-Centers vom 14. August 2023, Fragen 30–32, 36; Staatsanwaltschaft III, Delegierte Einvernahme des Direktionscontrollers vom 18. August 2023, Frage 36; Staatsanwaltschaft III, Delegierte Einvernahme des Projektleiters SAP der Digital Solutions vom 21. Juli 2023, Frage 33; Staatsanwaltschaft III, Delegierte Einvernahme des Projektleiters der Digital Solutions vom 20. März 2024, Frage 20–21; Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 18–20; Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 17–18, 20; Protokoll der Befragung von Christian Zünd vom 30. August 2024, S. 10–11, 13; Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 7, 12; Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 19.

[385] Protokoll der Befragung von Christian Zünd vom 30. August 2024, S. 13; Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 12; Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 8–9.

[386] Staatsanwaltschaft III, Delegierte Einvernahme des Direktionscontrollers vom 18. August 2023, Frage 83.

[387] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 27.

[388] Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 19.

Einmischung in das operative Geschäft

Trotz der räumlichen Trennung mit der Informatik im Bezirksgebäude und dem Generalsekretariat im Kaspar-Escher-Haus sei der Leiter LFC, Renato Widmer, laut dem Leiter der JI-Informatik, Fredi Steiner, stark in das operative Geschäft involviert gewesen und habe sich zeitweise wie der Chef der Abteilung verhalten.[389] Er sei teilweise direkt zu den Mitarbeitenden gegangen und habe diesen gesagt, was zu tun sei.[390] Das eigentlich dem operativen Bereich zugeordnete Inventar sei beispielsweise eher in der Obhut des Leiters LFC gewesen, da dieser es für die Verrechnung benötigt habe. Auch die eigentlich ihm, als Leiter JI-Informatik, unterstellte JI-Mitarbeiterin, Erika W., habe sich direkt an den Leiter LFC gewandt und dessen Weisungen umgesetzt.[391] Auch im Personalbereich habe der Leiter LFC das letzte Wort gehabt und sicherlich anfangs auch die Verfügungen unterschrieben.[392] Auch wenn der Leiter der JI-Informatik Personen kündigen wollte, habe er die Autorität des Leiters LFC zu spüren bekommen.[393] Der Leiter LFC räumte in der Befragung gegenüber der PUK Datensicherheit ein, dass er im Bereich der Applikationsentwicklung sowie bei der potenziellen Anstellung von fachlich ungenügendem Personal interveniert habe.[394]

8.3.4 Begleitung durch Generalsekretariat und Direktionsvorsteher der JI

In der Befragung durch die PUK Datensicherheit führte der frühere Direktionsvorsteher der JI, Markus Notter, aus, dass für ihn die Entsorgung von Datenträgern im Konkreten kein Thema war und er diese auch nicht verfolgt oder durch den Generalsekretär habe prüfen lassen. Er sei davon ausgegangen, dass die Entsorgung verordnungskonform umgesetzt werde.[395] Auch sein Nachfolger Martin Graf ging davon aus, dass die Entsorgung über ein professionelles Unternehmen ablaufe.[396] Was genau passierte, wenn die Hardware nicht mehr in den Büros war, war auch aus Sicht des Kommunikationsbeauftragten, Benjamin Tommer, der seit 2011 im Generalsekretariat tätig ist, kein Thema, das über die direkt beteiligten Fachleute hinaus gross interessiert hätte.[397]

Allgemeine Fragen zur Informationssicherheit und der diesbezüglichen Compliance hätten jedoch alle Vorsteherinnen und Vorsteher der JI ernst genommen, so der ehemalige Generalsekretär, Christian Zünd, und sie hätten sich auch darum gekümmert.[398] So gab beispielsweise der frühere Direktionsvorsteher, Markus Notter, an, 2003 zur Sicherheitslösung der Direktion und 2008 zur anstehenden Erneuerung des Rechtsinformationssystems externe Gutachten eingeholt zu haben. Weiter habe er die Finanzkontrolle gebeten, den Informatikbereich aufgrund der diesbezüglichen Risiken genau anzuschauen. Im Zeitraum 2001–2011 legte die Finanzkontrolle fünf Berichte mit

---

389 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 7.

390 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 19.

391 Staatsanwaltschaft III, Delegierte Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023, Frage 85.

392 Staatsanwaltschaft III, Delegierte Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023, Frage 20.

393 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 19.

394 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 14, 23.

395 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 21, 29.

396 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 29.

397 Protokoll der Befragung von Benjamin Tommer vom 27. September 2024, S. 8.

398 Protokoll der Befragung von Christian Zünd vom 30. August 2024, S. 19.

Konnex zur JI-Informatik vor. Die damaligen Feststellungen betrafen die Applikationen der Buchhaltung und der Arbeitszeiterfassung sowie die Anlagenverzeichnisse und Inventare der Informatik.[399]

Zu den grösseren IT-Beschaffungen der JI liegen Regierungsratsbeschlüsse vor. Der Leiter LFC bereitete diese Anträge vor.[400] Gemäss dem ehemaligen Generalsekretär, Christian Zünd, haben er und der Direktionsvorsteher diese Beschaffungen jeweils genau angeschaut.[401] Mit der Entsorgung von Geräten hatte er gemäss eigenen Angaben hingegen nichts zu tun, da diese in der Finanzkompetenz seiner Unterstellten lag. Der Leiter LFC habe darauf geachtet, Entscheide in seinem eigenen Kompetenzbereich selbst zu fällen und umzusetzen und diese dem Generalsekretär nicht vorzulegen. Der Generalsekretär sei seiner Sorgfaltspflicht aber nachgekommen, indem er die Kompetenzen in einem Organisationsreglement geregelt, qualifiziertes Personal ausgewählt und Pflichtenhefte erstellt habe. Zudem seien die Personen entsprechend instruiert worden. Auch er sei davon ausgegangen, dass die Entsorgung von Geräten fachgerecht abgewickelt werde.[402] Die diesbezügliche Verantwortung lag seiner Ansicht nach beim Hauptabteilungsleiter, Renato Widmer, und dem Abteilungsleiter, Fredi Steiner. Zwar habe er nach eigener Einschätzung den Leiter LFC enger geführt als sein Vorgänger, er habe sich aber auch darauf verlassen, dass seine Unterstellten korrekt vorgehen und allfällige Probleme an ihn herantragen würden. Grundsätzlich habe das gut funktioniert. Im konkreten Fall habe der Leiter LFC das Problem scheinbar selbst nicht erkannt.[403] Auch aus Sicht des ehemaligen Direktionsvorstehers, Markus Notter, hat das Generalsekretariat, inklusive der Hauptabteilung LFC, gut funktioniert. Die Informatikabteilung selbst hatte gemäss dem ehemaligen Leiter der JI-Informatik jedoch wenig direkten Kontakt zum Generalsekretär, da die Kommunikation über den Leiter LFC kanalisiert wurde.[404]

Die heutige Generalsekretärin, Jacqueline Romer, erhielt bei ihrem Stellenantritt den Eindruck, dass sich die JI-Informatik weit weg vom Generalsekretariat und vom Management befand und von diesem zu wenig erfasst wurde.[405] Auch der ehemalige Direktionsvorsteher, Martin Graf, hält es rückblickend für möglich, dass sie als Vorgesetzte damals zu wenig Informationen darüber hatten, was in der Informatik genau lief.[406] Dies, aber auch den Umstand, dass das Generalsekretariat noch stärker juristisch geprägt war, hat der Leiter LFC gemäss der heutigen stv. Generalsekretärin auch etwas zu seinen Gunsten genutzt.[407] Die heutige Generalsekretärin, Jacqueline Romer, hat gemäss eigenen Aussagen die Schwerpunkte gegenüber früher etwas anders gesetzt und den Fokus stärker auf Managementfragen gelegt. Diese hätten mit der wachsenden Digitalisierung im Zeitverlauf natürlich auch an Bedeutung gewonnen.[408]

---

399 Finanzkontrolle Kanton Zürich, Bericht vom 17. April 2001 über die EDV-Revision 2001 bei der Direkk tion der Justiz und des Innern (Logistik, Finanzen, Controlling); Finanzkontrolle Kanton Zürich, Auszug aus dem Bericht vom 18. Juli 2003; Finanzkontrolle Kanton Zürich, Auszug aus dem Bericht vom 14. Oktober 2003.

400 Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 15.

401 Protokoll der Befragung von Christian Zünd vom 30. August 2024, S. 18.

402 Protokoll der Befragung von Christian Zünd vom 30. August 2024, S. 8–11.

403 Protokoll der Befragung von Christian Zünd vom 30. August 2024, S. 13, 15–16.

404 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 7.

405 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 17.

406 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 20.

407 Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 7.

408 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 17.

8.4 Erneuerung der PC-Arbeitsplätze

Vor dem 2021 erfolgten Rollout des digitalen Arbeitsplatzes (DAP) durch das Amt für Informatik (AFI) waren die PC-Arbeitsplätze in der Direktion der Justiz und des Innern (JI) seit der Jahrtausendwende viermal umfassend erneuert worden. In den Jahren davor waren die Beschaffungen tranchenweise erfolgt. Tabelle 15 enthält für die vier Beschaffungen den jeweiligen Regierungsratsbeschluss und die Anzahl ausgetauschter Geräte.

Tabelle 15 Übersicht zu den IT-Ersatzbeschaffungen der JI

RRB Nr. 880/2001[409]	Ersatz der PC-Arbeitsplätze	1300 Geräte
RRB Nr. 390/2005[410]	Ersatz von PC und Bildschirmen	1440 Geräte
RRB Nr. 1917/2009[411]	Ersatz von PC und Bildschirmen	1550 Geräte
RRB Nr. 387/2016[412]	Ersatzbeschaffung von Hard- und Software, gebundene Ausgabe	1850 Geräte

Die von der Staatsanwaltschaft beigezogenen Akten enthielten auch Unterlagen zu diesen Beschaffungen. In Ergänzung zu den Befragungen und den Akten der JI konnte die PUK Datensicherheit so ein Bild über die damaligen Abläufe gewinnen. Gemäss den Abklärungen der Staatsanwaltschaft könnten im Rahmen der Rollouts Daten auf die Netboxen gelangt sein, da die Mitarbeitenden des PC-Supports Daten der Endgeräte auf den Netboxen zwischengespeichert hätten, um sie dann wieder zurückzuspielen.[413]

Gemäss dem ehemaligen Leiter LFC, Renato Widmer, war bei solchen Umstellungsprojekten der damalige Leiter der JI-Informatik für die Projektleitung zuständig.[414] Nachdem ein Regierungsratsantrag gutgeheissen worden war, ging das Projekt laut dem ehemaligen Leiter LFC jeweils an den ehemaligen Leiter der JI-Informatik, Fredi Steiner, der dann die Ausschreibung durchführte und den Projektplan ausarbeitete.[415] Zumindest bei der Serverbeschaffung war dies gemäss der Wahrnehmung des ehemaligen Leiters des Data-Centers nicht so. Auch wenn der ehemalige Leiter der JI-Informatik die Verhandlungen geführt habe, sei der Entscheid beim Leiter LFC gelegen.[416]

8.4.1 Beschaffung 2001

In den Ausschreibungsunterlagen aus dem Jahr 2001 zur Ersatzbeschaffung von 1200 Geräten wird der ehemalige Leiter der JI-Informatik, Fredi Steiner, als Kontaktperson angegeben.[417] Es gab ein Pflichtenheft und die Offerte sollte auf den Allgemeinen Geschäftsbedingungen der Schweizerischen Informatikkonferenz (AGB SIK) basieren. Aus dem Submissionsergebnis vom 26. Oktober 2001 geht hervor, dass der Auftrag,

[409] RRB Nr. 880/2001 vom 13. Juni 2001, Ersatz der PC-Arbeitsplätze.

[410] RRB Nr. 390/2005 vom 16. März 2005, Ersatz von PC und Bildschirmen.

[411] RRB Nr. 1917/2009 vom 25. November 2009, Direktion der Justiz und des Innern (Ersatz von PC und Bildschirmen).

[412] RRB Nr. 387/2016 vom 20. April 2016, Ersatzbeschaffung von Hard- und Software, gebundene Ausgabe.

[413] Staatsanwaltschaft III, Delegierte Einvernahme des ehemaligen Leiters des Data-Centers vom 14. August 2023, Frage 102.

[414] Staatsanwaltschaft III, Delegierte Einvernahme von Renato Widmer vom 28. Juni 2023, Fragen 12, 36–37.

[415] Protokoll der Befragung von Renato Widmer vom 6. September 2024, S. 9.

[416] Staatsanwaltschaft III, Delegierte Einvernahme des ehemaligen Leiters des Data-Centers vom 14. August 2023, Frage 73.

[417] Direktion der Justiz und des Innern, Logistik, Finanzen & Controlling, Abteilung Informatik, Ausschreibungsunterlagen PC-Ersatzbeschaffung.

1300 Geräte zu ersetzen, an ein etabliertes IT-Unternehmen ging.[418] Gemäss den Abklärungen der Staatsanwaltschaft III liegen keine Dokumente vor, welche die Entsorgung der ersetzten Geräte belegen resp. aufzeigen, wer dafür verantwortlich war.[419]

8.4.2 Beschaffung 2005

Die Ausschreibung im GATT/WTO-Verfahren führten der Leiter LFC und der Leiter der JI-Informatik gemeinsam und unter Beizug eines Beratungsunternehmens durch. Der Leiter LFC war dabei Auftraggeber und der Leiter der JI-Informatik Projektleiter.[420]

Das Pflichtenheft zur Ausschreibung hielt die Vorgaben des Auftragnehmers fest. Der Aspekt der Entsorgung der Geräte war darin – im Gegensatz zur Entsorgung des Verpackungsmaterials – nicht adressiert.[421] Der Zuschlag für die Lieferung von 1400 Desktop-Computern ging am 28. Juni 2005 an dasselbe Unternehmen wie schon 2001.[422]

Laut dem ehemaligen Leiter der JI-Informatik wurden Entsorgung und Löschung nicht über die Lieferanten der neuen Geräte abgewickelt, sondern man arbeitete bereits mit professionellen Brokern zusammen, wobei man für die Entsorgung der Geräte und deren Wiederverkauf Geld erhalten habe. Mit Blick auf die Entsorgung der 2005 ersetzten Geräte räumte er jedoch ein, dass er nicht mehr genau wisse, wie diese entsorgt worden seien.[423] Die Staatsanwaltschaft III geht schliesslich davon aus, dass hier keine Dokumente vorliegen, welche die Entsorgung belegen würden.[424] Aus dem IT-Inventar geht hervor, dass im Jahr 2005 1450 Geräte entsorgt wurden.[425]

8.4.3 Beschaffung 2010

Der Leiter der JI-Informatik fungierte auch bei der Beschaffung 2010 als Kontaktperson.[426] Die Beschaffung wurde jedoch gemeinsam mit der Baudirektion (BD) realisiert und über die Kantonale Drucksachen- und Materialzentrale (kdmz) abgewickelt. Die Entsorgung der ersetzten Geräte war auch im Pflichtenheft zur gemeinsamen Ausschreibung der BD und der JI kein Thema.[427] Der Zuschlag wurde am 31. Mai 2010 erteilt[428] und die JI konnte die Bestellung von 1535 Geräten auslösen.[429] Die 2005 beschafften Geräte gingen durch einen regulären Entsorgungsprozess und wurden über einen Broker entsorgt. Nach internen Diskussionen über die Entsorgungskosten wickelte man diese Entsorgung erstmals institutionalisiert ab und verlangte auch Zerti-

---

418 Direktion der Justiz und des Innern, Logistik, Finanzen & Controlling, Abteilung Informatik, Submissions-Ergebnis PC-Ersatzbeschaffung vom 26. Oktober 2001.

419 Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 21.

420 Staatsanwaltschaft III, Delegierte Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023, Fragen 68–69.

421 Direktion der Justiz und des Innern, Logistik, Finanzen & Controlling, Abteilung Informatik, Pflichtenheft Beschaffung Desktop Computer inkl. Bildschirm, Maus und Tastatur vom 15. April 2005.

422 Direktion der Justiz und des Innern, Beschaffung Desktop Computer Submissionsergebnis Los Computer vom 28. Juni 2005.

423 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 17.

424 Kantonspolizei, Schlussbericht zum Ermittlungsverfahren Memory vom 19. Dezember 2024, S. 18.

425 Direktion der Justiz und des Innern, IT-Inventar Übersicht vom 11. März 2023.

426 Direktion der Justiz und des Innern, Logistik, Finanzen & Controlling, Pflichtenheft Beschaffung Desktop-Computer inkl. Maus und Tastatur vom 3. März 2010.

427 kdmz, Beschaffung Desktop-Computer inkl. Monitor, Notebook, Maus und Tastatur für die Direktionen Bau und Justiz vom 29. März 2010.

428 Simap-Meldungs-Nr. 497837, Projekt: 38813 – Beschaffung Desktop-Computer inkl. Monitor, Maus und Tastatur für die Direktionen Bau und Justiz.

429 Direktion der Justiz und des Innern, Logistik, Finanzen &Controlling, Schreiben «Bestellung von Hardware gem. GATT/WTO-Submission» vom 28. Juni 2010.

fikate des Brokers.[430] Die PUK Datensicherheit konnte diese Zertifikate einsehen. Aus der Inventarübersicht geht hervor, dass im Jahr 2010 insgesamt 2649 Geräte ausgemustert wurden, wofür heute noch 2385 Löschzertifikate vorliegen. André Gisler war folglich nicht in diesen Entsorgungsprozess involviert.

Die Staatsanwaltschaft III kommt zum Schluss, dass davon ausgegangen werden kann, dass André Gisler bzw. die AG Transporte (rund) 2700 Computer (2001: 1300 Geräte, 2005: 1400 Geräte) von der JI zur Löschung, Aufbereitung und Entsorgung erhalten haben könnte.[431]

8.5 Entsorgungen mit dokumentierter Beteiligung des externen Dienstleisters

Gemäss der Aussage der direkt beteiligten JI-Mitarbeiterin, Erika W., hat der Dienstleister André Gisler bei grossen PC-Rollouts, mit Ausnahme der Erneuerung der Netboxen 2011/2012, keine Aufträge übernommen. Die Entsorgung übernahmen die im Rahmen des Projekts beauftragten spezialisierten Firmen.[432] Neben diesen Geräten, die im Rahmen der grossen Erneuerungszyklen ausgetauscht wurden, gab es gemäss dem ehemaligen Leiter der JI-Informatik auch kleinere Tranchen von Geräten, die ausgetauscht wurden. Diese Geräte, die beispielsweise liegengeblieben waren, seien jedoch vor ihrer Abgabe durch einen internen Löschprozess gegangen. Wegen Ressourcenmangels waren jedoch nur Stichprobenkontrollen möglich, womit nicht klar ist, ob alle Geräte auf diese Weise gelöscht wurden.[433]

Im Rahmen ihrer Ermittlungen zur IT-Infrastruktur der JI konnte die Staatsanwaltschaft III auf Basis der Dokumenteneingaben sowie der forensischen Auswertung des Laufwerks der Digital Solutions feststellen, dass (mindestens) 337 Speicherkomponenten zur Entsorgung an den Dienstleister André Gisler gegangen waren. Es blieben aber erhebliche Zweifel an der Vollständigkeit dieser Aufstellung bestehen.[434] Tabelle 16 fasst die Informationen zusammen, welche die Staatsanwaltschaft III im Rahmen ihrer Befragungen[435], gestützt auf beigebrachte Geräte-Listen, zusammentrug.

---

[430] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 13–14, 17–18.

[431] Kantonspolizei, Schlussbericht zum Ermittlungsverfahren Memory vom 19. Dezember 2024, S. 36.

[432] Staatsanwaltschaft Zürich-Sihl, Delegierte Einvernahme von Erika W. vom 23. November 2020, Fragen 30, 44, 52.

[433] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 14.

[434] Staatsanwaltschaft III, Einstellungsverfügung vom 8. September 2025, S. 16; Kantonspolizei, Ermittlungsbericht IT-Infrastruktur der Digital Solution (DigiSol) mit Schwerpunkt Entsorgung Hardware vom 10. Juni 2024, S. 28.

[435] U. a. mit den Befragungen des heutigen ICT-Security-Architekten: Staatsanwaltschaft III, Erste delegierte Einvernahme des ICT-Security-Architekten vom 15. Mai 2023, zweite delegierte Einvernahme des ICT-Security-Architekten vom 15. Juni 2023.

Tabelle 16 Übersicht zu Speicherkomponenten mit Entsorgungsbeteiligung von André Gisler

Art der Speicherkomponente	Zeitraum	Anzahl Geräte	Belege
Netboxen	Juni 2005	56	SN A40
PC-Geräte der Gefängnisse und Arbeitserziehungsanstalten	November 2005 und Februar/ März 2006	51	Excel-Liste ‹PC GF›, Mappen ‹M41 BS15› (3a) und ‹M41 BS15 2› (3b)
PC-Geräte der Staatsanwaltschaften und weiterer Amtsstellen	Januar 2006 Februar 2006	34	Color DR
Laptops	November 2006	76	Laptop Kauf / ZUFATP
Server	2007	35	ZUFAPC
PC-Geräte der Statthalterämter	2011/2012	85	A. Gisler Entsorgung
Anzahl Speicherkomponenten		***337***	

8.5.1 Beteiligung am Rollout der Netboxen

Gemäss dem früheren Leiter des Data-Centers fand die Erneuerung der Netboxen jeweils im 5-Jahres-Rhythmus statt, wobei André Gisler wohl ab 2007 oder allenfalls auch früher die alten durch die neuen Netboxen ersetzt hatte und mit der Entsorgung der alten Geräte beauftragt worden war. In der Wahrnehmung des ehemaligen Leiters des Data-Centers hatte der Leiter der JI-Informatik diesen Auftrag «im Sinne» des Leiters LFC erteilt.[436] Laut dem Leiter der JI-Informatik, Fredi Steiner, zog André Gisler die Netboxen ein. Er konnte sich aber nicht erinnern, inwieweit die Geräte André Gisler auch zur Entsorgung oder als Gegenleistung für seine Arbeit übergeben worden waren.[437]

Aus den der PUK Datensicherheit vorliegenden Arbeitsrapporten geht hervor, dass André Gisler nicht nur 2005, sondern auch 2012 in den Austausch von Netboxen involviert war. Gemäss eigenen Angaben erhielt er jeweils von der direkt beteiligten JI-Mitarbeiterin, Erika W., Zettel mit Aufträgen, wo welche Geräte auszutauschen waren. Er gab an, die Harddisks dann durchbohrt und entsorgt zu haben.[438] Ihm sei jedoch nicht bewusst gewesen, dass die Netboxen Daten speicherten und damit heikel sein konnten.[439]

8.5.2 Rollout der Geräte der Statthalterämter 2011/2012

Der Regierungsrat beschloss mit RRB Nr. 766/2011 auf Antrag der Direktion der Justiz und des Innern sowie der Sicherheitsdirektion, die Zuständigkeitsbereiche anzupassen. Auf den 1. Januar 2012 übernahm die JI die Aufsicht über die zwölf Statthalterämter und die Sicherheitsdirektion wurde für die Gebäudeversicherung zuständig.[440] Damit verbunden war die Übertragung der von den Statthalterämtern eingesetzten Hardware. 85 Computer kamen so von der Sicherheitsdirektion zur JI.

---

436 Staatsanwaltschaft III, Delegierte Einvernahme des ehemaligen Leiters des Data-Centers vom 14. August 2023, Fragen 84–113.

437 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 16.

438 Staatsanwaltschaft III, Einvernahme von André Gisler vom 23. Februar 2023, Fragen 53–59, 65.

439 Staatsanwaltschaft III, Einvernahme von André Gisler vom 24. Januar 2023, Frage 124.

440 RRB Nr. 766/2011 vom 15. Juni 2011, Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung (Änderung). Verordnung über die Gebühren, Auslagen und Entschädigungen der Strafverfolgungsbehörden (Änderung).

Gemäss dem Protokoll der Projektgruppe zur Angliederung der Statthalterämter an die JI war die Verantwortung für die Rollout-Vorbereitung und damit auch die Rücknahme und den Verkauf der alten Hardware u. a. dem Abteilungsleiter der JI-Informatik und der Helpdesk-Mitarbeiterin zugewiesen worden.[441]

Der damalige Direktionsvorsteher, Martin Graf, kann sich vorstellen, dass man bei der Übernahme dieser Geräte einen Fehler gemacht hat, da man davon ausging, dass sie in derselben Art verschlüsselt waren wie die Geräte der JI.[442] Der heutige ICT-Security-Architekt schätzte es in einer ersten Befragung so ein, dass auf den übertragenen Geräten keine Verschlüsselung aktiv war, weshalb die Daten auf diesen Clients gelesen werden konnten.[443] Gestützt auf die Aussagen und Eingaben des damaligen Informatikverantwortlichen der Sicherheitsdirektion kommt die Kantonspolizei gegenüber der Staatsanwaltschaft III jedoch zum Schluss, dass die Statthalterämter-Endgeräte seit Oktober 2008 über dieselbe Verschlüsselungslösung (bzw. Nicht-Verschlüsselung in Temporär- und Downloadverzeichnissen sowie Backup-Programmen) wie die Justizdirektion verfügten. Sie nimmt weiter an, dass im Zuge des Wechsels unverschlüsselte Daten der Statthalterämter den Weg in die JI und damit zu André Gisler fanden.[444]

Der Dienstleister André Gisler gab an, dass er die Geräte der Statthalterämter erhalten habe. Es habe sich um die letzten Geräte gehandelt, die er bekommen habe. Da er seinen Laden zu diesem Zeitpunkt bereits aufgelöst hatte, habe er die Geräte bei sich zu Hause gelagert, wobei es sich um sehr viel Material gehandelt habe. Da sein damaliger Mitarbeiter die Geräte nicht gelöscht habe, habe er sie physisch mit Durchbohren zerstört und zu einem Entsorgungsdienstleister gebracht. Als er sein Haus verkaufen wollte, begann er dieses im Jahr 2014 zu räumen.[445]

Nach der Einschätzung der beteiligten Staatsanwälte der Staatsanwaltschaft III ist André Gisler die Sache angesichts der Menge der zu entsorgenden Geräte, des fehlenden Platzes oder des zeitlichen Aufwands solcher Löschungen über den Kopf gewachsen. Deshalb konnte er schliesslich eine gewisse Anzahl Datenträger nicht mehr neu aufbereiten.[446]

8.5.3 Räumung des RIS-Entwicklungsbüros 2013

Aus einem Arbeitsrapport von André Gisler geht hervor, dass er im Mai 2013 auch beim Umzug des RIS-Entwicklungsbüros beteiligt war.[447] Gemäss eigenen Angaben war er beigezogen worden, um das Büro am Stauffacher zu räumen (siehe auch Kapitel 7.2.3). Dabei habe er drei Kisten mit physischen Akten erhalten und diese dann, da er auch für die PC-Löschung eine Karenzfrist abwarten musste, in seinen Keller gestellt.[448] Da er üblicherweise keine Papierdokumente erhalten habe, fiel dies auch seinem ehemaligen Mitarbeiter auf. Dieser bestätigte diesen Ablauf.[449] Die Kisten

---

441 Direktion der Justiz und des Innern, Generalsekretariat, Logistik, Finanzen &Controlling, Abteilung Informatik, Angliederung der Statthalterämter an die JI, Protokoll und Pendenzenliste der Projektgruppe «Informatik», Sitzung vom 9. November 2011.

442 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 30.

443 Staatsanwaltschaft III, Erste delegierte Einvernahme des ICT-Security-Architekten vom 15. Mai 2023, Frage 77.

444 Kantonspolizei, Schlussbericht zum Ermittlungsverfahren Memory vom 19. Dezember 2024, S. 9, 37.

445 Staatsanwaltschaft III, Einvernahme von André Gisler vom 24. Januar 2023, Fragen 77–82, 90–93.

446 Protokoll der Befragung von David Zogg und Mathias Eberli vom 3. Mai 2024, S. 18.

447 Staatsanwaltschaft Zürich-Sihl, Delegierte Einvernahme von Erika W. vom 23. November 2020, Frage 67.

448 Staatsanwaltschaft III, Einvernahme von André Gisler vom 24. Januar 2023, Fragen 103–106.

449 Staatsanwaltschaft III, Einvernahme des ehemaligen Mitarbeiters vom 22. März 2023, Fragen 51–54.

wurden aber nicht entsorgt und gerieten daher wohl in die Hände des Bruders von André Gisler. Für die Staatsanwaltschaft ist einigermassen glaubhaft, dass die Unterlagen aus dem Entwicklungsbüro auf diese Weise an den Bruder gelangt sind.[450] Im Dezember 2022 tauchte dieser dann mit den Unterlagen in den Räumlichkeiten des Kantonsrates auf.

8.6 Feststellungen der Finanzkontrolle 2014

8.6.1 Berichte der Finanzkontrolle

Die Finanzkontrolle hat für den fraglichen Zeitraum relevante Beobachtungen gemacht und Mängel mit Bezug zur JI-Informatik festgestellt. Die Geschäftsbeziehung von André Gisler oder seiner AG Transporte mit der JI war jedoch nie expliziter Gegenstand der Prüfungstätigkeit der Finanzkontrolle.[451]

Bereits bei den IT-Kurzchecks in den Direktionen im Rahmen der Prüfung der kantonalen IT identifizierte die Finanzkontrolle 2012 das Selbstverständnis der IT-Zuständigen, die sich selbst sehr positiv einschätzten, als mögliches Risiko.[452]

Als Anfang 2014 Bestechungsvorwürfe bei IT-Vergaben im Staatssekretariat für Wirtschaft (SECO) bekannt wurden, erteilte der damalige Direktionsvorsteher, Martin Graf, der Finanzkontrolle den Auftrag, auch die Geschäftsbeziehungen der JI zum involvierten Unternehmen zu untersuchen.[453] Es ging darum, das Umfeld der Auftragsvergaben an das im Fokus stehende Unternehmen sowie deren Umgebung unter submissions- und finanzrechtlichen Aspekten zu prüfen.

Seit Mitte Februar 2014 hatte auch die Staatsanwaltschaft III im Zusammenhang mit den IT-Vergaben Ermittlungen wegen möglicher Bestechung und Annahme von Geschenken (Vorteilsnahme) unternommen.[454] Von den Ermittlungen war ein JI-Mitarbeiter betroffen. Im Rahmen ihrer Abklärungen hat die PUK Datensicherheit den diesbezüglichen Strafbefehl sowie die Einstellungsverfügung beigezogen.

In ihrem Sonderbericht vom 20. März 2014 wies die Finanzkontrolle darauf hin, dass die obersten Verantwortlichen im IT-Bereich, namentlich der Leiter LFC, Renato Widmer, sehr unabhängig agieren konnten.[455] Den Umstand, dass der Leiter LFC, als Hauptverantwortlicher für den IT-Betrieb und die IT-Beschaffung, die Strategie beeinflusste, IT-Beschaffungen auslöste und auch die Verantwortung für die Finanzen und das Controlling trug, beurteilte die Finanzkontrolle als erhebliches Risiko hinsichtlich der Compliance und der Korruption, zumal in der damaligen Situation ohne Vertragsmanagement und ohne klare Dokumentation der Entscheidungsfindung keine Transparenz herrschte. Sie empfahl in ihrem Bericht, dem Compliance Management besondere Aufmerksamkeit zu schenken sowie die organisatorische Struktur und das Dokumenten- und Vertragsmanagement zu überprüfen.[456] Die Finanzkontrolle wies also darauf hin, dass Anpassungen dringend notwendig seien, um die IT-Führung zu verbessern und besser zu überwachen.

---

[450] Protokoll der Befragung von Mathias Eberli vom 31. Januar 2025, S. 10.

[451] Finanzkontrolle Kanton Zürich, Aktennotiz «Datenleck Justizdirektion» vom 7. Dezember 2022.

[452] Finanzkontrolle Kanton Zürich, Kurz-Check Justiz und Inneres (JI), Protokollarische Zusammenfassung der Arbeitsschritte und Erkenntnisse, 23. Januar 2012.

[453] SRF, Korruptionsaffäre beim Bund: Auch Kanton Zürich klärt ab, 31. Januar 2014.

[454] Oberstaatsanwaltschaft, Medienmitteilung vom 20. März 2014 «Strafverfahren im Zusammenhang mit IT-Vergaben auch im Kanton Zürich».

[455] Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 18.

[456] Finanzkontrolle Kanton Zürich, Bericht zum Prüfauftrag der Direktion der Justiz und des Innern über IT Beschaffung und Unterhalt vom 20. März 2014, S. 23–25.

Im Anschluss an die erste Prüfung untersuchte die Finanzkontrolle weitere IT-Beschaffungen und Geschäftsbeziehungen der Jahre 2011–2014. Im Dezember 2014 legte sie ihren Bericht[457] vor und nahm diesen auch in die nächste Semesterberichterstattung auf. Die Finanzkontrolle stellte fest, dass die Beurteilung, welche der Leiter LFC im Rahmen des IT-Kurzchecks u. a. bezüglich Compliance, Outsourcing, Funktionentrennung, Vertragsmanagement und Vergaberecht abgegeben hatte, in erheblichem Widerspruch zum vorgefundenen Zustand stehe.

Dazu finden sich im Semesterbericht 2014 folgende Feststellungen:

– «Von Bedeutung erscheint darüber hinaus, dass die im Rahmen der Prüfung von den Verantwortlichen geltend gemachten Sachverhaltsdarstellungen und Einwände von einer Herangehensweise zeugen, welche hinsichtlich Sorgfaltspflicht und Rechtsauffassung erhebliche Fragen aufwirft.»
– «Nach Einschätzung der Finanzkontrolle führen die Art der Aktenführung, das Fehlen von Kreditkontrollen und die Intransparenz der Geschäftsabwicklung insgesamt dazu, dass eine genügende Aufsicht nicht mehr möglich ist.»[458]
– «Vor beschriebenem Hintergrund ist die Finanzkontrolle der Auffassung, dass die Hauptforderung gegenüber den Verantwortlichen der DJI [Direktion der Justiz und des Innern] darin bestehen muss, im Umfeld des Beschaffungswesens, insbesondere im Bereich IT-Einkauf, ein grundsätzliches Umdenken herbeizuführen.»[459]

Aus der damals in der Berichterstattung aufgezeigten Stimmung und den grundlegenden organisatorischen Mängeln lasse sich nach Ansicht der Finanzkontrolle auch in Bezug auf die Informationssicherheit einiges ableiten.[460] Die Forderung der Finanzkontrolle, dass im IT-Beschaffungswesen ein Umdenken herbeizuführen sei, nehme die damalige Atmosphäre in der Abteilung auf. Auch heute noch kommt die Finanzkontrolle zum Schluss, dass die damals herrschende Stimmung eine Situation begünstigt habe, in der es zu einem Datensicherheitsvorfall kommen konnte.[461]

Der zweite Bericht vom 18. Dezember 2014 hält dazu folgende Empfehlung fest:

– «Vor beschriebenem Hintergrund ist die Finanzkontrolle der Auffassung, dass die Hauptforderung gegenüber den Verantwortlichen DJI darin bestehen muss, im Umfeld des Beschaffungswesens, insbesondere im Bereich IT-Einkauf, ein grundsätzliches Umdenken herbeizuführen. Diese Forderung bedingt einen Kulturwandel, welcher von höchster Stelle ausgelöst werden muss und sämtliche relevanten Stellen einbindet.»[462]

Dieses Bild der Situation stimmt mit den Eindrücken bezüglich Intransparenz und fehlender Dokumentation sowie mangelnder vertraglicher Abmachungen überein, die sich die PUK Datensicherheit auf Grundlage der eigenen Befragungen sowie der Kenntnisnahme der Unterlagen der Staatsanwaltschaft, namentlich der Einvernahmeprotokolle, machen konnte. Aufgrund der gut ausgebauten technischen Sicherheit bestand wohl das Gefühl, im Bereich der Informationssicherheit allgemein gut aufgestellt zu sein.

---

457 Finanzkontrolle Kanton Zürich, Bericht zur Vertiefungsprüfung bei der Direktion der Justiz und des Innern, Generalsekretariat: IT-Beschaffungen vom 18. Dezember 2014.

458 Finanzkontrolle Kanton Zürich, Bericht der Finanzkontrolle über ihre Prüftätigkeit im zweiten Semester 2014 vom 11. März 2015, S. 22.

459 Finanzkontrolle Kanton Zürich, Bericht der Finanzkontrolle über ihre Prüftätigkeit im zweiten Semester 2014 vom 11. März 2015, S. 25.

460 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 8.

461 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 20.

462 Finanzkontrolle Kanton Zürich, Bericht zur Vertiefungsprüfung bei der Direktion der Justiz und des Innern, Generalsekretariat: IT-Beschaffungen vom 18. Dezember 2014, S. 42.

8.6.2 Massnahmen der JI

Die Berichte der Finanzkontrolle wurden dem Direktionsvorsteher und dem Generalsekretär zur Kenntnis gebracht. Im Generalsekretariat befasste man sich in der Folge intensiv damit und war klar der Meinung, dass Kompetenzen überschritten wurden und auch die ungenügende Aktenführung nicht akzeptabel sei.[463] Massnahmen personeller und organisatorischer Art wurden bereits ab Mai 2014 umgesetzt.

Aufteilung der Hauptabteilung Logistik, Finanzen & Controlling (LFC)

Der ehemalige Leiter LFC, Renato Widmer, trat im Januar 2015 frühzeitig von seiner Funktion zurück. Fredi Steiner übernahm anschliessend während einer Übergangsphase bis 2016 dessen Funktion als Gesamtleiter der JI-Informatik.[464]

Die Anhäufung von Funktionen in der Hauptabteilung LFC, in der die Bereiche Logistik, Finanzen, Controlling und Informatik beim Leiter LFC zusammenkamen, wurde aufgebrochen. Noch im Mai 2014 schuf man einen Leiter Informatik sowie einen Leiter Finanzen, trennte damit die Zuständigkeit für die Finanzen von der Informatik und ermöglichte so das Vier-Augen-Prinzip.[465] 2015 wurden offiziell die Hauptabteilung Informatik (IT-JI) sowie die Hauptabteilung Finanzen, Controlling & Logistik (FCL) als eigene Einheiten innerhalb des Generalsekretariats geschaffen. Dies, wie es in der Begründung zur Änderung der Organisationsverordnung zu lesen ist, um der Grösse und Eigenständigkeit des Bereichs Informatik besser Rechnung zu tragen.[466] Dem ehemaligen Generalsekretär, Christian Zünd, war die Funktionentrennung schon länger ein Anliegen gewesen und er wollte den Direktionscontroller ausserhalb der Informatik ansiedeln. Da er dort ein Risiko für die Governance sah, habe er gemäss eigenen Angaben bereits im August 2010 dem damaligen Direktionsvorsteher, Markus Notter, eine Änderung vorgeschlagen. Dieser habe ihn aber übersteuert und gegen Ende seiner Amtszeit keine diesbezügliche Änderung mehr vornehmen wollen.[467]

In der Befragung durch die PUK Datensicherheit widersprach der ehemalige Direktionsvorsteher, Markus Notter, dieser Darstellung. Aus seiner Sicht war die damals gewählte Verortung des Controllings auch in anderen Direktionen üblich. An eine diesbezügliche Diskussion kann er sich nicht mehr erinnern. Eine Trennung der Finanzen vom Controlling hätte aus seiner Sicht auch organisatorisch keinen Sinn gemacht. Er könne sich höchstens vorstellen, dass man über die Abteilung IT gesprochen habe. Seiner Ansicht nach hätte der Generalsekretär, als Vorgesetzter, bei Zweifeln an der Kompetenzanhäufung bei einer Person diesen Bereich genauer prüfen und nicht organisatorische Veränderungen anstrengen müssen.[468]

Die PUK Datensicherheit konnte im Staatsarchiv Unterlagen aus dem Jahr 2010 zur Revision der Organisationsregelung des Generalsekretariats der JI sowie zur Revision des Organisationsreglements des Generalsekretariats der JI (ORGS) einsehen.[469] Offenbar waren solche Fragen in diesem Zusammenhang aber kein Thema.

---

[463] Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 24–25.

[464] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 6; Stellungnahme von Fredi Steiner vom 5. November 2025.

[465] Protokoll der Finanzkommission Nr. 105 vom 26. März 2015.

[466] Organisationsverordnung der Direktion der Justiz und des Innern (JIOV; LS 172.110.1), Änderung vom 28. Januar 2015, Amtsblatt des Kantons Zürich vom 13. Februar 2015.

[467] Protokoll der Befragung von Christian Zünd vom 30. August 2024, S. 15–18.

[468] Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 17–18.

[469] Direktion der Justiz und des Innern, Organisationsregelung vom 9. November und Organisationsregg lement des Generalsekretariats der JI (ORGS) (Entwurf vom 22. Dezember 2010), STAZH, Ablieferung 2021/020, Dossier 2010/594.

Dem nachfolgenden Direktionsvorsteher, Martin Graf, war bewusst, dass die Frage auch mit dem Vorgänger besprochen worden war und dieser, so seine Annahme, dann nichts mehr machen wollte. Er räumt aber ein, dass er beim Amtsantritt diese Ausgliederung auch nicht vorgenommen habe, obwohl er gewusst habe, dass der Generalsekretär die Kompetenzanhäufung bei dieser Person als Risiko erachtete. Man habe die Überprüfung der Organisation zwar mehrmals diskutiert, aber entschieden, diese Pendenz erst im Rahmen einer personellen Veränderung, wohl der Pensionierung des Leiters LFC, angehen zu wollen.[470]

Weitere Massnahmen

Neben den organisatorischen Anpassungen wurde angesichts des ungenügenden Vertragsmanagements als weitere Massnahme eine zentrale Vertragsdatenbank eingeführt.[471] Fredi Steiner, der Leiter der JI-Informatik bis 2018, gab an, er habe mit Blick auf die Sicherheitsüberprüfungen bei seinem Amtsantritt 2015 einen neuen Prozess etabliert. So habe er eingeführt, dass es heute bei Externen, sobald Dienstleistungen im Spiel seien, einen mindestens drei- bis vierseitigen Vertrag gebe. Als Lehre aus den Feststellungen der Finanzkontrolle müssten Externe eine Non-Disclosure oder eine Geheimhaltungserklärung unterzeichnen. Zusätzlich würden externe Mitarbeitende mit Fernzugriff oder Zugang zum Rechenzentrum sicherheitsüberprüft. Grundsätzlich werde dabei ein Strafregisterauszug sowie die Einwilligung in eine erweiterte Sicherheitsüberprüfung verlangt. Ob eine erweiterte Prüfung erfolge, liege dann im Ermessen der Staatsanwaltschaft oder der Polizei. Nicht kontrolliert werde bisher der Betreibungsregisterauszug, was in diesem konkreten Fall allenfalls zielführender gewesen wäre.[472] Axel Mayer, Leiter der JI-Informatik von 2018–2020, beurteilte auf der Basis dessen, was er gesehen hatte, die Überprüfung in der JI als vorbildlich.[473]

Im Bereich des Beschaffungswesens stellte man sich nach 2014 auch anders auf: Bestellungen wurden durch zwei Personen ausgelöst und die Auftragserteilung, materielle Prüfung und Freigabe der Rechnung konnte nicht durch dieselbe Person erfolgen. Dass in der Vergangenheit die gleiche Person die materielle Prüfung und Visierung vorgenommen hatte, sei, so der ehemalige Leiter der JI-Informatik, für ihn damals nicht befremdlich gewesen, da er an den finanziellen Aspekten nicht interessiert gewesen sei. Er habe gedacht, sein Vorgesetzter wisse wohl schon, was er mache.[474]

8.7 Würdigung durch die PUK

Wie in Kapitel 7.4 bereits gewürdigt, war die technische Informationssicherheit innerhalb der JI auf einem guten Stand und es bestanden strategische Grundlagen sowie erste Ansätze einer direktionsinternen Sicherheitsorganisation. Im konkreten Fall, gemäss Berichterstattung der Finanzkontrolle auch in weiteren Fällen, hat sich leider gezeigt, dass die durchaus bestehenden Vorgaben bezüglich vertraglicher Absicherung von Dienstleistungen Externer, Sicherheitsüberprüfungen und interner Kontrollen nicht gelebt wurden.

---

[470] Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 18–19, 22.

[471] Protokoll der Finanzkommission Nr. 105 vom 26. März 2015.

[472] Staatsanwaltschaft III, Delegierte Einvernahme von Alfred [Fredi] Steiner vom 30. Juni 2023, Frage 30; Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 23.

[473] Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 10.

[474] Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 31–32.

In Bezug auf die vertragliche Absicherung gilt es festzuhalten, dass weder die Staatsanwaltschaft noch die PUK Datensicherheit eruieren konnten, wie genau André Gisler für die JI tätig geworden war und wer für dessen Leistungserbringung verantwortlich gewesen wäre. Es scheint aber so, dass kein Vertrag abgeschlossen wurde. Aus Sicht der PUK Datensicherheit ist es eher unwahrscheinlich, dass ein solcher Vertrag im Rahmen der Räumungsaktion 2019 weggekommen ist.

Die Abklärungen der PUK Datensicherheit zeigen, dass sich die Zusammenarbeit der JI mit André Gisler von 2002 bis 2014 erstreckte.

Für die PUK Datensicherheit ist es erwiesen, dass André Gisler für seine Arbeit unter anderem Geräte erhalten hat und folglich Abmachungen über diese Form der Entschädigung existiert haben müssen. Dieses Entschädigungsmodell ist heute jedoch mangels Dokumentation sowie aufgrund der ausbleibenden Rechnungsstellung kaum mehr zu belegen oder nachzuvollziehen. Es ist denkbar, dass man versucht hatte, auf diese Weise mit den bestehenden Mitteln eine kostengünstige «Lösung» zu erreichen. Es ist hier festzuhalten, dass eine solche «Lösung» Vorgaben verletzt hat.

Für die Umsetzung der ISV-Vorgaben, die Kontrolle der unterstellten Mitarbeitenden und die unterschiedlichen Rollout-Projekte, wie beispielsweise die Migration der Geräte der Statthalterämter, war der ehemalige Leiter der JI-Informatik, Fredi Steiner, verantwortlich. Die Verantwortung für die Aufsicht über die Informatik, das Vertragswesen sowie die Auftragserteilung zum Austausch und damit auch zur Entsorgung von PC-Geräten lag beim Leiter LFC, Renato Widmer. Sowohl der ehemalige Leiter LFC als auch der ehemalige Leiter der JI-Informatik sind diesen Verantwortlichkeiten, wie der Datensicherheitsvorfall zeigt, ungenügend nachgekommen.

Für die PUK Datensicherheit zeigt sich aber auch, dass der ehemalige Leiter der JI-Informatik aufgrund des dominanten Führungsstils von Renato Widmer, aber auch wegen seiner eigenen Zurückhaltung, seine Rolle nie im Sinne der strategischen Grundlagen wahrnehmen konnte. Gerade im Bereich des Austauschs der PC-Arbeitsplätze weisen auch die QM-Vorgaben auf eine besondere Rolle des Leiters LFC hin. Eine Abwicklung direkt zwischen dem Leiter LFC und der beteiligten Mitarbeiterin wäre somit eine der möglichen Varianten. Der ehemalige Leiter LFC weist eine solche direkte Abwicklung in seiner Stellungnahme von sich und auch die Staatsanwaltschaft und die PUK Datensicherheit konnten nicht klären, wer tatsächlich diese Aufträge erteilt hatte.[475]

Die Art der Führung durch den Leiter LFC war auch den Direktionsvorstehern sowie dem Generalsekretär bekannt. Die PUK Datensicherheit stellt fest, dass diese den Informatikbereich zu wenig eng begleitet und den beteiligten Personen angesichts der inhaltlich guten Arbeit dieser Abteilung stark vertraut haben. Weiter ist die PUK Datensicherheit erstaunt darüber, dass selbst die in den Ämtern involvierten Personen davon ausgingen, dass die Entsorgungen fachgerecht abgewickelt würden, ohne dass diesbezüglich eigene Kontrollen stattgefunden hätten. Um die Verantwortung für die Informationssicherheit wahrzunehmen, ist es aus Sicht des ehemaligen Datenschutzbeauftragten, Bruno Baeriswyl, zentral, dass neben der sorgfältigen Auswahl von Dritten und der Instruktion immer auch die Umsetzung überprüft und kontrolliert wird.[476] Dieser Verantwortung sind verschiedene Personen in ihren Funktionen nicht nachgekommen.

---

[475] Stellungnahme von Renato Widmer vom 5. Oktober 2025.

[476] Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 26.

Mit Blick auf den konkreten Datensicherheitsvorfall scheinen aus Sicht der PUK Datensicherheit die Netboxen, auf denen mutmasslich Daten zwischengespeichert wurden, ein mögliches Element für das Datenleck zu sein. Weiter bleibt unklar, inwieweit André Gisler in die Entsorgung der 2700 Client-Geräte involviert war, die bei den Rollouts 2001 und 2005 ersetzt worden waren. Informationen, die in den nicht-verschlüsselten Bereichen dieser Geräte abgelegt worden waren, sowie unverschlüsselte Daten auf USB-Sticks, die mutmasslich mit anderem Elektroschrott an den Dienstleister gingen, sind weitere Quellen des Datenlecks. In kleinerem Ausmass gelangten auch Servergeräte an André Gisler. Zudem waren die Papierunterlagen mit sensitiven Informationen aus dem RIS-Entwicklungsbüro ohne jegliche Sicherheitsvorkehrungen an André Gisler übergeben worden.

Die PUK Datensicherheit würdigt, dass in der JI rasch personelle und organisatorische Massnahmen ergriffen wurden, als durch die Prüfung der Finanzkontrolle die schwierige Situation in Bezug auf Organisation und Kontrolle bekannt geworden war. Angesichts der dominanten Führung im Bereich LFC hätten die Verantwortlichen diesen Risiken frühzeitig mehr Beachtung schenken sollen. Nach der Prüfung durch die Finanzkontrolle wurde es aber verpasst, eine grundlegende Aufarbeitung der direktionsinternen IT-Situation an die Hand zu nehmen, obwohl der damalige Direktionsvorsteher, Martin Graf, gegenüber der Oberaufsicht festhielt, dass der Bericht «unerfreulich» sei, es ein «lausiges Contract-Management» gegeben habe und der Leiter LFC das Ganze doch «auf die leichte Schulter» genommen habe.[477] Vor diesem Hintergrund ist es für die PUK Datensicherheit unverständlich, dass die IT-Situation nicht vertieft und umfassend aufgearbeitet wurde.

[477] Protokoll der Finanzkommission Nr. 105 vom 26. März 2015, S. 984.

9. 2000–2014: Entsorgungspraxis in den Direktionen und der Staatskanzlei

9.1 Einleitung

Die Entsorgungspraxis in den Direktionen und der Staatskanzlei hing im betrachteten Zeitraum 2000–2014 auch davon ab, inwieweit sie bereits über eine zentralisierte Informatikabteilung verfügten, die den Betrieb der Informatik sowie die Erneuerung und Entsorgung der Hardware überhaupt zentral abwickeln konnte. Zur Zentralisierung auf Direktionsebene hielt das Kantonale IT-Team (KITT) 2009 fest, dass erst die Bau-, die Justiz- und die Volkswirtschaftsdirektion sowie die Staatskanzlei über eine zentral ausgerichtete Informatik verfügten und bei den übrigen vier Direktionen (Bildungs-, Finanz-, Gesundheits- und Sicherheitsdirektion) ein höherer Anpassungsbedarf bestehe.[478]

Die Finanzkontrolle gab an, in den anderen Direktionen und der Staatskanzlei hinsichtlich Führung und Organisation der Informatik nie auf eine derart schwierige Situation gestossen zu sein, wie sie sie 2014 in der Direktion der Justiz und des Innern angetroffen habe und wie sie in Kapitel 8.6 dieses Berichts aufgezeigt wird.[479]

9.2 Situation in der Staatskanzlei

Mit der zunehmenden Bedeutung der Informatik wurde deutlich, dass die Staatskanzlei als Einheit zu klein war, um Informatikleistungen selbständig zu erbringen. Sie schloss deshalb mit der Baudirektion (BD) eine Vereinbarung über den Betrieb der Informatik ab. Die BD übernahm die Aufgabe 2010 zuerst im Rahmen einer Übergangslösung und ab 2011 schliesslich vollständig. Die Entsorgung der Hardware wickelte die Staatskanzlei ab diesem Zeitpunkt ebenfalls über die BD ab. Der ehemalige Staatsschreiber, Beat Husi, gab in der Befragung durch die PUK an, sich auf den internen Partner verlassen und sich nicht mehr um das Thema gekümmert zu haben.[480] Aus heutiger Sicht, räumt die Staatsschreiberin, Kathrin Arioli, ein, habe die Staatskanzlei damals wenig eigene Verantwortung übernommen, was angesichts der kleinen Organisation personell jedoch auch schwierig gewesen wäre. Die damaligen Servicevereinbarungen enthielten überdies allgemein nur wenige Regelungen zur Informationssicherheit.[481] Gemäss dem ehemaligen Staatsschreiber habe man den Vereinbarungen mit Dritten zu Beginn sicherlich generell zu wenig Aufmerksamkeit geschenkt. Im Informatikbereich habe er mangels vertiefter IT-Kenntnisse zudem der Fachperson vertrauen müssen. Somit sei nicht ausgeschlossen, dass sich bei einem Fehlverhalten von Mitarbeitenden auch in seinem Bereich so etwas wie ein Datensicherheitsvorfall hätte ereignen können.[482]

---

[478] Kantonales IT-Team (KITT), Projekt: Strategieumsetzung UE1 Projektauftrag, Version 1.0 vom 3. April 2009, Beilage zum RRB Nr. 1072/2009 vom 1. Juli 2009, Informatikstrategie, Umsetzung.

[479] Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 25.

[480] Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 18–19.

[481] Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 7.

[482] Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 15.

9.3 Situation in der Sicherheitsdirektion

In den Ämtern der Sicherheitsdirektion (DS) lagen zu Beginn der Legislaturperiode 2011–2015 die Informationen noch vorwiegend als physische Akten vor. Gemäss dem Sicherheitsdirektor, Mario Fehr, war der Schutz dieser Informationen jedoch schon vor der Digitalisierung immer eine zentrale Aufgabe der Ämter. Das blieb auch nach der Digitalisierung so. Rückblickend räumt er ein, dass der Regierungsrat diese Aufgabe vielleicht zu spät als zentrale Aufgabe aufgefasst habe.[483] Der BDO-Bericht vom 31. Oktober 2016 über die unabhängige Untersuchung der kantonalen Informatik zeigt, dass zum Zeitpunkt der IT-Überprüfung verschiedene Ämter in der Sicherheitsdirektion noch eigene Serverräume betrieben und Informatikmittel beschafft hatten.[484] Auch die Entsorgung war folglich amtsweise organisiert. Das Generalsekretariat, das Amt für Militär und Zivilschutz, das Sozialamt sowie das Sportamt hatten eine gemeinsame Entsorgungsregelung mit einem externen Dienstleister. Die Ämter erneuerten im Projekt «Informatik BasisInfrastruktur Sicherheitsdirektion 2008» (IBIS08) die Basisinfrastruktur gemeinsam und übernahmen bei dieser Gelegenheit von der JI auch die Sicherheitslösung mit Chipkarte, PIN-Code und Verschlüsselung. Im Rahmen des Rollouts sollten die Geräte von einer externen Firma abtransportiert und für den Wiederverkauf aufbereitet werden.[485] Die PUK Datensicherheit konnte die Belege einsehen, die bezeugen, dass der Dienstleister im Jahr 2008 Geräte entgegengenommen und gelöscht respektive physisch zerstört hatte.[486]

Die Kantonspolizei war selbst um die physische Zerstörung ihrer Datenträger besorgt. Auch das Strassenverkehrsamt und das Migrationsamt nahmen die Datenlöschungen respektive Datenträgervernichtungen selbst vor. Dort wurden die Datenträger durchbohrt oder die Daten mit einer speziellen Löschsoftware gelöscht.[487] Im Nachgang zum Datensicherheitsvorfall liess sich der Sicherheitsdirektor von den damals für die Entsorgung zuständigen Personen bestätigen, dass die Datenträger tatsächlich auf diese Weise gelöscht oder zerstört wurden.[488]

Im Frühling 2025 wurde das Strassenverkehrsamt als letztes Amt ins AFI integriert. Die Entsorgung der Datenträger läuft zum Zeitpunkt der Berichtsredaktion über das Amt für Informatik ab. Die Kantonspolizei (KAPO), die aufgrund ihrer spezifischen Anforderungen vom Geltungsbereich der kantonalen IKT-Strategie (RRB Nr. 383/2018) ausgenommen ist, verfügt weiterhin über separate Prozesse.[489]

---

[483] Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 20.

[484] BDO AG, Unabhängige Überprüfung der Informatik des Kantons Zürich, 31. Oktober 2016, S. 22–26.

[485] Informatik BasisInfrastruktur Sicherheitsdirektion 2008 ein Gemeinschaftsprojekt von AMZ, SA, STHA und GS, IBIS08 Newsletter, Ausgabe 1 vom 1. Oktober 2008.

[486] ReCare, Erasing Journals vom 30. Oktober 2008 und 3. November 2008.

[487] Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 24–25, 31.

[488] Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 28.

[489] Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 10; Informationssicherheitsbeauftragter der Sicherheitsdirektion, Schreiben vom 20. Februar 2025 zum Stand der Informationssicherheit in der Sicherheitsdirektion.

9.4 Situation in der Finanzdirektion

Zur IT-Situation innerhalb der Finanzdirektion (FD) enthielt der Bericht der Finanzkontrolle 2013 die Aussage, dass die Direktion auf dem Weg der Zentralisierung wenig weit sei.[490] In der Tat verfügten die verschiedenen Ämter der FD gemäss BDO-Bericht 2016 über eigene IT-Stellen und betrieben teilweise eigene Serverräume.[491] Diese dezentrale Organisation zeigt sich auch darin, dass die IT-Einheiten der FD mit direktionsübergreifenden Aufgaben erst 2017 im Rahmen des Projekts der neuen IKT im neugeschaffenen Amt für Informatik (AFI) organisatorisch zusammengefasst wurden.[492]

Zu den Entsorgungsprozessen in der Finanzdirektion vor dem Aufbau des Amtes für Informatik liegen der PUK Datensicherheit keine Angaben vor.

9.5 Situation in der Volkswirtschaftsdirektion

Die Volkswirtschaftsdirektion verfügte mit der VD-Informatik (VDI) über eine zentrale Stelle für den Betrieb von Serverräumen und die Beschaffung von Informatikmitteln.[493] Zudem zeugen die Weisungen der Volkswirtschaftsdirektion aus dieser Zeit von einem bewussten Umgang mit der Informationssicherheit.

Die Informatik-Weisung vom 5. Juni 2000 diente dazu, die Mitarbeitenden der VD für die Informatiksicherheit zu sensibilisieren und sie über die Sicherheitsvorkehrungen in Kenntnis zu setzen. Die Mitarbeitenden hatten deren Kenntnisnahme schriftlich zu bestätigen.[494] Sowohl die Weisung aus dem Jahr 2000 als auch die spätere Version vom 12. März 2002 wiesen der VDI die Verantwortung für Beschaffung, Installation, Wartung und Entsorgung von Hard- und Software zu. Beide Weisungen machten konkrete Vorgaben zur Löschung resp. Zerstörung von Datenträgern. Die Zuständigkeit für die Entsorgung von kompletten PC lag explizit bei der VDI.[495] Bei Sachmitteln mit schützenswerten Daten, wie Festplatten oder Memory-Sticks, war gemäss der späteren Weisung vom 1. Januar 2015 die Weisung «Entsorgung von Informatik-Sachmitteln» einzuhalten, wobei die Sachmittel der VDI übergeben werden konnten.[496]

Der damals zuständige Leiter der VDI wird sowohl von der Direktionsvorsteherin als auch vom ehemaligen kantonalen Informatik-Sicherheitsbeauftragten (I-SiBe) als eine Person beschrieben, die auf die Sicherheit und die Entsorgung grossen Wert gelegt und diesen Themen eine hohe Aufmerksamkeit geschenkt habe. Er habe die Datenträger auch eigenhändig zerstört.[497]

Das Sicherheitsbewusstsein des Leiters der VD-Informatik zeigte sich auch darin, dass er zur Situation der IT in der Direktion Auditberichte erstellen und diese auch dem Informatik-Sicherheitsbeauftragten (I-SiBe) zukommen liess.[498] Schliesslich wurde die VD-Informatik als zweite Informatikeinheit nach jener der Baudirektion am 1. Juli 2019 beim Amt für Informatik der Finanzdirektion zentralisiert.[499]

---

[490] Bericht der Finanzkontrolle in Zusammenarbeit mit bprex group AG vom 30. August 2013: «Erkenntnisse zur IT-Situation des Kantons Zürich. Würdigung anhand der Resultate aus den IT-Kurzchecks unter Berücksichtigung der KITT-Aktivitäten», S. 30.

[491] BDO AG, Unabhängige Überprüfung der Informatik des Kantons Zürich, 31. Oktober 2016, S. 36.

[492] RRB Nr. 780/2017 vom 30. August 2017, Neue kantonale IKT (Informations- und Kommunikationstechnologie), strategische Eckpfeiler.

[493] BDO AG, Unabhängige Überprüfung der Informatik des Kantons Zürich, 31. Oktober 2016, S. 22–26.

[494] Volkswirtschaftsdirektion, Informatik-Weisung vom 5. Juni 2000.

[495] Volkswirtschaftsdirektion, Informatik-Weisung vom 12. März 2002.

[496] Volkswirtschaftsdirektion, Informatik-Weisung vom 1. Januar 2015.

[497] Protokoll der Befragung von Carmen Walker Späh vom 13. Dezember 2024, S. 7, 10.

[498] Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 17–19.

[499] Protokoll der Befragung von Carmen Walker Späh vom 13. Dezember 2024, S. 8.

9.6 Situation in der Gesundheitsdirektion

Die Gesundheitsdirektion (GD) wies gemäss BDO-Bericht 2016 eine dezentrale IT-Infrastruktur auf. Einerseits war die Informatik in der Abteilung Logistik & Controlling des Generalsekretariats angesiedelt, andererseits verfügten auch die Kantonsapotheke, das kantonale Labor oder die kantonale Heilmittelkontrolle über eigene IT-Einheiten und konnten IT-Beschaffungen durchführen. Die letzten beiden betrieben auch eigene Serverräume.[500]

Gemäss den Aussagen der heutigen Direktionsvorsteherin, Natalie Rickli, kam es im Jahr 2014 in der Gesundheitsdirektion zur Ablösung der zentralen Server sowie des Storage Area Networks. Nach der intern erfolgten Löschung der Daten nahm der beauftragte Dienstleister die Hardware zurück. Im Jahr 2016 löste man die Client-Infrastruktur ab.[501] Zu diesen Abläufen wurden der PUK Datensicherheit jedoch keine Zertifikate vorgelegt. Die nächste Ablösung von Hardware im Sommer 2024 lief dann bereits über das Amt für Informatik (AFI), welches die Datenträger übernahm und sachgemäss entsorgte resp. löschte. Hierzu bestehen zwischen der GD und dem AFI entsprechende Verträge (zur Datenträgerentsorgung beim AFI siehe Kapitel 14.3.4).

9.7 Situation in der Bildungsdirektion

Gemäss dem BDO-Bericht verfügte die Bildungsdirektion (BI) 2016 über IT-Einheiten beim Generalsekretariat, beim Mittelschul- und Berufsbildungsamt (MBA), bei den kantonalen Mittel- und Berufsschulen sowie beim Amt für Jugend und Berufsberatung (AJB).

Zur Entsorgung von Datenträgern liegen der PUK Datensicherheit folgende Informationen vor: Im Jahr 2007 führte die BI-Informatik für das Generalsekretariat, das Hochschulamt, die Fachstelle für Schulbeurteilung, die Berufsprüfung, das Volksschulamt sowie Teile des Mittelschul- und Berufsbildungsamtes eine Gesamterneuerung der Hardware durch. Die sichere Entsorgung resp. Verwertung der Altgeräte war Teil dieses Projekts. Die Unterlagen dazu brachte man der Bildungsdirektorin bei ihrem Amtsantritt 2015 zur Kenntnis. Inzwischen sind die entsprechenden Projektunterlagen jedoch entsorgt worden. Bei der Client-Erneuerung 2013 arbeitete die BI-Informatik auch mit dem AJB zusammen. Die Rücknahme der Altgeräte war, inklusive einer sicheren Löschung der Daten als Option, Teil der Ausschreibung. Das Betriebskonzept BI Client 2013 regelte die Entsorgung und wurde in der Prozessdokumentation beschrieben.[502] Die heutige Direktionsvorsteherin, Silvia Steiner, gab an, dass sie von diesem Konzept und den Ausschreibungsunterlagen im Nachhinein Kenntnis nehmen konnte. Den Auftrag zur Entsorgung der Festplatten gab der Auftragnehmer für die Client-Erneuerung an eine spezialisierte Firma weiter, wobei der Projektleiter der BI gemäss Aussage der Direktionsvorsteherin die sichere Löschung vor Ort stichprobenweise überprüfte.[503]

Seit dem 1. Juli 2020 trägt das Amt für Informatik die Verantwortung für die IKT-Grundversorgung der Bildungsdirektion. Es hat alle Geräte der BI übernommen und ist seit der buchhalterischen Übertragung im Jahr 2021 für die Entsorgung von alter oder defekter Hardware verantwortlich.

---

[500] BDO AG, Unabhängige Überprüfung der Informatik des Kantons Zürich, 31. Oktober 2016, S. 22–26.

[501] Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 13.

[502] ISID BI, Schreiben vom 20. Februar 2025, Ihre Anfrage vom 22. Januar 2025 betreffend Stand der Informationssicherheit in den Direktionen und der Staatskanzlei, S. 3.

[503] Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 8, 26.

9.8 Situation in der Baudirektion

Seit Beginn der 2000er-Jahre war die Informatik der Baudirektion (BD) zentral organisiert und liess die Rücknahme und Entsorgung der IT-Clients von qualifizierten Firmen durchführen. Gemäss dem ehemaligen I-SiBe, Renzo Mühlebach, verfügte die BD, im Gegensatz zu den anderen Direktionen, im Bereich der Informatiksicherheit zudem über einen Fachmann mit den notwendigen Ausbildungen und war entsprechend sensibilisiert.[504]

Die Migration 2004 wurde an eine etablierte IT-Firma vergeben. Aufgrund des Ablaufs der Aufbewahrungsfrist sind die diesbezüglichen Projektunterlagen nicht mehr vorhanden. Relevante Dokumente wurden jedoch dem Staatsarchiv für eine Archivierung angeboten. Bei der Migration 2010, zu der die Unterlagen noch vorhanden sind, war der Rückschub der alten Hardware, inkl. Datenlöschung, Teil des vergebenen Leistungspaketes. Anschliessend wurde die alte Hardware mit den gelöschten Datenträgern durch die beauftragte Firma intern oder extern weiterverkauft. Die Rücknahme der alten Hardware und die Datenlöschung waren auch bei der Migration 2016 Teil des Pflichtenhefts der beauftragten Firma.

Der Umgang mit Servern lief folgendermassen ab: Datenstorage-Systeme gingen für die konforme Entsorgung jeweils an den Lieferanten zurück. Harddisks sammelte man in Vernichtungscontainern und liess sie, dem Verfahren bei vertraulichen Papierakten ähnlich, schreddern.[505]

Die Informatikabteilung der BD genoss einen guten Ruf. Auch deshalb entschloss sich die Staatskanzlei 2010 auf Empfehlung des eigenen Informatikleiters, ihre Informatik in die BD auszulagern.[506] Schliesslich verlagerte die BD 2018 als erste Direktion ihre Informatik ins Amt für Informatik (AFI). Die letzte IT-Client-Migration der BD im Jahr 2021 war somit bereits in der Zuständigkeit des AFI.[507]

9.9 Würdigung durch die PUK

Die PUK Datensicherheit stellt fest, dass in den anderen Direktionen und der Staatskanzlei im Gegensatz zur Situation in der JI bisher keine Datensicherheitsvorfälle zutage getreten sind. Die Auskünfte, welche die PUK Datensicherheit erhalten hat, weisen darauf hin, dass die Direktionen die Datenträgervernichtungen und Datenlöschungen intern vorgenommen haben oder die Entsorgung im Rahmen von Neubeschaffungen mit spezialisierten Auftragnehmern gelöst haben. Zu den Direktionen, welche ihre Entsorgung dezentral in verschiedenen Ämtern abgewickelt haben, liegen der PUK Datensicherheit jedoch nicht für alle Ämter lückenlose Informationen vor. Bei diesen Entsorgungen von Datenträgern und Datenlöschungen, die nicht in der Direktion koordiniert und über Beschaffungsprozesse abgewickelt wurden, sind frühere Risiken nicht auszuschliessen.

Es ist zudem äusserst fraglich, ob in allen Direktionen und der Staatskanzlei das Bewusstsein ausreichend vorhanden und diesbezügliche Kontrollprozesse etabliert waren, die bei einem Fehlverhalten der zuständigen Personen einen Datensicherheitsvorfall verhindert hätten. Vor diesem Hintergrund ist es nicht ausgeschlossen, dass sich ähnliche Vorfälle in anderen Direktionen und der Staatskanzlei in früherer Zeit hätten ereignen können. Es ist also wohl eher als glückliche Fügung zu bezeichnen, dass in den Direktionen und der Staatskanzlei nicht mehr geschehen ist.

---

504 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 9.

505 Baudirektion, Generalsekretariat, Projekte und Informatik, Datenleck in der JI/DS Statusbericht BD, GL BD Sitzung vom 2. Februar 2023.

506 Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 18.

507 Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S. 16.

10. Kantonale Entwicklung 2015–2019: Schritte auf dem Weg zum heutigen System der Informationssicherheit

10.1 Informationssicherheitsorganisation

Mit der Genehmigung des Organisationskonzepts Informatiksicherheit machte der Regierungsrat am 11. Februar 2015 einen ersten wesentlichen Schritt auf dem Weg zur heutigen Informationssicherheitsorganisation.[508] Nun konnte das Kompetenzzentrum Informatiksicherheit in der Finanzdirektion realisiert werden. Im April 2015 schuf der Regierungsrat die Stelle des Informatik-Sicherheitsbeauftragten des Kantons Zürich (I-SiBe), dem die Leitung des Kompetenzzentrums und der Fachgruppe Informatiksicherheit, bestehend aus den zu bezeichnenden Informatik-Sicherheitsbeauftragten der Direktionen und der Staatskanzlei, zukam.[509] Diese Stelle fungierte gemäss Organisationskonzept als die zentrale Ansprechposition für alle Aspekte der Informatiksicherheit der kantonalen Verwaltung.[510] Die Funktion entsprach der eines Chief Information Security Officers (CISO). Der erste Informatik-Sicherheitsbeauftragte, Renzo Mühlebach, trat seine Stelle im Oktober 2015 an. Er war in der Geschäftsstelle des Kantonalen IT-Teams (KITT) angesiedelt und beauftragt, über die Direktionen hinweg die Informatiksicherheit in einer unterstützenden, beratenden Funktion ohne Weisungsbefugnis zu koordinieren.

Aus Sicht der Finanzkontrolle war es eine richtige Massnahme, diese Person zu benennen und die Verantwortlichkeit zu adressieren.[511] Auch der ehemalige Datenschutzbeauftragte, Bruno Baeriswyl, nahm die Schaffung der CISO-Stelle, die er bereits früher gefordert hatte, positiv auf, auch wenn es bis zu diesem Schritt seiner Ansicht nach lange gedauert hatte.[512] Damit waren Entwicklungen in die richtige Richtung angestossen, die man vom Standpunkt der Finanzkontrolle aus aber noch nicht konsequent umsetzte.[513] Aus Sicht des ehemaligen Staatsschreibers, Beat Husi, stellte die Schaffung dieser zentralen Stelle insofern einen Durchbruch dar, als nun die Informationssicherheit auch zentral betrachtet werden konnte; daran hatte es vorher wegen des Direktionsdenkens gefehlt. Seine Gesamtverantwortung als Gremium könne der Regierungsrat nur wahrnehmen, indem er entsprechende Strukturen, in diesem Fall den Informatik-Sicherheitsbeauftragten, schaffe. Nach diesem ersten Schritt seien aber weitere konkrete Massnahmen durch den Regierungsrat ausgeblieben. Wie bei der früheren Einrichtung der neuen Funktionen des Datenschutzbeauftragten oder der Finanzkontrolle habe sich beobachten lassen, dass der Regierungsrat einen halben Schritt nach vorn und dann wieder einen Schritt zurück gemacht habe.[514] Diese Aussage wurde durch die GPK in ihrem Bericht 2018 bestätigt. Sie hielt im Rahmen ihrer Abklärungen zur Anwendung des Datenschutzgesetzes in den Direktionen fest, dass der Regierungsrat ihr gegenüber noch im Jahr 2018 eingeräumt habe, dass die Informationssicherheit von einer zentralen, professionellen und leistungsstarken Sicher-

---

508 RRB Nr. 129/2015 vom 11. Februar 2015, Organisationskonzept für die Informatiksicherheit in der kantonalen Verwaltung (Genehmigung).

509 RRB Nr. 379/2015 vom 15. April 2015, Informatiksicherheit in der kantonalen Verwaltung (Stellenschaffung). Gemäss Budget 2015 wies die KITT-Geschäftsstelle insgesamt, inklusive der neu geschaffenen Stelle des Informatik-Sicherheitsbeauftragten, 10,6 Stellen aus.

510 Kantonales IT-Team, Strategie Umsetzungseinheit 2, Informatiksicherheit, Organisationskonzept für die Informatiksicherheit in der kantonalen Verwaltung Zürich vom 19. September 2014.

511 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 12.

512 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 19.

513 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 13.

514 Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 11–13.

heitsorganisation wahrgenommen werden müsse, die bis anhin nicht bestehe. Die GPK kam damals zum Schluss, dass der Regierungsrat dem Datenschutz als Grundrecht einen nicht sehr hohen Stellenwert einräumte.[515]

10.1.1 Begrenzte Ressourcen und fehlende Rollentrennung

Der Informatik-Sicherheitsbeauftragte funktionierte als «One-Man-Show».[516] Er war in einem 100%-Pensum tätig und die einzige zentrale Person in dieser Funktion. Die Mitglieder der Fachgruppe Informationssicherheit, der späteren FAGIS, waren, mit einer Ausnahme, allesamt Informatikleiter, die neben ihrer Leitungsfunktion auch die Funktion der direktionalen Informatik-Sicherheitsbeauftragten übernahmen. Trotz entsprechender Sensitivität verfügten sie aus Sicht des ehemaligen kantonalen Informatik-Sicherheitsbeauftragten nicht über die notwendigen Kompetenzen in der Informatik- oder Informationssicherheit.[517] Gemäss dem ehemaligen Staatsschreiber, Beat Husi, war den Direktionen 2015 noch nicht bewusst, dass diese Doppelfunktion aus Gründen der Governance eigentlich nicht ging.[518] Vielmehr führte sie zu Interessenkonflikten, weshalb der damalige Informatik-Sicherheitsbeauftragte darauf hinzuwirken versuchte, dass die Rolle des Informatik-Sicherheitsbeauftragten der Direktionen und der Staatskanzlei nicht mehr durch den Informatik-Leiter wahrgenommen werden darf. Diesen Punkt brachte er auch informell in Gesprächen ein.[519] Der Regierungsrat sah die Dringlichkeit allerdings nicht in dieser Weise.[520] Erst im Jahr 2020, als die neuen Regeln der Allgemeinen Informationssicherheitsrichtlinie (AISR) eine Trennung der Funktionen verlangten, schuf der Regierungsrat die sieben unbefristeten Stellen «Informationssicherheitsbeauftragte/r der Direktion und der Staatskanzlei, ISID»; dies auch, um die wachsenden Anforderungen an die Informationssicherheit zu erfüllen.[521]

10.1.2 Auf die IT-Sicherheit beschränkter Wirkungskreis

Der Begriff der Informatiksicherheit umfasst die Sicherheit der IT-Systeme und der darin gespeicherten Daten. Der breitere Begriff der Informationssicherheit beinhaltet zusätzlich auch die Sicherheit von nicht elektronisch verarbeiteten Informationen.[522] Das Organisationskonzept Informatiksicherheit hielt klar fest, dass das Thema der Informationssicherheit nicht Gegenstand der IT-Sicherheitsorganisation sei.[523] Der Informatik-Sicherheitsbeauftragte sah sich hingegen auch für den Schutz von Papierdokumenten in der Verantwortung und sprach sich klar für die Umbenennung der Rolle in «Informationssicherheits-Beauftragter» aus. Im Gegensatz zu seinen Erfahrungen in der Privatwirtschaft war das damalige Rollenverständnis in der kantonalen Verwaltung aber noch stark technisch geprägt, deshalb blieb sein Wirkungskreis auf die IT-Sicherheit beschränkt.[524]

---

[515] Bericht der Geschäftsprüfungskommission an die Geschäftsleitung des Kantonsrates vom 20. September 2018, Abklärungen zu Verfahren und Abläufen zur Gewährleistung des Datenschutzes.

[516] Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 12.

[517] Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 6, 9.

[518] Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 12.

[519] Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 25.

[520] Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 16.

[521] RRB Nr. 1193/2020 vom 2. Dezember 2020, Informationssicherheit, Umsetzung in den Direktionen und der Staatskanzlei (Stellenpläne, gebundene Ausgabe).

[522] Datenschutzbeauftragte des Kantons Zürich, Lexika, Informationssicherheit Glossar und Abkürzungen. Online verfügbar auf datenschutz.ch/lexika/informationssicherheit-glossar [Zugriff 4. Mai 2025].

[523] Kantonales IT-Team, Strategie Umsetzungseinheit 2, Informatiksicherheit, Organisationskonzept für die Informatiksicherheit in der kantonalen Verwaltung Zürich vom 19. September 2014, S. 7.

[524] Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2025, S. 21, 25.

10.1.3 Ungünstige Verortung und fehlende Aufmerksamkeit der Führungsebene

Aus Sicht des ehemaligen Informatik-Sicherheitsbeauftragten (I-SiBe), Renzo Mühlebach, fehlte es im Kanton Zürich in Bezug auf die Informationssicherheit an der Aufmerksamkeit der Führungsebene und dem Wissen, dass eine Veränderung und eine Stärkung der Informationssicherheit notwendig gewesen wären. Zwischen dem I-SiBe und den Direktionsvorsteherinnen und -vorstehern oder gar dem Gesamtregierungsrat bestand kein direkter Austausch. Das Reporting lief über die KITT-Geschäftsstelle und das KITT-Gremium. Damit konnten die Vertreterinnen und Vertreter im KITT den Inhalt der Berichte bereits in der FAGIS oder dann im Gremium wesentlich beeinflussen und steuern. Eine Transparenz gegenüber dem Gesamtregierungsrat konnte so nicht geschaffen werden. Der I-SiBe, der anfangs in der KITT-Geschäftsstelle und ab 2018 im Amt für Informatik verortet war, gelangte mit seinen Anliegen an seinen Vorgesetzten und hatte trotz dessen Unterstützung Mühe, irgendetwas zu bewegen. Er spürte bei seiner Tätigkeit den Regierungsrat kaum, bemerkte aber bei seiner täglichen Arbeit den Widerstand der Informatikleiter der Direktionen und scheiterte schliesslich, wie auch der Leiter der KITT-Geschäftsstelle, an der fehlenden Weisungsbefugnis.[525] Die Bemühungen, über die FAGIS bei den Informatikleitern Wissen und Fähigkeiten zur Informationssicherheit aufzubauen, nahmen diese grundsätzlich positiv auf. Den Zustand der Informationssicherheit in den Direktionen konnten oder wollten sie dem Informatik-Sicherheitsbeauftragten jedoch – in Ausnahmefällen sogar mit Verweis auf das Amtsgeheimnis – nicht transparent aufzeigen.[526]

Aus Sicht des ehemaligen Staatsschreibers, Beat Husi, war der Entscheid richtig, den Informatik-Sicherheitsbeauftragten in der KITT-Geschäftsstelle zu verorten und damit dem direkten Einfluss eines einzelnen Direktionsvorstehenden zu entziehen. Rückblickend hätte man ihn mit Blick auf die institutionell schwache Position der KITT-Geschäftsstelle auch direkter der politischen Verantwortung unterstellen können.[527]

Mit Blick auf die Verortung im Organigramm – im neugeschaffenen AFI war er dann unter dem Amtschef und dem Leiter Stab angesiedelt – liessen sich sogar von aussen die fehlenden Kompetenzen der Funktion erahnen.[528]

10.1.4 Diskussionen bezüglich Weisungsbefugnis

Auf ein Weisungsrecht hatte der Regierungsrat verzichtet. Zwar war er sich bewusst, dass es die Stelle eines Informatik-Sicherheitsbeauftragten (I-SiBe) brauchte, aber er wollte vermeiden, dass dieser sich als subalterner Mitarbeiter in den Direktionen einmischte. Während seiner Amtszeit, so der ehemalige Staatsschreiber, Beat Husi, habe sich, wenn man neue Strukturen schaffen oder eine Aufgabe zentral angehen wollte, stets die Frage durch alle Diskussionen gezogen, inwiefern dadurch die Autonomie der Direktionen eingeschränkt würde.[529]

Dieses starke «Gärtchen-Denken», in dem sich manche Regierungsmitglieder mehr als Direktionsvorsteherinnen oder -vorsteher verstehen und die gesamtkantonale gegenüber der direktionalen Sicht vernachlässigen, liegt aus Sicht der befragten ehemaligen Regierungsmitglieder am Regierungssystem. Denn die Wahl der Regierungs-

[525] Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 13–16, 27–28.

[526] Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 8, 11–12.

[527] Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 11.

[528] Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 15.

[529] Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 12–13, Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 15.

räte und Regierungsrätinnen erfolgt einzeln und es besteht kein ständiges Präsidium, das eine gesamtkantonale Sicht stärken könnte.[530] In einem Regierungsrat mit jährlich wechselndem Vorsitz und ohne Präsidium auf Amtsdauer sei die Wahrnehmung der Gesamtverantwortung kaum möglich.[531]

10.2 Regelwerk Informationssicherheit

10.2.1 Vorgeschichte: Totalrevision der Informatiksicherheitsverordnung (ISV)

Als der erste Informatik-Sicherheitsbeauftragte seine Stelle 2015 antrat, bestand das gesamtkantonale Regelwerk bezüglich Informatik- bzw. Informationssicherheit im Wesentlichen aus den diesbezüglichen Bestimmungen aus dem Gesetz über die Information und den Datenschutz (IDG) sowie aus der ISV. Ein Informationssicherheits-Managementsystem (ISMS), also eine Aufstellung von Verfahren und Regeln, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern und zu sichern, fehlte. Die ISV stammte aus dem Jahr 1997, basierte ursprünglich noch auf dem alten Datenschutzgesetz und war revisionsbedürftig. Mit dem Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999[532] und der Verordnung über die Nutzung von Internet und E-Mail vom 17. September 2003[533] waren zudem neue Regelungen zu berücksichtigen.

Gemäss der Informatikstrategie von 2008 hatte das KITT den Auftrag, die Verantwortlichkeiten und die Organisation zugunsten einer zeitgemässen Informatiksicherheitsorganisation zu regeln. Mit dem Ziel, eine neue Grundlage für alle informatiksicherheitsrelevanten Regelungen im Kanton zu schaffen, erhielt die Finanzdirektion den Auftrag, bis Ende 2014 einen Entwurf für eine revidierte Informatiksicherheitsverordnung (ISV) auszuarbeiten. Darin sollte auch die Überprüfung der Sicherheitsmassnahmen im Sinne eines Informatiksicherheits-Controllings geregelt werden.[534]

Eine breit abgestützte Projektgruppe[535] legte dem Regierungsrat im April 2015 einen Entwurf für die Verordnung vor, welche neu als Informationssicherheitsverordnung (ISV) bezeichnet wurde. Der Entwurf enthielt folgende Regelungsbereiche:[536]

- Risikomanagement
- Organisation
- Benutzerinnen und Benutzer
- Klassierung und Sicherheit von Informationen
- Geschäftliche und private Informationen
- Sicherheit bei der Informationsverwaltung in der ruhenden Ablage
- Sicherheitsverfahren bei der Projektarbeit
- Datenaustausch und Datentransport
- Auslagerung der Informationsbearbeitung

---

530 Protokoll der Befragung von Markus Notter vom 20. September 2024, S. 27–28.

531 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 15.

532 Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999 (LS 172.71).

533 Verordnung über die Nutzung von Internet und E-Mail vom 17. September 2003 (LS 177.115).

534 RRB Nr. 231/2014 vom 26. Februar 2014, Informatiksicherheitsverordnung, Totalrevision, Konzept.

535 Die Projektgruppe bestand aus Vertretungen der Bildungsdirektion, der Gerichte, der Universität, des Universitätsspitals, der Gemeinden, der Städte Zürich und Winterthur sowie des Datenschutzbeauftragten.

536 RRB Nr. 400/2015 vom 29. April 2015, Informationssicherheitsverordnung (Vernehmlassung, Ermächtigung).

Neu sollte die ISV für alle öffentlichen Organe im Kanton Zürich gelten und u. a. auch die Pflichten des Leistungsbezügers wie auch des Leistungserbringers explizit nennen.[537] Die Finanzkontrolle, welche die Entwicklung am Rande begleitet hatte, nahm die geplanten, klareren und verschärften Regeln positiv zur Kenntnis.[538] Auch aus Sicht des damaligen Datenschutzbeauftragten, Bruno Baeriswyl, war die Revision auf einem guten Weg.[539]

10.2.2 Regelungsbedarf zur Informationsverwaltung

Etwa zur gleichen Zeit zeichnete sich ab, dass auch im Bereich der Informationsverwaltung Regelungsbedarf bestand. Der Regierungsrat hatte bis dahin darauf verzichtet, die Informationsverwaltung in einer Verordnung zu regeln. Ab 2012 liess er abklären, ob es Regelungen für die Schriftgutverwaltung und insbesondere für elektronisch geführte Akten brauchte. 2014 kam er zum Schluss, dass Handlungsbedarf bestand, und beauftragte das Staatsarchiv, einen Entwurf konkreter Regelungen auszuarbeiten.[540] Die zunehmende Bedeutung der elektronischen Aktenführung zeigt sich auch darin, dass das Staatsarchiv 2015 organisatorische und benutzertechnische Basisanforderungen vorlegte, um die Führungsebene bei der Beschaffung von Systemen für die digitale Informationsverwaltung zu unterstützen.[541]

10.2.3 Gemeinsame Regelung der Informationsverwaltung und -sicherheit (IVSV)

Die beiden Entwürfe gingen in die Vernehmlassung und deren Ergebnisse lagen im Herbst 2015 vor. Gemäss den Ausführungen im entsprechenden Regierungsratsbeschluss (RRB Nr. 1226/2016) zeigten die Auswertungen in beiden Fällen die Notwendigkeit einer Straffung und verstärkten Abstimmung oder gar Zusammenlegung der Regelungsvorhaben, woraufhin die Vorsteherin der Direktion der JI, Jacqueline Fehr, in Absprache mit der Staatskanzlei und der Finanzdirektion dem Staatsarchiv den Auftrag erteilte, einen gemeinsamen Regelungsentwurf zu formulieren und zu prüfen, inwieweit die Informationssicherheit integriert oder separat behandelt werden sollte. Im April 2016 prüfte die direktionsübergreifend zusammengesetzte Arbeitsgruppe sämtliche Punkte gründlich auf die Regelungswürdigkeit und beschloss dann, einen gemeinsamen Entwurf für eine Verordnung über die Informationsverwaltung und -sicherheit (IVSV) vorzulegen.[542]

In den Augen des Datenschutzbeauftragten wurde damit aber die bereits erarbeitete Verordnung zusammengestrichen, da man rund um den «Hype der Digitalisierung» keine klaren Vorgaben in Bezug auf die Datensicherheit mehr wollte, was – mit seinen Worten – ein «verheerender Schritt» war.[543] Das explizite Ziel des Regierungsrates war, eine übersichtliche, auf das Wesentliche beschränkte und für die Mitarbeitenden des Kantons und der Gemeinden akzeptable und praktikable Regelung zu erhalten. Technische Details wollte man im Sinne eines offenen Regelungsansatzes in

---

[537] Tätigkeitsbericht des Datenschutzbeauftragten 2015, März 2016, «Vernehmlassungen Neue Informationssicherheitsverordnung», S. 32.

[538] Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 9.

[539] Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 16, 21.

[540] RRB Nr. 538/2014 vom 7. Mai 2014, Regelungen für die insbesondere elektronisch gestützte Schriftgutverwaltung (Records Management; Ergebnis der Bedarfsabklärung).

[541] Direktion der Justiz und des Innern, Staatsarchiv, Basisanforderungen an ein Records-Management-System, Januar 2015.

[542] RRB Nr. 1226/2016 vom 14. Dezember 2016, Verordnung über die Informationsverwaltung und -sicherheit (Vernehmlassung, Ermächtigung).

[543] Protokoll der Befragung des Datenschutzbeauftragten vom 7. Juni 2024, S. 8.

verwaltungsinternen Richtlinien beschliessen. Damit wollte man den öffentlichen Organen bei der Bezeichnung der zuständigen Stellen und Personen Organisationsfreiheit gewähren.[544] Als Resultat befassen sich in der heute noch geltenden Verordnung über die Informationsverwaltung und -sicherheit (IVSV) lediglich zwei allgemein gehaltene Paragrafen (§§ 12 und 13) mit Informationssicherheit.[545] Die früheren Informationssicherheitsvorgaben zur Risikoabschätzung und Bestimmung der Schutzziele, die damit verbundenen, zu ergreifenden Massnahmen sowie die Kontrollmechanismen, die man gemäss dem Datenschutzbeauftragten in der Verwaltung etablieren wollte und hätte etablieren sollen, waren nicht mehr vorgesehen. In dieser Hinsicht gab und gibt es auf Verordnungsstufe keine konkreten, verbindlichen Vorgaben mehr, was nach Ansicht des Datenschutzbeauftragten auch nicht dem Verwaltungshandeln entspricht, das sich stark am Legalitätsprinzip und damit an den Vorgaben aus Gesetz und Verordnung orientiert.[546]

In seiner Vernehmlassungsantwort deklarierte der Datenschutzbeauftragte die neue Regelung als Rückschritt und machte in seinem Tätigkeitsbericht 2016 deutlich, dass die alte, revisionsbedürftige Informatiksicherheitsverordnung einen weit besseren Orientierungsrahmen bieten würde:

«Mit der fortschreitenden Digitalisierung tritt vermehrt die Sicherheit der Daten in den Vordergrund. Die kantonale Verwaltung tut sich schwer, hier die notwendigen Rahmenbedingungen zu schaffen […]. Der Datenschutzbeauftragte wies in seiner Vernehmlassungsantwort darauf hin, dass die geplante Verordnung einen Rückschritt in Bezug auf die geltende Informatiksicherheitsverordnung bedeutet. Sie verpasst es, Vorgaben zu machen, sodass ein einheitliches Sicherheitsniveau in der Verwaltung entsteht. Vielmehr überlässt sie die Beurteilung des Sicherheitsniveaus den einzelnen öffentlichen Organen, die – wie Kontrollen zeigen – sich der Risiken für ihre Daten oft nicht bewusst sind.» [547]

Der damalige Informatik-Sicherheitsbeauftragte, Renzo Mühlebach, teilte die Einschätzung des ehemaligen Datenschutzbeauftragten und war mit ihm der Meinung, dass es bessere, präzisere Vorgaben brauche.[548] Die Feststellung des Datenschutzbeauftragten entsprach und entspricht auch den Erfahrungen der Finanzkontrolle, die gerade bei Querschnittsthemen mit dem Problem konfrontiert ist, dass die einzelnen Direktionen Themen selbständig bearbeiten möchten und es Kraftanstrengungen braucht, um zu gemeinsamen Lösungen zu kommen.[549]

Auch die heutige Datenschutzbeauftragte, Dominika Blonski, bedauert, dass die Bestimmungen zum Aspekt, wann eine Information in welche Schutzstufe fällt und welche Sicherheitsmassnahmen demzufolge angezeigt sind, nicht mehr auf Verordnungsstufe geregelt sind und somit auch für die Gemeinden keine Geltung mehr haben.[550]

Die konkreten Gründe für den Entscheid, beide Regulierungsentwürfe zusammenzulegen, liessen sich in den Befragungen nicht mehr klären. Die Beteiligten erinnerten sich jedoch, dass diese Zusammenführung zu Diskussionen geführt hatte und der Regierungsrat den Entscheid im Wissen fällte, dass man ihn auch anders hätte fällen können.[551]

---

544 Begründung zur Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019, Amtsblatt vom 13. September 2019, S. 9.

545 Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019 (IVSV; LS 170.8).

546 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 11, 16–17.

547 Tätigkeitsbericht des Datenschutzbeauftragten 2016, April 2017, S. 33–31.

548 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 7.

549 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 9.

550 Protokoll der Befragung von Dominika Blonski vom 26. Januar 2024, S. 10.

551 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 19.

10.2.4 Verbindlichkeitserklärung der Allgemeinen Geschäftsbedingungen (AGB)

Der Entwurf für die neue Informationssicherheitsverordnung (ISV) sah ursprünglich vor, die Auslagerung der Informationsbearbeitung zu regeln. Die ISV sollte die Pflichten des Leistungsbezügers wie auch des Leistungserbringers explizit nennen.[552] In der neuen Verordnung über die Informationsverwaltung und -sicherheit (IVSV) verzichtete man darauf, diesen Aspekt auf Verordnungsstufe festzulegen. Der Regierungsrat erklärte jedoch 2015 die AGB der Schweizerischen Informatikkonferenz für IKT-Leistungen (AGB SIK), die in der Verwaltung seit 2004 standardmässig Verwendung fanden, sowie die vom Datenschutzbeauftragten neu erarbeiteten «AGB Auslagerung Informatikleistungen» und die «AGB Datenbearbeitung durch Dritte» für alle dem Regierungsrat unterstellten Verwaltungseinheiten und die Staatskanzlei für verbindlich. Damit dürfen bis heute nur in Ausnahmefällen abweichende Bedingungen ausgehandelt werden. In seinem Beschluss RRB Nr. 670/2015 taxierte der Regierungsrat die Verbindlicherklärung als angemessene Massnahme, um den Schutz der Informationen gemäss § 7 IDG ausreichend zu konkretisieren.[553]

Weiter empfahl der Regierungsrat zwar die Nutzung der AGB durch weitere öffentliche Organe, sie waren und sind aber beispielsweise für Gemeinden nicht verbindlich. Fehlende oder unpassende Geschäftsbedingungen bei Verträgen von Gemeinden mit Dienstleistern waren dann auch Thema bei Kontrollen der heutigen Datenschutzbeauftragten.[554] Auch die Finanzkontrolle befasste sich regelmässig mit der Frage, wie die auslagernden Stellen ihre Verantwortung für die Überwachung der Umsetzung der vertraglich festgehaltenen Leistungen wahrnehmen. Nach Ansicht der Finanzkontrolle müssten dort, wo Dritte relevante Datenbearbeitungen machen, Kontrollen, Standards und Audits respektive diesbezügliche Testate eingefordert werden. Hierzu gibt es gemäss der Finanzkontrolle keine kantonalen Kriterien. Sie sind auch in den heutigen AGB nicht abgebildet. Da die Einforderung von Testaten Kosten verursacht, sollte dieser Aspekt gemäss der Finanzkontrolle jedoch ohnehin im Vertrag und nicht nur in den AGB geregelt werden.[555]

In Bezug auf die geltenden AGB kam auch der Schlussbericht zur Administrativuntersuchung (siehe dazu auch Kapitel 12.3) zum Schluss, dass beide AGB, gemessen an gängigen Auftragsbearbeitungsverträgen im privatrechtlichen Bereich, nicht sehr umfangreich seien.[556]

10.2.5 Allgemeine Informationssicherheitsrichtlinie (AISR) und Besondere Informationssicherheitsrichtlinien (BISR)

Parallel zur Erarbeitung der Verordnung über die Informationsverwaltung und -sicherheit (IVSV) begann der Informatik-Sicherheitsbeauftragte (I-SiBe) die Allgemeine Informationssicherheitsrichtlinie (AISR) und die Besonderen Informationssicherheitsrichtlinien (BISR) zu entwickeln. Denn ihm war klar, dass im Bereich der Informationssicherheit zusätzliche Werkzeuge notwendig waren. Trotz der Einstimmigkeitsklausel ermöglichte das KITT-Gremium die Erarbeitung der Richtlinien. Die Richt-

---

552 RRB Nr. 400/2015 vom 29. April 2015, Informationssicherheitsverordnung (Vernehmlassung, Ermächtigung).

553 RRB Nr. 670/2015 vom 24. Juni 2015, Allgemeine Geschäftsbedingungen in den Bereichen Informations- und Kommunikationstechnik sowie der Datenbearbeitung (Erlass und Verbindlicherklärung).

554 Protokoll der Befragung von Dominika Blonski vom 26. Januar 2024, S. 20.

555 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 14–16.

556 Direktion der Justiz und des Innern des Kantons Zürich, Administrativuntersuchung bei der Direktion der Justiz und des Innern des Kantons Zürich im Zusammenhang mit dem Umgang von Informationen und Datenmissbrauch, 30. März 2021, IT & Law Consulting GmbH, S. 31.

linien orientierten sich an der ISO-Norm 27001, die im Bereich Datenschutz und Informationssicherheit Anforderungen an Informationssicherheits-Managementsysteme definiert. Ein erster Entwurf der AISR lag Ende 2016 vor.[557] Erst mit der Schaffung solcher Vorgaben konnten gemäss dem I-SiBe Abweichungen überhaupt festgestellt, die diesbezüglichen Risiken beurteilt und Massnahmen und Zuständigkeiten festgelegt werden. Diese Vorgaben waren nach seiner Ansicht also grundlegend, um das Informationssicherheitsmanagement überhaupt messen zu können.[558] Obwohl der Regierungsrat die unter der Verordnung angesiedelten Richtlinien als verbindlich festlegte,[559] hängen diese in der Einschätzung des ehemaligen Datenschutzbeauftragten ohne formelles Fundament jedoch «etwas wie Ballone» in der Luft. Sie seien leicht veränderbar und böten den Verwaltungsmitarbeitenden im Gegensatz zu einer Regelung in einer Verordnung keine ausreichende Orientierung, weshalb sie, nach Ansicht des Datenschutzbeauftragten, in den Direktionen niemanden interessieren.[560] Aus Sicht des heutigen Informationssicherheitsbeauftragten, Philipp Grabher, zeigt sich allgemein, dass Regularien bei Organisationen, die Vorgaben nur zurückhaltend umsetzen, hilfreich seien, weshalb eine stärkere gesetzliche Verankerung sicher prüfenswert sei.[561]

10.2.6 Schwieriger Erarbeitungsprozess mit Verzögerungen

Ende 2016 lag der neue gemeinsame Regelungsentwurf zur Verordnung über die Informationsverwaltung und -sicherheit (IVSV) vor. Der Regierungsrat verabschiedete die IVSV jedoch erst 2019[562] und setzte sie mit der ergänzenden Allgemeinen Informationssicherheitsrichtlinie (AISR) auf das Jahr 2020 in Kraft.[563] Zwischen dem ersten Konzept für eine neue ISV 2014 und dem Inkrafttreten der IVSV 2020 vergingen also ganze sechs Jahre.

In dieser Zeit blieb die alte ISV aus dem Jahr 1997 noch gültig. Nach Ansicht des ehemaligen Datenschutzbeauftragten war die Verwaltung angesichts der angekündigten Revision natürlich weniger bereit, sich weiterhin an die detaillierten Vorgaben aus der ISV von 1997 zu halten.[564]

In der Erinnerung der zuständigen Vorsteherin der Direktion der JI, Jacqueline Fehr, war die Erarbeitung der IVSV bezüglich der Regelungsdichte eine anspruchsvolle Aufgabe. Namentlich galt es sich zu einigen, was in der Verordnung und was in den untergeordneten Regulativen festzulegen sei. Der Entwurf war auch mit den Bestimmungen aus dem IDG und der Archivverordnung passend abzugleichen.[565] Die IVSV musste, auch aufgrund der Rückmeldung des Datenschutzbeauftragten, mehrere Schlaufen nehmen. Durch zusätzliche Konsultationen, Rücksprachen und Formulierungsanpassungen ergab sich die überaus lange Erarbeitungszeit von sechs Jahren. Angesichts der Regelungsinhalte stand zwischen den Direktionen auch die Frage im Raum, wo bei diesem Geschäft die Federführung liegen sollte. Zu weiteren Verzögerungen führte der Umstand, dass sich der Kanton in dieser Zeit auch in Bezug auf seine

---

557 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 7, 10–11.

558 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 13.

559 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 27.

560 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 8, 17.

561 Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 15.

562 RRB Nr. 794/2019 vom 3. September 2019, Verordnung über die Informationsverwaltung und -sicherheit; Erlass, Archivverordnung, Änderung.

563 RRB Nr. 795/2019 vom 3. September 2019, Allgemeine Informationssicherheitsrichtlinie (AISR) (Erlass).

564 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 14.

565 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 19; Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 9–10.

IT strategisch neu aufstellte und somit diesbezügliche Entscheide abzuwarten waren (siehe Kapitel 10.3). Schliesslich beschloss die Direktionsvorsteherin der JI, Jacqueline Fehr, die schwierigen Arbeiten an der IVSV abzuschliessen.[566]

Auch die Erarbeitung der weiteren Vorgaben, die für die Umsetzung eines Informationssicherheits-Managementsystems (ISMS) wesentlich waren, brauchte gemäss dem damaligen Informatik-Sicherheitsbeauftragten sehr viel Zeit und dauerte viel zu lange. In der AISR wird die Aufbau- und Ablauforganisation der Informationssicherheit festgelegt. Da die einzelnen Direktionen gern eine gewisse Eigenverantwortung behalten hätten, war die Erarbeitung der AISR in der FAGIS, die ja grösstenteils aus den KITT-Vertretern der Direktionen und der Staatskanzlei bestand, von intensiven Diskussionen geprägt. Um eine Einigung zu erzielen, wurden die AISR und die BISR in mehreren Runden durch die Fachgruppe diskutiert. Nach der Bereinigung der Rückmeldungen innerhalb der FAGIS folgten die Stellungnahmen der KITT-Geschäftsstelle und des Datenschutzbeauftragten, bevor das KITT-Gremium beschliessen konnte.[567] Für den ehemaligen Informatik-Sicherheitsbeauftragten, Renzo Mühlebach, der dieses Thema auf der Stufe des Gesamtkantons als Einzelperson voranzutreiben hatte, waren die zeitintensiven Prozesse, um überhaupt zu Grundlagen für die Informationssicherheit im Kanton Zürich zu gelangen, frustrierend.[568]

10.3 Entwicklung der kantonalen Informatik

10.3.1 Vorgeschichte

Gemäss den Aussagen damals beteiligter Regierungsmitglieder hatten die Zentralisierungsbemühungen im IT-Bereich in den Jahren 2011–2015 einen schweren Stand. Der Regierungsrat sah die Dringlichkeit für ein gemeinsames Vorgehen kaum.[569] Daran änderten vorerst auch die Feststellungen der Finanzkontrolle aus dem Jahr 2013 nichts. Nachdem Empfehlungen der GPK vom Regierungsrat nicht umgesetzt worden waren, begann die GPK im Sommer 2015 mit ihrer vertieften Untersuchung zur IT in der kantonalen Verwaltung.

10.3.2 Überprüfung der kantonalen Informatik

Erst zweieinhalb Jahre nach den Feststellungen der Finanzkontrolle leitete der Regierungsrat im September 2015, mit Verweis auf deren Bericht und die laufende Untersuchung der GPK, seinerseits die Überprüfung der kantonalen IT ein. Gemäss dem Regierungsratsbeschluss hatte ein externer Auftragnehmer die bestehende Informatikstrategie, -steuerung und -organisation, ausgewählte Fachanwendungen, Querschnittsapplikationen sowie die IT-Grundversorgung zu analysieren und Verbesserungen vorzuschlagen. Der Finanzdirektor, Ernst Stocker, die Justizdirektorin, Jacqueline Fehr, und die Bildungsdirektorin, Silvia Steiner, begleiteten das Projekt.[570] Der Finanzdirektor gab gegenüber der PUK Datensicherheit an, nach seiner Erinnerung sei man aufgrund der Feststellungen und des allgemeinen Umbruchs in der Digitalisierungsland-

---

566 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 13; Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 19–20.

567 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 6–9, 11–13.

568 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 19–20.

569 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 15; Protokoll der Befragung von Ursula Gut-Winterberger vom 20. September 2024, S. 17–18; Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 11.

570 RRB Nr. 883/2015 vom 15. September 2015, Unabhängige Überprüfung der Informatik des Kantons Zürich (Auftrag).

schaft zum Schluss gekommen, dass eine Überprüfung angezeigt sei.[571] Der wichtige Anstoss hierzu stammte wohl von der KITT-Geschäftsstelle.[572] In der Folge konnte der Finanzdirektor seine Kolleginnen und Kollegen im neu gewählten Regierungsrat davon überzeugen, dass bei der Grundversorgung eine Zentralisierung notwendig sei.[573]

Der Regierungsrat beauftragte die BDO AG mit der Untersuchung zur Situation der kantonalen Informatik. Neben einer beachtlichen Dokumentenerhebung und -analyse führte die BDO AG zwischen März und Oktober 2016 auch zahlreiche Gespräche mit IT-Verantwortlichen und Personen aus der kantonalen Verwaltung und legte dann ihren Bericht vor.[574] Die Finanzkontrolle hatte ihre früheren Feststellungen und diesbezüglichen Unterlagen an die BDO übergeben und war folglich von den Aussagen der BDO nicht überrascht.[575] Die Ergebnisse des Berichts deckten sich mit den Eindrücken des befragten Informatik-Sicherheitsbeauftragten, Renzo Mühlebach.[576]

Aus Sicht der Autoren des Berichts waren die strategischen Grundlagen des Kantons zwar weitsichtig und angemessen, die KITT-Organisation für deren Umsetzung aber ungeeignet. Der Bericht kam zum Schluss, dass die Umsetzung hinsichtlich verwaltungsweiter, direktionsübergreifender Themen gescheitert sei. In Bezug auf die Querschnitts- und Fachapplikationen hielten die Autoren fest, dass die Ziele der KITT-Verordnung aus dem Jahr 2006, zum Beispiel «eine Anforderung, eine Lösung», in Bezug auf die Anwendungsentwicklung nicht umgesetzt worden waren. Bei der Grundversorgung habe die angestrebte Konsolidierung der über 40 Betriebsstandorte nicht einmal ansatzweise stattgefunden. Weiter bemängelte der Bericht die fehlende direktionsübergreifende Kultur[577] und kam überdies zum Schluss, dass die Aussage im Legislaturbericht 2011–2015, die Informatikstrategie 2008 sei abgeschlossen, schlicht falsch sei, da wesentliche Punkte der Informatikstrategie noch nicht umgesetzt seien.[578]

Betreffend die Informationssicherheit kam der Bericht zu folgender Kernaussage:

«Eine den Schutzbedürfnissen der Informationen und Anwendungen angepasste Informations- und IT-Sicherheit kann mit der aktuellen Organisationsform und den bestehenden Weisungen und Richtlinien nicht erreicht werden.»[579]

In diesem Umfeld einer vielfältigen und heterogenen IT-Landschaft mit unterschiedlichsten Systemen konnte der Informatik-Sicherheitsbeauftragte (I-SiBe), Renzo Mühlebach, nur generelle Leitplanken setzen, die technologische Umsetzung musste weiterhin dezentral erfolgen.[580] Ohne eine zentrale IT-Infrastruktur konnte der I-SiBe auch keine eigene Auditaktivität entfalten und war darauf angewiesen, dass die Kontrollaktivitäten nach §§ 17 und 18 der ISV in den Direktionen tatsächlich stattfanden. Gemäss seiner Erinnerung hatte er jedoch nur von einer Direktion Kenntnis, in der regelmässig Audits stattfanden.[581]

---

571 Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 15.

572 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 28.

573 Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 9.

574 BDO AG, Unabhängige Überprüfung der Informatik des Kantons Zürich, 31. Oktober 2016, S. 7–8.

575 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 13.

576 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 11.

577 BDO AG, Unabhängige Überprüfung der Informatik des Kantons Zürich, 31. Oktober 2016, S. 6.

578 BDO AG, Unabhängige Überprüfung der Informatik des Kantons Zürich, 31. Oktober 2016, S. 15.

579 BDO AG, Unabhängige Überprüfung der Informatik des Kantons Zürich, 31. Oktober 2016, S. 60.

580 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 8.

581 Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 17–18.

Die kurz voher erfolgte Besetzung der Stelle des I-SiBe führte gemäss dem BDO-Bericht dazu, dass sich die Verwaltungseinheiten auf keine verbindlichen kantonalen Vorgaben zu einem Informationssicherheits-Managementsystem (ISMS) abstützen konnten. Damit in Zusammenhang stand auch der damals noch ausstehende Abschluss der Überarbeitung der Informationssicherheitsverordnung (ISV) und der Erstellung einheitlicher Weisungen und Vorgaben für Informationssicherheit. Die Autoren empfahlen deshalb, die geplanten Massnahmen mit hoher Priorität zu bearbeiten und fertigzustellen. Um den Rollenkonflikten, die der Informationssicherheit abträglich waren, und dem fehlenden Informationssicherheits-Know-how entgegenzutreten, regten sie überdies an, für die FAGIS dezidierte IT-Sicherheitsfachleute anzustellen resp. den Personen, welche die Direktionen in der FAGIS vertreten, ein ausreichendes Zeitbudget für diese Aufgabe zur Verfügung zu stellen.[582]

10.3.3 Projekt zur neuen kantonalen IT und Erarbeitung der kantonalen IKT-Strategie

Trotz gewissen Vorbehalten gegenüber dem BDO-Bericht, namentlich bezüglich der zu wenig berücksichtigten Komplexität der kantonalen Verwaltung und Möglichkeiten zur Vereinheitlichung, teilte der Regierungsrat die Schlussfolgerung, dass die kantonale Informatik neu zu organisieren und verstärkt zu harmonisieren sei. Die bestehenden, direktionsübergreifend wirkenden Organisationseinheiten sollten zusammengeführt und/oder abgelöst werden. Dazu formierte man einen Projektausschuss, dem wiederum der Direktionsvorsteher der Finanzdirektion, Ernst Stocker, sowie die Direktionsvorsteherinnen der Direktion der Justiz und des Innern, Jacqueline Fehr, und der Bildungsdirektion, Silvia Steiner, angehörten.[583] Im Ausschuss herrschten unterschiedliche Ansichten darüber, inwieweit eine übergreifende Strategie zielführend sei. Es folgten intensive Diskussionen und Aushandlungsprozesse über das Ausmass der anzustrebenden Zentralisierung, wobei die Justizdirektorin und der Finanzdirektor einer stärkeren Zentralisierung wohl positiver gegenüberstanden als die Bildungsdirektorin. Für Letztere war die Berücksichtigung der direktionsspezifischen Sachverhalte wesentlich.[584] Mit dem Grundsatzentscheid, die IKT-Grundversorgung künftig gesamtkantonal zu organisieren, die Fachapplikationen in den Direktionen und der Staatskanzlei zu belassen und zwei Standorte für Rechenzentren vorzusehen, fand man schliesslich eine gemeinsam getragene Lösung. Die Kantonspolizei, die gemäss dem BDO-Bericht und nach Ansicht des Datenschutzbeauftragten bezüglich der Informationssicherheit bereits gut aufgestellt war, war nicht Bestandteil des Projekts.[585] Im Rahmen eines gemeinsamen Lernprozesses verständigte sich der Regierungsrat auf diese Ausnahme und verhinderte damit aus Sicht des zuständigen Direktionsvorstehers, Mario Fehr, einen Rückschritt bei der Kantonspolizei in Bezug auf die Informationssicherheit.[586]

---

582 BDO AG, Unabhängige Überprüfung der Informatik des Kantons Zürich, 31. Oktober 2016, S. 61.

583 RRB Nr. 68/2017 vom 25. Januar 2017, Grundlagen für eine zukünftige kantonale Informations- und Kommunikationstechnologie (IKT), Auftrag.

584 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 17–18; Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 9–10.

585 RRB Nr. 780/2017 vom 30. August 2017, Neue kantonale IKT (Informations- und Kommunikationstechnologie), strategische Eckpfeiler.

586 Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 10.

10.3.4 IKT-Strategie vom 25. April 2018

In der Sitzung vom 25. April 2018 genehmigte der Regierungsrat die neue IKT-Strategie und ermöglichte damit die Ablösung der KITT-Organisation durch das neugeschaffene Amt für Informatik (AFI), welches die Zuständigkeit für die standardisierte Grundversorgung und die diesbezüglichen Beschaffungen übernahm. Damit wurde das heutige Dreischichtenmodell aus kantonaler IKT-Grundversorgung, Kantonsapplikationen und Fachapplikationen Realität. Die parlamentarische Subkommission IKT und Digitale Verwaltung, welche die Umsetzung der IKT-Strategie und der Strategie Digitale Verwaltung 2018–2023 (siehe folgender Abschnitt) begleitet hatte, zeigte in ihrem Bericht die diesbezüglichen Umsetzungsarbeiten übersichtlich auf.[587]

Mit der IKT-Strategie wollte man das Management der IKT-Sicherheit als Teil der übergeordneten Informationssicherheit verwaltungsweit umsetzen.[588] In diesem Bereich legte die IKT-Strategie fest, dass die Zuständigkeiten und diesbezüglichen Massnahmen in der IVSV und der AISR zu regeln sind. Sie sah auch ein Informations- und Sensibilisierungsprogramm sowie die Schaffung eines operativen Security Operation Center (SOC) zur Behandlung von Sicherheitsvorfällen vor.

Nach Ansicht des Finanzdirektors hatte der Regierungsrat nach dem BDO-Bericht den Handlungsbedarf erkannt und verschiedene Schritte unternommen. Namentlich mit der vom Regierungsrat getragenen Vereinheitlichung der Grundversorgung machte der Kanton in seinen Augen einen «Riesenschritt in eine neue Welt».[589] Die damit einhergehende Standardisierung der Arbeitsplätze hatte aus Sicht des ehemaligen Staatsschreibers, Beat Husi, auch positive Auswirkungen auf die Informatiksicherheit.[590]

10.3.5 Strategie Digitale Verwaltung 2018–2023 vom 25. April 2018

Für den Umgang mit der fortschreitenden Digitalisierung beauftragte der Regierungsrat 2016 die Staatskanzlei, eine Strategie «Digitale Verwaltung» sowie einen Umsetzungsplan zu erarbeiten, um die auslaufende E-Government-Strategie abzulösen. Mit der Strategie und dem damit verbundenen Impulsprogramm verfolgte man das Ziel, den Herausforderungen der digitalen Transformation zu begegnen, deren interdisziplinärem Charakter gerecht zu werden und damit die Massnahmen in den unterschiedlichsten Handlungsfeldern zu koordinieren und zu steuern.[591]

Die Herausforderungen der Digitalisierung bezüglich des Datenschutzes oder der Informationssicherheit waren kein wesentliches Element der Strategie. Folglich äusserte sich der Datenschutzbeauftragte in seinem Tätigkeitsbericht 2018 kritisch zur Strategie:

«Der richtige und sichere Umgang mit den Daten ist kritisch für die Akzeptanz und das Vertrauen der betroffenen Personen. Wie diesen Herausforderungen der Digitalisierung begegnet wird, bleibt mit der vorliegenden Strategie weitgehend offen. Dafür bräuchte es eine Politik der Datenvermeidung und der Datensparsamkeit als Teil der Strategie der Digitalisierung. Der Datenschutzbeauftragte schlug deshalb vor, dass das Leitbild mit einem übergeordneten Zweck ergänzt wird, der mit der Digitalisie-

---

587 Bericht der Subkommission IKT und Digitale Verwaltung über die Umsetzung der kantonalen IKT-Strategie und der Strategie Digitale Verwaltung 2019–2023 vom 23. März 2023 (KR-Nr. 67/2023).

588 RRB Nr. 383/2018 vom 25. April 2018, Kantonale IKT-Strategie (Organisation und Umsetzung), Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung (Änderung).

589 Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S.10, 15–16.

590 Protokoll der Befragung von Beat Husi vom 5. Juli 2024, S. 15.

591 RRB Nr. 390/2018 vom 25. April 2018, Strategie Digitale Verwaltung des Kantons Zürich 2018–2023; Festsetzung.

rung im Kanton Zürich erreicht werden soll. Darin müsste zum Ausdruck kommen, dass die Digitalisierung zur Stärkung des Rechtsstaats und seiner Institutionen, der föderalen Demokratie und der Grundrechte beitragen soll.»[592]

Neben dem Entscheid, die Informationssicherheit nicht mehr detailliert in einer Verordnung zu regeln (siehe Kapitel 10.2.3), widerspiegelt für den ehemaligen Datenschutzbeauftragten, Bruno Baeriswyl, die fehlende Berücksichtigung der Thematik auf der strategischen Ebene durch den Regierungsrat die Marginalisierung von Datenschutz und Informationssicherheit in der Digitalisierung.[593] Institutionell bemängelte der Datenschutzbeauftragte, dass er keinen Einsitz in die entsprechenden Strategieorgane erhielt und auch nicht als Beobachter zugelassen wurde.[594]

Gemäss der heutigen Staatsschreiberin, Kathrin Arioli, ging man Fragen des Datenschutzes bei der Umsetzung des Impulsprogramms der Strategie Digitale Verwaltung jeweils konkret auf der Projektebene an. Aus ihrer Sicht ist es wichtiger, dass die Datenschutzthemen bei der konkreten Umsetzung berücksichtigt werden. Die Verwirklichung des Datenschutzes hängt nach ihren Aussagen nicht von der Verankerung des Themas in einem Leitbild ab.[595]

10.3.6 Zuständigkeiten gemäss den neuen strategischen Grundlagen

Der Regierungsrat hatte die Entwicklung der neuen IKT-Strategie eng begleitet. Im Bewusstsein um die Tragweite der Themen der Digitalisierung in der Verwaltung sowie der Organisation der kantonalen IKT, war für ihn ein starkes Engagement der obersten Führungsebene endlich im Fokus. Er setzte zur Führung der beiden Strategien das Gremium Steuerung Digitale Verwaltung und kantonale IKT (SDI) ein. Unter dem Vorsitz der Staatsschreiberin haben darin der Finanzdirektor, die Direktorin der JI sowie die Bildungsdirektorin Einsitz. Die weiteren Direktionen werden durch die Generalsekretärinnen oder Generalsekretäre vertreten.[596] Die Empfehlung der GPK, im IT-Management künftig eine starke Führungsrolle des Regierungsrates und seiner Mitglieder vorzusehen und ein strategisches Führungs- und Leitungsgremium unter Einbezug von Regierungsratsmitglieder einzusetzen, nahm der Regierungsrat damit auf.[597]

Mit der IKT-Strategie kam auch Bewegung in das bis anhin stiefmütterlich behandelte Thema der Informationssicherheit.[598]

– Die übergeordnete strategische und finanzielle Steuerung der IKT kommt gemäss Ziff. 16 der IKT-Strategie nun dem Gesamtregierungsrat zu.
– Nach Ziff. 17 der IKT-Strategie liegt die Verantwortung für die kantonale Steuerung der IKT und der digitalen Verwaltung beim Gremium SDI. Es steuert u. a. die Umsetzung der IKT-Strategie, erlässt die verbindlichen Vorgaben und legt die Kantonsapplikationen fest. Die Besonderen Informationssicherheitsrichtlinien (BISR), welche die AISR konkretisieren, hat nach Ziff. 11 der IKT-Strategie das Amt für Informatik (AFI) in Zusammenarbeit mit den Direktionen zu erstellen. Konkret verabschiedet die Fachgruppe Informatiksicherheit (FAGIS) die BISR zuhanden des SDI, das sie dann erlässt.

---

592 Tätigkeitsbericht 2018 des Datenschutzbeauftragten, April 2019, S. 38.

593 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 9–11, 13.

594 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 10.

595 Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 11.

596 RRB Nr. 392/2018 vom 25. April 2018, Steuerung Digitale Verwaltung und kantonale IKT, Vertretungen und Konstituierung.

597 Bericht der Geschäftsprüfungskommission (GPK) über die vertiefte Untersuchung zur IT in der kantonalen Verwaltung vom 13. Juli 2017 (KR-Nr. 2003/2017), S. 25.

598 Kanton Zürich, Kantonale IKT-Strategie. Festgesetzt vom Regierungsrat am 25. April 2018.

– Als weiteres zentrales Gremium entstand mit der IKT-Strategie die Operative Informatiksteuerung (OIS, Ziff. 20 der IKT-Strategie). Sie übernimmt die Rolle des Koordinations- und Konzeptgremiums für verwaltungsweit relevante, fachtechnische Fragen. Namentlich nimmt sie als vorbereitendes Gremium zuhanden des SDI Stellung zu strategischen Fragen, prüft die Anträge der Direktionen und der Staatskanzlei an die Regierung und beurteilt Anträge über die finanziell bedeutsamen Fach- und Kantonsapplikationen. Sie besteht aus dem Leiter des AFI, Hansruedi Born, sowie den IKT-Verantwortlichen der einzelnen Direktionen und der Staatskanzlei. Falls innerhalb des OIS bezüglich der Grundversorgung keine Einigung erzielt werden kann, ist das Gremium SDI die Eskalationsstelle.

10.3.7 Strategie Digitaler Wandel an den Schulen der Sek II (DiWaSek II)

Versuche zur stärkeren Zentralisierung der IT waren gemäss dem ehemaligen Regierungsrat, Martin Graf, bei der Bildungsdirektion mit Problemen verbunden; dies wegen ihrer Verbindungen zu den dezentral organisierten Schulen.[599]

Vor dem Hintergrund der sehr heterogenen IKT-Strukturen an der Sekundarstufe II verabschiedete der Regierungsrat daher bereits im März 2019 eine Strategie zum digitalen Wandel an den Schulen der Sek II.[600] Darin war in einem strategischen Ziel zur Informationssicherheit festgehalten, dass alle Beteiligten für den Datenschutz und die Datensicherheit zu sorgen haben. Das Mittelschul- und Berufsbildungsamt (MBA) erhielt den Auftrag, für die Schulen Dienstleistungen im Bereich des Datenschutzes und der Datensicherheit sowie für die Erarbeitung von Standards und Empfehlungen zur Verfügung zu stellen.

Das MBA und die kantonalen Mittel- und Berufsfachschulen waren von der IKT-Strategie erfasst, weshalb der Regierungsrat die Finanzdirektion mit der Durchführung des Projekts «IKT-Grundversorgung Sek II» als Teil des IKT-Programms beauftragte.[601] Vom allgemeinen Regierungsratsbeschluss zur Umsetzung der Informationssicherheit in den Direktionen und der Staatskanzlei war das MBA jedoch ausgenommen.[602] Für die über 60 000 Nutzerinnen und Nutzer der 18 kantonalen Berufsfachschulen und 21 kantonalen Mittelschulen schuf der Regierungsrat mit RRB Nr. 1178/2019 eine eigene Stelle. Die IKT-Sicherheitsbeauftragte beim MBA sollte die Strukturen des Datenschutzes und der Datensicherheit aufbauen, sich mit dem IKT-Sicherheitsbeauftragten des Kantons (ISIK) und der IKT-Sicherheitsbeauftragten der Bildungsdirektion koordinieren und im Hinblick auf den Aufbau der kantonalen Sicherheitsorganisation abstimmen.[603]

Aus Sicht der Bildungsdirektorin, Silvia Steiner, benötigt die geteilte Zuständigkeit zwischen dem AFI und dem MBA einen ständigen Dialog und Austausch, ermöglicht aber eine passgenaue Lösung unter Berücksichtigung der jeweiligen Fachkenntnisse.[604]

---

599 Protokoll der Befragung von Martin Graf vom 20. September 2024, S. 12.

600 RRB Nr. 259/2019 vom 20. März 2019, Strategie «Digitaler Wandel an kantonalen Schulen der Sekundarstufe II».

601 RRB Nr. 260/2019 vom 20. März 2019, Projekt «IKT-Grundversorgung an den kantonalen Schulen der Sekundarstufe II».

602 RRB Nr. 1193/2020 vom 2. Dezember 2020, Informationssicherheit, Umsetzung in den Direktionen und der Staatskanzlei (Stellenpläne, gebundene Ausgabe).

603 RRB Nr. 1178/2019 vom 10. Dezember 2019, Erarbeitung der Grundlagen zur Umsetzung der Strategie «Digitaler Wandel an kantonalen Schulen der Sekundarstufe II», gebundene Ausgabe, Stellenplan.

604 Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 9.

10.4 Würdigung durch die PUK

Die PUK Datensicherheit stellt fest, dass der Regierungsrat ab 2015 in Bezug auf die Neuausrichtung der kantonalen Informatik wesentliche Schritte unternommen hat, wobei sicherlich die Impulse durch den von ihm in Auftrag gegebenen BDO-Bericht und die Arbeit der GPK ausschlaggebend waren. Die Zentralisierung der Grundversorgung und die Einführung des Digitalen Arbeitsplatzes (DAP) haben den Kanton in Bezug auf die Informationssicherheit weitergebracht. Bei der Ausgestaltung der Informationssicherheitsorganisation sowie der Schaffung rechtlicher Grundlagen waren hingegen lange keine Fortschritte zu verzeichnen.

Zwar hatte der Regierungsrat 2015 die Stelle des Informatik-Sicherheitsbeauftragten (I-SiBe) geschaffen. Die Etablierung einer wirklichen Sicherheitsorganisation folgte aber nicht. Der Informatik-Sicherheitsbeauftragte war äusserst bemüht, doch die Rahmenbedingungen waren wegen der fehlenden Funktionentrennung innerhalb der FAGIS und der ungünstigen Verortung der Stelle ohne Zugang zum Regierungsrat sehr schwierig. Zudem hatte es der Regierungsrat versäumt, die Sicherheitsorganisation bereits früher breiter aufzustellen und dezidierte Stellen für Fachpersonen der Informationssicherheit in den Direktionen und der Staatskanzlei zu schaffen. Damit verzichtete er bewusst auch auf die Umsetzung der diesbezüglichen Empfehlung aus dem BDO-Bericht. Der aktive Widerstand aus den Direktionen, das vorherrschende enge Verständnis von Informationssicherheit als Informatiksicherheit sowie der Verzicht auf eine Weisungsbefugnis schränkten den Aktionsradius des Informatik-Sicherheitsbeauftragten (I-SiBe) ebenfalls ein. In diesem Umfeld war auch die Erarbeitung von verbindlichen neuen Grundlagen erschwert.

Für die PUK Datensicherheit ist nicht nachvollziehbar, weshalb der Regierungsrat den I-SiBe nicht mit einem Weisungsrecht ausgestattet hat. Die Kommission kann sich dies nur damit erklären, dass die einzelnen Direktionen und die Staatskanzlei einen entsprechenden Machtverlust nicht hinnehmen wollten.

Obwohl bereits 2015 ein detaillierter Entwurf für eine neue Informationssicherheitsverordnung (ISV) erarbeitet worden war, dauerte es noch weitere fünf Jahre, bis die Verordnung über die Informationsverwaltung und -sicherheit (IVSV) 2020 in Kraft trat. Die Verzögerung bei diesem Geschäft, welches für die Informationssicherheit von eminenter Bedeutung war, zeigt für die PUK Datensicherheit, dass der Informationssicherheit vonseiten des Regierungsrates keine Priorität eingeräumt wurde.

Mit dem Erlass der neuen IVSV 2019, die kaum noch Paragrafen zur Informationssicherheit enthält, hat der Regierungsrat zudem entschieden, die konkreten Regelungen zur Informationssicherheit (AISR) auf einer hierarchisch tieferen Normstufe zu regeln. Dies ist angesichts der Tatsache, dass der Bund 2020 die Informationssicherheit in einem neuen Erlass auf Gesetzesstufe geregelt hat, ziemlich erstaunlich.[605] Damit ist auch die ursprünglich in der ISV vorgesehene Regelung der Datenbearbeitung durch Dritte entfallen. Zwar hat der Regierungsrat 2015 die Allgemeinen Geschäftsbedingungen (AGB) für verbindlich erklärt. Aus Sicht der PUK Datensicherheit hat diese Lösung jedoch im Vergleich mit einer Regelung auf Verordnungsstufe nicht dieselbe Bedeutung. Die PUK Datensicherheit ist – im Gegensatz zur Argumentation im RRB Nr. 670/2015 – nicht davon überzeugt, dass die Massnahmen zum Schutz der Daten (§ 7 IDG) mit der Verbindlichkeitserklärung der heutigen AGB im Bereich der Informationsbearbeitung durch Dritte ausreichend konkretisiert sind. Die AGB sind um zusätzliche Vorgaben zu erweitern. Generell ist die PUK Datensicherheit jedoch der

[605] Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG; SR 128).

Ansicht, dass auch die Regelungen der Datenbearbeitung auf Verordnungsstufe zu regeln sind. Darüber hinaus sind auch die weiteren genauen Bestimmungen zur Informationssicherheit rechtlich stärker zu verankern.

Weiter dauerte es viel zu lange, bis die Richtlinien zur Informationssicherheit, die AISR und die BISR, vorlagen. Unverständlicherweise rückten durch die Priorisierung der laufenden strategischen Arbeiten rund um die Neuausrichtung der Informatik die Bemühungen zur Etablierung von Grundlagen zur Informationssicherheit in den Hintergrund. Dem Informatik-Sicherheitsbeauftragten (I-SiBe) fehlten lange die dazu nötigen Ressourcen. Schliesslich teilt die PUK Datensicherheit die Einschätzung des ehemaligen Datenschutzbeauftragten, dass die AISR und die BISR im Gegensatz zu einer Verordnung weniger gut geeignet sind, den Mitarbeitenden der Verwaltung eine Orientierung zu geben. Deshalb ist die AISR als Verordnung zu erlassen, um ihr mehr Gewicht und Geltungskraft zu verleihen.

Mit der Verabschiedung der IKT-Strategie, der Strategie Digitale Verwaltung sowie der Strategie Digitaler Wandel an den Schulen Sek II hat der Regierungsrat in den Jahren 2018/2019 die Basis der heutigen IT-Governance gelegt. Diesbezüglich ist die PUK Datensicherheit der Ansicht, dass die Informationssicherheit angesichts der vielfältigen und komplexen Dynamik in der digitalen Transformation auch auf der Ebene der strategischen Überlegungen zu behandeln ist. Es reicht nicht, diese Fragen nur im Kontext der Organisation oder der konkreten Projekte zu berücksichtigen. Aus Sicht der PUK Datensicherheit wurde die Informationssicherheit in den Digitalisierungsstrategien bisher nicht zufriedenstellend berücksichtigt.

11. Entwicklungen in der Direktion der Justiz und des Innern (JI) 2015–2020

11.1 Personelle und organisatorische Anpassungen

11.1.1 Wechsel des Direktionsvorstands

Der bisherige Direktionsvorsteher Martin Graf wurde am 12. April 2015 nicht wieder in den Regierungsrat gewählt und Jacqueline Fehr wurde seine Nachfolgerin. Gemäss ihrer Aussage hat sie sich mit ihrem Vorgänger bei zwei eher informellen Treffen über die Amtsübergabe ausgetauscht, ohne dass in diesem Rahmen eine systematische Einführung möglich gewesen wäre. Da die Direktionsverteilung offiziell erst mit der Konstituierung im Kantonsrat erfolgt, ist eine systematische Einarbeitung unter Einbezug der Mitarbeitenden nicht möglich.[606] Die neue Direktionsvorsteherin, Jacqueline Fehr, erfuhr auf Nachfrage die Vorgeschichte zum kurz zuvor erfolgten Wechsel in der Leitung des Bereichs Logistik, Finanzen und Controlling (LFC). Aufgrund der Schilderungen zur Situation in der Informatik der JI zu jener Zeit gewann sie den Eindruck, dass der ehemalige Leiter LFC, Renato Widmer, als Chef alles dominierte und der damalige Leiter der JI-Informatik, Fredi Steiner, klar untergeordnet war und keine eigenen Entscheidungsbefugnisse und somit keine echte Verantwortung hatte. Bei ihrem Amtsantritt war die Reorganisation jedoch bereits erfolgt: Fredi Steiner war neu für den Teil der Informatik und der Direktionscontroller für den Bereich Logistik und Finanzen zuständig.[607]

Die Direktionsvorsteherin, Jacqueline Fehr, kam unmittelbar mit dem hohen technischen Sicherheitsstandard der JI und den damit verbundenen Auswirkungen auf die Arbeit in Kontakt. Die technische Sicherheit wurde 2016 mit der Diskverschlüsselung mittels Bitlocker zusätzlich verbessert.[608] Sie habe bereits damals gespürt, dass die IT-Mitarbeitenden der JI auf diesen hohen Sicherheitsstandard stolz waren.[609] Im Informatikbereich liess sich die Direktionsvorsteherin über den Stand bezüglich Beschaffung und Sicherheit sowie über die Organisation, Kompetenzen und Ressourcen informieren. Sie entschied jedoch angesichts der hohen Belastung durch andere Themen – hier ist sicherlich an die RIS-Entwicklung zu denken –, vorwärtszuschauen und sich nicht im Detail mit der Vergangenheit auseinanderzusetzen. Gegenüber der PUK Datensicherheit gab sie an, sie wisse nicht, ob dies ein Fehler gewesen sei.[610]

11.1.2 Wechsel der Generalsekretärin und Reorganisation des Generalsekretariats

Kurz nach ihrem Amtsantritt teilte die Direktionsvorsteherin, Jacqueline Fehr, dem damaligen Generalsekretär, Christian Zünd, mit, dass sie dessen Stelle mit einer langjährigen politischen Weggefährtin besetzen möchte.[611] Dabei handelte es sich um Jacqueline Romer. Diese führte gegenüber der PUK Datensicherheit aus, dass es Regierungsrätin Jacqueline Fehr ein Anliegen war, mit einer Person zusammenarbeiten zu können, die sie sehr gut kannte, von der sie genau wusste, wie sie arbeitete, und zu

606 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 14–15.

607 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 9–11.

608 Direktion der Justiz und des Innern, Technologieentwicklung JI Clients Timeline 1996 bis 2016.

609 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 7.

610 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 10.

611 Direktion der Justiz und des Innern, Generalsekretariat, Arbeitszeugnis Christian Zünd vom 31. März 2016.

der sie grosses Vertrauen hatte.[612] Als Jacqueline Romer am 16. Januar 2016 ihr Amt als Generalsekretärin antrat, war ihr Vorgänger bereits nicht mehr in der JI tätig, weshalb keine Einführung stattfinden konnte. Diese erfolgte durch seine Stellvertretung.[613] Der Übergabeprozess, welcher sich auf eine Übergabe der Akten zu den diesbezüglichen Finanzkontrollberichten beschränkte, erschwerte es der Generalsekretärin, Jacqueline Romer, sich ein vollständiges Bild über die frühere Situation in der IT zu machen.[614]

Die neue Generalsekretärin wollte sich stärker Managementaufgaben widmen und die Aufgaben so verteilen, dass ihre Funktion kein «Flaschenhals» blieb. Sie übernahm innerhalb des Generalsekretariats die Leitung der Querschnittthemen, darunter die Digitalisierung.[615] Sie habe anfangs den Blick stark auf die Informatik der JI, die grösste Abteilung des Generalsekretariats mit vielen laufenden Projekten, gelegt. Gemäss ihrem damaligen Eindruck hatte sich vorher im Generalsekretariat niemand mit dem Management der Informatik befasst. Wie ihr erzählt wurde, waren unter der «autarken» Führung des ehemaligen Leiters LFC, Renato Widmer, keine tiefen Einblicke in den Informatikbereich möglich. Das habe sie geändert und auch deshalb ihr besonderes Augenmerk darauf gerichtet.[616] Sie ging ab und zu vor Ort ins Bezirksgebäude und stand mit dem Leiter der JI-Informatik in engem Austausch. Einerseits liefen grosse Digitalisierungsprojekte und es galt zunehmend, Digitalisierungsfragen zu lösen, andererseits sah die Generalsekretärin aber auch Bedarf hinzuschauen, wie die Informatik der JI aufgestellt war und ihre Aufgaben umsetzte.[617]

Hinsichtlich IT-Sicherheit und diesbezüglicher Awareness konnte sie feststellen, dass das technische Sicherheitslevel sehr hoch war und die Daten gut geschützt waren. Aber auch die Sensibilisierung der Mitarbeitenden entsprach einem Standard, der ihrerseits keine Massnahmen erforderte.[618] Angesichts der späteren Feststellungen der Administrativuntersuchung räumte sie aber ein, dass wohl zu wenig Monitoring aus dem Generalsekretariat stattgefunden habe.[619]

Im Jahr 2016 erfolgte die vollständige Erneuerung sämtlicher PC-Arbeitsplätze. Die abgelöste Flotte von etwa 1850 Geräten wurde über einen etablierten Broker entsorgt respektive gelöscht. Zu diesem Zeitpunkt war André Gisler bereits nicht mehr für die JI tätig. Die PUK Datensicherheit konnte hier die Löschprotokolle aus dem Jahr 2017 einsehen.

11.1.3 Einführung eines Geschäftsverwaltungssystems

Rasch nach ihrem Amtsantritt musste die Direktionsvorsteherin, Jacqueline Fehr, über die Weiterentwicklung von RIS2 entscheiden. Sie entschied im September 2015 eine Überprüfung des Projekts anzuordnen. Aufgrund der Ergebnisse dieser Überprüfung beantragte die JI beim Regierungsrat Ende 2016, es sei darauf zu verzichten, RIS2 in weiteren Bereichen der JI einzuführen. Für die allgemeinen Verwaltungstätigkeiten wollte man in der JI stattdessen auf eine einheitliche Lösung für die Geschäftsverwaltung (GEVER) setzen.[620] Die damit beauftragte Generalsekretärin be-

---

612 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 17.

613 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 6.

614 Stellungnahme von Christian Zünd vom 1. November 2025 sowie Ergänzung vom 6. November 2025.

615 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 17–18, Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 11.

616 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 9.

617 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 7.

618 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 9, 17.

619 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 10.

620 RRB Nr. 1116/2016 vom 23. November 2016, RIS2-Überprüfung (Ergebnisse und weiteres Vorgehen).

mühte sich rasch, ein solches Geschäftsverwaltungssystem einzuführen.[621] Im Oktober 2017 konnte die GEVER im Generalsekretariat in Betrieb genommen werden. Die Einführung in den anderen Amtsstellen erfolgte schrittweise und konnte Ende 2019 abgeschlossen werden.[622] Den Umgang mit der GEVER regelte das Generalsekretariat mit Organisationsvorschriften.[623] Nach Aussage des Leiters der JI-Informatik[624] von 2018–2020, Axel Mayer, schuf man über das Geschäftsverwaltungssystem sehr viel Awareness für die Informationssicherheit.[625]

11.1.4 Personelle Wechsel in der IT-Leitung

Nach dem Abgang des Leiters LFC, Renato Widmer, war Fredi Steiner bereit, dessen Aufgaben zu übernehmen.[626] Er war ein pflichtbewusster Informatik-Experte, aber die Besetzung war damals ohne Ausschreibung und Bewerbungsverfahren erfolgt. Die Direktionsvorsteherin und die Generalsekretärin stellten fest, dass es Fredi Steiner an Führungserfahrung und den nötigen Managementkompetenzen fehlte, die es für die Weiterentwicklung der Informatik im Umfeld des technologischen Wandels und des laufenden Aufbaus des Amtes für Informatik brauchte. Sie entschieden sich deshalb 2017 für eine Neuausschreibung der Informatikleitung.[627] Fredi Steiner führte seinen Nachfolger ein und trat nach dessen Amtsantritt 2018 ins zweite Glied zurück.[628]

Axel Mayer trat seine Stelle am 1. Januar 2018 an und erhielt den Eindruck, dass man auf den grössten Sicherheitsrisikofaktor Mensch nicht vorbereitet war.[629] Die Informatik war technisch zwar gut aufgestellt, aber im Bereich der Awareness für Informationssicherheit, besonders bei den Mitarbeitenden und der Leitung der Ämter, bestanden noch Schwächen. Dies zeigte sich für ihn auch am Widerstand gegen das von ihm eingeführte sichere Drucken, das nur noch mit Chipkarte möglich war.[630] Darüber hinaus gab es keine Online-Trainings zur Datenklassifizierung und die geltende Richtlinie war veraltet.[631] Axel Mayer führte pilotweise Online-Trainings ein und begann mit der Überarbeitung der IT-Strategie der JI, welche die Bedürfnisse der einzelnen Ämter stärker berücksichtigte.[632] Auch im Bereich der Zeichnungsberechtigungen nahm er eine Straffung vor.[633]

---

621 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 8.

622 Direktion der Justiz und des Innern, Generalsekretariat, Schreiben vom 12. März 2025 mit Roadmap und Programmauftrag zu JI GEVER als Beilagen.

623 Direktion der Justiz und des Innern Generalsekretariat, Vorschriften über die Geschäftsverwaltung im Generalsekretariat der Direktion der Justiz und des Innern (Organisationsvorschriften) vom 12. Juli 2019.

624 Bis zur offiziellen Umbenennung der «Hauptabteilung Informatik» in «Digital Solutions (DigiSol)» vom 1. Juli 2021 mit der Änderung der Organisationsverordnung (JIOV) ist in diesem Bericht immer von JI-Informatik die Rede. Aus dem Staatskalender 2019/2020 geht hervor, dass die Bezeichnung Digital Solutions aber bereits früher üblich war.

625 Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 9.

626 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 33.

627 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 9; Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 10.

628 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 6.

629 Staatsanwaltschaft III, Delegierte Einvernahme von Axel Mayer vom 24. Juli 2023, S. 37.

630 Direktion der Justiz und des Innern, Generalsekretariat, Digital Solutions, Merkblatt «FollowMe-Printing mit Chipkarte» und Merkblatt zur neuen Chipkarte.

631 Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 10.

632 Es existiert ein Strategieentwurf aus dem Jahr 2018. Seit 2022 ist die Digital Solutions daran einen neuen Entwurf zu erarbeiten, der dann dem strategischen und operativen Gremium vorgelegt werden soll.

633 Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 6–8.

Aus Sicht der Generalsekretärin, Jacqueline Romer, hat Axel Mayer in seiner Zeit als Leiter von 2018 bis 2020 in den gewachsenen Strukturen der Informatik der JI einiges bewegt und installiert.[634] Axel Mayer gab gegenüber der PUK Datensicherheit an, dass sowohl bei der Direktionsvorsteherin als auch der Generalsekretärin ein gutes Bewusstsein dafür vorhanden war, dass das Thema Informationssicherheit verfolgt und fachlich sauber geregelt werden muss. Seine Rückmeldungen hätten sie aufgenommen und ihm auch Rückendeckung gegeben.[635]

11.1.5 IT-Beschaffungen 2018/2019

Axel Mayer gab an, aufgrund der negativen Erfahrungen habe die Beschaffungsthematik in der JI-Informatik eine hohe Aufmerksamkeit genossen und auch er habe als Leiter in seiner Amtszeit Beschaffungen «extrem stark beobachtet».[636]

Angesichts von etwa 200 bis 300 unbenutzten Desktopgeräten, die in Schränken eingelagert waren, musste der Leiter der JI-Informatik feststellen, dass vor seiner Zeit zu viele Geräte beschafft worden waren.[637] Laut dem RRB Nr. 387/2016 war eine Reserve von 5%, also von etwa 90 Geräten, explizit vorgesehen. Der ehemalige Leiter der JI-Informatik gab in seiner Stellungnahme dazu an, dass die eingelagerten Desktopgeräte eine Folge der geänderten Bedürfnisse der Nutzenden waren. Auf Wunsch tauschte man nachträglich Desktopgeräte durch Notebooks aus und lagerte die Desktopgeräte ein.[638]

Als 2018 die Druckerflotte ersetzt wurde, geschah dies über bestehende Rahmenverträge der kdmz.[639] 2019 fand eine Erneuerung der Infrastruktur der Rechenzentren statt. Mittels einer Ausschreibung wurden die verschiedenen Lose an Informatikunternehmen vergeben.[640] Die physische Zerstörung der alten Server wurde gemäss Aussage des damaligen Leiters der JI-Informatik, Axel Mayer, vom Leiter des Data-Centers, also dem Zuständigen für die Rechenzentren, begleitet und auch dokumentiert.[641] Auch hier liegen der PUK Datensicherheit Bestätigungen über die Vernichtung von Bändern und Harddisks vor.

In diese Zeit fiel auch die Beschaffung von iPads in der JI. Mit der Registrierung hatten laut Axel Mayer die Benutzer zu bestätigen, die entsprechende Nutzungsrichtlinie zur Kenntnis genommen zu haben.[642] Die Geräte waren zentral verwaltet und vor unbefugtem Zugriff geschützt. Beim Austritt aus der JI hatte eine Meldung an den Servicedesk zu erfolgen. Mit der Rückmeldung wurde das Gerät gewiped, also sicher gelöscht. Alle herausgegebenen Geräte kamen zurück.[643]

---

634 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 19.

635 Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 9.

636 Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 17.

637 Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 15–16.

638 Stellungnahme von Fredi Steiner vom 5. November 2025.

639 RRB Nr. 1221/2018 vom 12. Dezember 2018, Ersatzbeschaffung Druckerflotte 2018 (Ausgabenbewilligung, Auftragserteilung).

640 RRB Nr. 501/2019 vom 22. Mai 2019, Ersatzbeschaffung Rechenzentrum (Ausgabenbewilligung und Vergabe).

641 Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S 22.

642 Direktion der Justiz und des Innern, Generalsekretariat, Digital Solutions, Richtlinien zum Einsatz von mobilen Geräten vom 30. April 2019.

643 Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 14–15.

11.1.6 Neue Prozesse bei Amtsübergaben

Auch aufgrund der eigenen Erfahrungen machten sich die Direktionsvorsteherin und die Generalsekretärin Gedanken, wie der Wissenstransfer im Rahmen von Amtsübergaben besser ausgestaltet werden könnte. Dazu befassten sie sich 2019 auch mit dem Bericht zur Administrativuntersuchung bei Entsorgung und Recycling Zürich (ERZ), der festhielt, dass die Leitung zu wenig Kontrolle, Führung und kritisches Hinterfragen angetroffen habe. Infolge mehrfachen Wechsels der politisch Verantwortlichen und Fehlens von systematischen Amtsübergaben war eine konsistente Aufsicht fast nicht möglich.[644]

Auf Basis dieser Erkenntnisse passte die JI ihre internen Übergabeprozesse an, sodass bei Leitungswechseln in grossen Ämtern die bestehenden Probleme nun aktiv über Gespräche und Formulare abgeholt werden.[645]

11.2 Räumungsaktion 2019

11.2.1 Vorgeschichte

Der Schlussbericht der Administrativuntersuchung (siehe Kapitel 12.3) wies darauf hin, dass im Jahr 2019 bei der JI-Informatik eine grosse Menge physischer Akten vernichtet worden sei. Diese Aussage stützte sich auf ein im Dezember 2020 verfasstes Memo des heutigen Leiters Operation Management, Fredi Steiner, der von 2000 bis 2017 selbst Leiter der JI-Informatik gewesen war. Weiter hielt der Schlussbericht fest, es könne davon ausgegangen werden, dass unter anderem Arbeitsrapporte und Verträge von externen Dienstleistern entsorgt worden seien[646] und diese Entsorgung auf Anweisung des damaligen Leiters der JI-Informatik, Axel Mayer, veranlasst worden sei.[647]

Im Rahmen des Point de Presse vom 6. Dezember 2022 (siehe Kapitel 13.6) der Direktionsvorsteherin, Jacqueline Fehr, gaben sie und die Autorin des Schlussberichts auch gegenüber der Öffentlichkeit in diesem Sinne Auskunft zur mutmasslichen Aktenentsorgung im Jahr 2019.[648]

Nachdem der Leitende Oberstaatsanwalt von der Administrativuntersuchung erfahren und den Schlussbericht erhalten hatte, erfolgte der Entscheid, den Aspekt der Datenentsorgung, wovon die Aktenentsorgung 2019 ein Element war, ergänzend zur damals bereits laufenden Untersuchung der Staatsanwaltschaft Zürich-Sihl, genauer zu untersuchen.[649] Die Ermittlungen der Staatsanwaltschaft III zeigten inzwischen jedoch, dass die Entsorgung im Jahr 2019 im Zusammenhang mit einer Aufräumaktion stand und sich der Verdacht bezüglich einer Urkundenunterdrückung nicht erhärten liess.[650] Im Rahmen der Kantonsratsdebatte vom 9. Januar 2023 zur dringlichen

---

644 Thomas Poledna, Bericht zur Administrativuntersuchung ERZ vom 31. Januar 2019, S. 48, 290.

645 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 15.

646 IT & Law Consulting GmbH, Administrativuntersuchung bei der Direktion der Justiz und des Innern des Kantons Zürich im Zusammenhang mit dem Umgang von Informationen und Datenmissbrauch, Schlussbericht vom 30. März 2021, S. 9; Direktion der Justiz und des Innern, Generalsekretariat, Digital Solutions, Memo von Fredi Steiner vom 10. November 2020 «Mögliches Datenleck IT JI».

647 IT & Law Consulting GmbH, Administrativuntersuchung bei der Direktion der Justiz und des Innern des Kantons Zürich im Zusammenhang mit dem Umgang von Informationen und Datenmissbrauch, Schlussbericht vom 30. März 2021, S. 12.

648 Direktion der Justiz und des Innern, Point de Presse vom 6. Dezember 2022 «Konsequenzen aus dem Datensicherheitsvorfall bei der Direktion JI».

649 Protokoll der Befragung von Andreas Eckert vom 28. Februar 2022, S. 11–12; Oberstaatsanwaltschaft, Medienmitteilung vom 6. Dezember 2022 «Staatsanwaltschaft prüft mögliches strafrechtliches Fehlverhalten bei Datenentsorgung vertieft».

650 Protokoll der Befragung von David Zogg und Mathias Eberli vom 3. Mai 2024, S. 14.

Interpellation (KR-Nr. 462/2022) gingen verschiedene Mitglieder des Kantonsrates auf die Verantwortlichkeit der Direktionsvorsteherin, Jacqueline Fehr, für die Aktenvernichtung 2019 ein und forderten eine politische Aufarbeitung des Sachverhalts. Sie äusserte sich im Kantonsrat dahingehend, dass es sich um einen strafrechtlich nicht relevanten, aber sehr groben verwaltungstechnischen Fehler gehandelt habe, da wohl ein früherer IT-Experte aus der Privatwirtschaft aufräumen und entrümpeln wollte.[651]

Die PUK Datensicherheit ging diesen Sachverhalten nach und klärte ab, inwiefern hier die geltenden Archivbestimmungen oder weitere Bestimmungen nicht eingehalten wurden und wer dafür die Verantwortung trägt.

11.2.2 Geltende Bestimmungen zur Archivierung

Gemäss § 8 des Archivgesetzes[652] sind die öffentlichen Organe verpflichtet, ihre Akten in der Regel innerhalb von zehn Jahren ab dem Zeitpunkt, ab dem sie die Unterlagen nicht mehr benötigen, dem Staatsarchiv anzubieten. Nach § 5 des IDG hat das Organ seine Informationen so zu verwalten, dass das Verwaltungshandeln nachvollziehbar und die Rechenschaftsfähigkeit gewährleistet ist. Die Anbietepflicht ist eine Bringschuld der Amtsstellen. § 9 der seit 2020 geltenden IVSV hält zudem fest, dass öffentliche Organe Dossiers mit den dazugehörigen Metadaten dem Archiv anbieten, wenn diese aufgrund der abgelaufenen Aufbewahrungsfrist oder des Wegfalls der öffentlichen Aufgabe ausgesondert werden. Das Staatsarchiv ist direktionsübergreifend für die Archivierung zuständig. Hierbei ist es aber auf die Kooperation der Verwaltungsstellen angewiesen. Es hat bisher keine Möglichkeiten, öffentliche Organe zu sanktionieren, welche die Akten nicht, wie gesetzlich vorgesehen, angeboten haben. Bisher kennt der Kanton Zürich im Gegensatz zu anderen Kantonen im Archivgesetz hierzu keine Strafbestimmung.[653]

Erst nach diesem Angebot sind Dossiers, die vom Archiv nicht übernommen werden, zu vernichten oder unwiderruflich zu löschen. Die Vernichtung jener Dokumente und Informationen, die das Staatsarchiv nicht übernimmt, liegt in der Verantwortung der öffentlichen Organe. Um hier eine bessere Nachvollziehbarkeit gewährleisten zu können, ist gemäss dem Staatsarchivar, Beat Gnädinger, im neuen Archivgesetz vorgesehen, Kassationsprotokolle einzuführen. Das heisst, dass die überliefernde Stelle schriftlich festhält, welche Akten sie im Rahmen der Abgabe vernichtet hat.[654]

Nach Auskunft des Staatsarchivars sind diese Bestimmungen rund um die Anbietepflicht rechtlich ausreichend. Aus Sicht der Verwaltung bestehe aber der Wunsch, die Bestimmungen in diesem Bereich noch klarer und nachvollziehbarer zu formulieren.[655]

Neben den allgemeinen Bestimmungen gibt es weitere spezifische Regelungen, die eine Aufbewahrung bestimmter Dokumente und Nachweise verlangen. So sind die Direktionen und die Staatskanzlei gemäss § 59 lit. c CRG[656] für die vorschriftsgemässe Erstellung und Archivierung von Belegen und die Inventarführung verantwortlich. Gemäss § 38 der Rechnungslegungsverordnung (RLV)[657] sind über Vermögenswerte ab einem bestimmten im Handbuch festgelegten Mindestwert Inventare zu führen.

---

[651] Protokoll des Zürcher Kantonsrates, 210. KR-Sitzung, 9. Januar 2023.

[652] Archivgesetz vom 24. September 1995 (LS 170.6) und Archivverordnung vom 9. Dezember 1998 (LS 170.61).

[653] Protokoll der Befragung von Beat Gnädinger vom 22. März 2024, S. 10.

[654] Protokoll der Befragung von Beat Gnädinger vom 22. März 2024, S. 15.

[655] Protokoll der Befragung von Beat Gnädinger vom 22. März 2024, S. 11–12.

[656] Gesetz über Controlling und Rechnungslegung vom 9. Januar 2006 (CRG; LS 611).

[657] Rechnungslegungsverordnung vom 29. August 2007 (RLV; LS 611.1).

Das zum Zeitpunkt der Räumungsaktion 2019 gültige Handbuch[658] hält fest, dass Mobilien unter diesem Schwellenwert auch inventarpflichtig sind, wenn sie besonders verlust- oder diebstahlgefährdet sind oder andere Gründe dafür sprechen. Letzteres sei bei IT-Geräten der Fall. Zur Inventarführung gilt es, Abgänge im Inventar so zu vermerken, dass alle Informationen vorliegen, welche die Kontrolle des Abgangs erlauben.

11.2.3 Äussere Umstände der Räumungsaktion

Mit Blick auf den anstehenden Umzug ins neue Polizei- und Justizzentrum (PJZ), aber auch als Folge eines Wasserschadens nach einem Brand in den IT-Räumlichkeiten an der Badenerstrasse war es gemäss dem damals zuständigen Leiter der JI-Informatik, Axel Mayer, notwendig, die Büroräumlichkeiten aufzuräumen und Platz für temporäre Büros zu schaffen. Die Aufräumarbeiten hätten sich vom Lagerraum über die Büros bis zum Rechenzentrum erstreckt. Besonders im Helpdesk-Büro hätten sich Altpapier, Notizzettel und Peripheriegeräte gestapelt.[659] Ihm sei es darum gegangen, im Bereich des Helpdesks Stapel abzuarbeiten sowie Elektroschrott und in seinen Augen offensichtlichen Müll wegzuräumen.

Bei ihren Besuchen im Bezirksgebäude sah auch die Generalsekretärin der JI, Jacqueline Romer, diverse Schachteln und Tastaturen in den Gängen herumliegen, weshalb sie anregte, dort «ein bisschen» aufzuräumen. Vom Leiter und von Mitarbeitenden habe sie auch erfahren, dass die Mitarbeiterin des Helpdesks, Erika W., viele Zettelchen aufbewahrt habe. Einen Auftrag, Akten zu vernichten, habe es nie gegeben. Und bei den in diesem Zusammenhang vernichteten Unterlagen habe es sich nicht um archivwürdige Dokumente gehandelt.[660] Auch die Direktionsvorsteherin, Jacqueline Fehr, konnte bisher nicht feststellen, dass in diesem Zusammenhang etwas Wichtiges vernichtet worden war. Inzwischen habe man verschiedene reglementarische Unterlagen sowie Lieferungsbestätigungen wieder gefunden, was der im Rahmen der Administrativuntersuchung geäusserten Vermutung, dass auch solche Unterlagen vernichtet worden seien, entgegenstehe. Die im Rahmen der Kantonsratsdebatte über die Einsetzung einer PUK vom 3. Juli 2023 von der Direktionsvorsteherin geäusserte Annahme, dass von den Geschäfts- und Verwaltungsakten wohl auch noch digitale Kopien vorhanden seien, habe sich damit wenigstens teilweise bestätigt.[661]

Der damalige Leiter der JI-Informatik, Axel Mayer, betonte in der Befragung durch die PUK Datensicherheit, er habe in «keinster Weise mit einer Anweisung Daten vernichten lassen». Da zu seiner Zeit Auftragspapiere jeweils der Rechnung beigeheftet und an weitere Stellen übermittelt oder allgemein Kundenaufträge online abgewickelt sowie nicht mehr benötigte Unterlagen ans Staatsarchiv abgeliefert wurden, war er überzeugt, dass sich dort keine Akten oder Lieferscheine befanden.[662] An einer Hauptabteilungssitzung sei auch explizit von «Aufräumen» gesprochen worden und man habe diesbezügliche Beispiele angeführt.[663] Er könne sich vorstellen, gesagt zu haben, dass Lieferscheine nicht aufbewahrungspflichtig seien; dies auch, weil er davon ausgegangen sei, dass bei Aufträgen immer auch Rechnungsbelege vorhanden seien.[664]

---

[658] Finanzdirektion, Finanzverwaltung, Kantonales Rechnungswesen, Handbuch für Rechnungslegung (HBR) 2019. Ausgabe vom 28. Februar 2018, in Kraft getreten am 1. Januar 2019, S. 359.

[659] Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 9.

[660] Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 25.

[661] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 35.

[662] Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 17–20.

[663] Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 21–22.

[664] Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 24.

Zudem liessen sich heute Lieferscheine beim Lieferanten einholen.[665] Abklärungen der PUK Datensicherheit beim damals für die JI zuständigen Mitarbeiter des Staatsarchivs haben weiter ergeben, dass der Leiter der JI-Informatik im Rahmen seines Stellenantritts bei einem Besuch des Staatsarchivs über die Abläufe informiert worden war.[666] Auch dies spricht gegen eine unzureichende Sensibilisierung des Leiters für solche Fragen.

11.2.4 Konkreter Sachverhalt

Gemäss den Aussagen des langjährigen Leiters der JI-Informatik (2000–2017), Fredi Steiner, und der Helpdesk-Mitarbeiterin, Erika W., waren die unterschriebenen Inventarblätter beim Helpdesk abgelegt. Sie wurden dort aufbewahrt, weil das Inventar keine Historie und somit keine Informationen über Zu- und Abgänge enthielt. Verträge seien dort keine abgelegt worden. Für die PUK Datensicherheit ist denkbar, dass diese teilweise sehr alten Inventarblätter, die als Belege fungierten, in den Stapeln oder im Schrank beim Helpdesk enthalten waren und dann im Rahmen der Aufräumaktion entsorgt wurden.

Aus Sicht des damaligen Leiters der JI-Informatik, Axel Mayer, läge in diesem Fall das Versäumnis aber nicht bei ihm. Vielmehr hätte man es dann in früherer Zeit verpasst, die Unterlagen korrekt abzulegen und – besonders nach den ersten Ermittlungen der Staatsanwaltschaft 2014, die im Zusammenhang mit den Vorgängen rund um die Bestechungsvorwürfe im SECO gemacht wurden – diese Stapel durchzusehen.[667] Überdies hätte die Mitarbeiterin bei Unklarheiten oder bevor sie etwas Wichtiges entsorgte mit ihren direkten Vorgesetzten Rücksprache nehmen können. Eigentlich sei den meisten Mitarbeitenden bewusst, was wichtige Daten sind und wie mit diesen umzugehen ist, das habe sich bei den übrigen Mitarbeitenden auch gezeigt. Rückblickend würde er allenfalls noch stärker abklären, ob den Mitarbeitenden wirklich bewusst sei, was Daten und Akten sind.[668]

11.3 Würdigung durch die PUK

Aus der Sicht der PUK Datensicherheit haben die Verantwortlichen der JI mit dem Stopp der RIS-Entwicklung und dem damit verbundenen raschen Aufbau eines eigenen Geschäftsverwaltungssystems eine wichtige Massnahme ergriffen und umgesetzt. Damit deckt sich das Bild mit der Feststellung aus dem Schlussbericht der Administrativuntersuchung, dass etwa ab dem Jahr 2016 vor allem im Bereich des Generalsekretariats der JI diverse Massnahmen ergriffen worden seien, um die Verwaltung der Informationen zu regeln. Mit der Einführung des Geschäftsverwaltungssystems ist gemäss der Administrativuntersuchung eine wichtige Grundlage für eine gesetzeskonforme Verwaltung der Informationen geschaffen worden.

Weiter konnte die PUK Datensicherheit auf Basis der Unterlagen, aber auch im Rahmen der geführten Gespräche feststellen, dass bei den Verantwortlichen bezüglich Digitalisierung, aber auch bei Fragen des Datenschutzes und der Informationssicherheit ein hohes Bewusstsein besteht. Mit der Reorganisation des Generalsekretariates und den durchgesetzten personellen Veränderungen hat die Direktionsleitung auch hier Massnahmen ergriffen, um die Informatik besser zu führen und zu gestalten. Trotz dieser Bemühungen ergab sich aber aus der Administrativuntersuchung, dass das

[665] Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 22.

[666] PUK Datensicherheit Aktennotiz Telefongespräch vom 28. Januar 2025.

[667] Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 23–24.

[668] Protokoll der Befragung von Axel Mayer vom 25. Oktober 2024, S. 25.

Monitoring der JI-Informatik verbesserungswürdig war. Dies zeigt sich für die PUK Datensicherheit auch darin, dass in den Räumen der JI-Informatik nach 2014 noch immer wenig Ordnung herrschte und somit auch die Aktenablage nicht angemessen ablief respektive die ruhende Ablage der nicht mehr benötigten Unterlagen ungenügend war. Hierfür wäre der damalige Leiter der JI-Informatik, Fredi Steiner, zuständig gewesen.

Mit dem Entscheid, 2017 eine neue IT-Leitung einzusetzen, konnte die Direktionsleitung hier zwar eine Verbesserung bewirken. Die neue Leitung brachte frischen Wind in die Abteilung und stiess dann beispielsweise auch auf die 200 bis 300 überzähligen Desktopgeräte aus früheren Beschaffungen. Doch durch den Entscheid der Direktionsvorsteherin, die Vergangenheit Vergangenheit sein zu lassen, konnten die früheren und zum Zeitpunkt der Aufräumaktion 2019 noch vorhandenen Altlasten nicht sauber bereinigt und aufgearbeitet werden. Der ehemalige Datenschutzbeauftragte, Bruno Baeriswyl, fand es, von aussen betrachtet, erstaunlich, dass es so lange gedauert hatte, bis die JI vom Datensicherheitsvorfall Kenntnis erhielt. Mit einer früheren Implementierung der richtigen Kontrollprozesse hätte man den Datensicherheitsvorfall schon damals entdeckt.[669]

Im Rahmen ihrer Abklärungen hat die PUK Datensicherheit festgestellt, dass die Amtsübergaben sowohl auf Ebene der Direktionsleitungen als auch auf Stufe der Generalsekretärinnen und Generalsekretäre sowie bei den Amtsleitungen kaum formalisiert sind. Die PUK Datensicherheit ist der Ansicht, dass erhebliche Risiken bestehen, wenn die nachfolgenden Funktionsträger nicht umfassend über die bestehenden Probleme und Herausforderungen informiert werden. Sie begrüsst zwar die internen Bemühungen der JI in diesem Bereich, regt jedoch an, sich auch auf der Ebene des ganzen Kantons Gedanken zu machen, wie diese heiklen Übergänge künftig besser ausgestaltet und geregelt werden können.

Die PUK Datensicherheit geht inzwischen davon aus, dass die lückenhafte Dokumentation wohl nicht wesentlich oder ursächlich eine Folge der Aufräumaktion ist, auch wenn im Rahmen der öffentlichen Behandlung dieser Aufräumaktion der Eindruck entstanden ist, es seien dabei wesentliche Unterlagen weggekommen und die Nachvollziehbarkeit der Abläufe würde dadurch äusserst erschwert. So ist es beispielsweise aus Sicht der Kommission unwahrscheinlich, dass in diesem Zusammenhang Vertragsunterlagen entsorgt wurden. Hingegen ist gut denkbar, dass im Rahmen der Aktion die jahrelang gelagerten Inventarblätter weggekommen sind, mit denen man, in Ergänzung zum Inventar, die Zu- und Abgänge von Geräten hätte nachvollziehen können. Zum Zeitpunkt der Aufräumaktion 2019 waren die Vorgaben zur Inventarführung aber bereits dergestalt, dass die Nachvollziehbarkeit durch Vermerke innerhalb des Inventars hätte gegeben sein müssen. Vor diesem Hintergrund ist plausibel, dass dem damaligen neuen Leiter der JI-Informatik, Axel Mayer, die Bedeutung dieser Inventarblätter nicht bewusst war. Zudem war nicht davon auszugehen, dass die externen Dienstleistungen auch in der Buchhaltung nicht verzeichnet waren. Der vormalige Leiter der JI-Informatik, Fredi Steiner, dem die Relevanz dieser Unterlagen bewusst war, hätte dies gegenüber der ihm unterstellten Mitarbeiterin oder gegenüber der Leitung signalisieren müssen. Da das Inventar zu diesem Zeitpunkt aus seiner Sicht nachgeführt war, sah jedoch auch Fredi Steiner gemäss seiner Stellungnahme keine Notwendigkeit die Inventarblätter weiter aufzubewahren. Die Untersuchung zeigte jedoch, dass besonders die Abgänge im Inventar unzureichend erfasst waren.[670]

---

[669] Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 28.

[670] Stellungnahme von Fredi Steiner vom 5. November 2025.

Weder die Autorinnen der Administrativuntersuchung noch die JI haben die Aussage, dass die Akten, welche die korrekte Löschung bestätigt hätten, auf Anweisung des Leiters der JI-Informatik entsorgt worden waren, kritisch hinterfragt oder kontextualisiert. So ist das Bild entstanden, dass der Leiter der JI-Informatik, Axel Mayer, 2019 einen Auftrag zur Datenentsorgung erteilt habe. Aus Sicht der PUK Datensicherheit hat der Leiter der JI-Informatik aber zum Aufräumen aufgefordert, und es sind, wie die Abklärungen der PUK Datensicherheit zeigen, wohl vor allem die Inventarblätter weggekommen.

Der Umstand, dass einzelne Inventarblätter für den Nachvollzug derart wichtig sind, zeigt für die PUK Datensicherheit, dass die JI-Informatik bereits vor der Aufräumaktion 2019 ihre Informationen nicht gemäss § 5 IDG verwaltet hatte und somit ihr Handeln nicht nachvollziehbar und die Rechenschaftsfähigkeit nicht gewährleistet war.

Die PUK Datensicherheit ist der Ansicht, dass bei der Revision des Archivgesetzes darauf zu achten ist, dass die Vorgaben zur Aktenführung, die Anbietepflicht, die Garantie für die korrekte Löschung der vom Staatsarchiv nicht übernommenen Unterlagen sowie die diesbezüglichen Zuständigkeiten klar aus dem Gesetz hervorgehen. Überdies ist zu gewährleisten, dass in allen Direktionen und der Staatskanzlei keine Aufräumaktionen stattfinden, ohne dass die für die Amtsstelle zuständige Person des Staatsarchivs informiert und allenfalls beteiligt wird.

12. Umgang mit dem Datensicherheitsvorfall nach dem internen Bekanntwerden

12.1 Bereits laufende Verfahren der Staatsanwaltschaften

Durch die am 28. November 2022 im Kantonsrat eingereichte Anfrage (KR-Nr. 456/2022) und die darauffolgende Medienberichterstattung erfuhr die Öffentlichkeit erstmals vom Datensicherheitsvorfall in der Direktion der Justiz und des Innern (JI). Zu diesem Zeitpunkt liefen bereits zwei Strafverfahren, die einen unmittelbaren Bezug zum Untersuchungsauftrag der PUK Datensicherheit aufweisen. In den nachfolgenden Abschnitten soll deshalb auf diese eingegangen werden. Ziel ist es, deren wesentliche Inhalte kurz darzulegen und eine zeitliche Einordnung vorzunehmen. Dadurch sollen ein besseres Verständnis für den jeweiligen Kontext geschaffen und die Relevanz der Strafverfahren im Hinblick auf den Untersuchungsgegenstand der PUK Datensicherheit nachvollziehbar gemacht werden.

12.1.1 Strafverfahren der Staatsanwaltschaft Zürich-Sihl

Am Sonntag, 8. November 2020 suchte die Mutter eines Beschuldigten einen Staatsanwalt des Kantons Zürich an dessen Privatadresse auf. Im Verlauf des Gesprächs wurde klar, dass sie die Kontaktdaten über Roland Gisler erhalten hatte, den sie persönlich kannte und gegen den ein Strafverfahren lief. Am Folgetag kontaktierte der betroffene Staatsanwalt mittels E-Mail den Leitenden Oberstaatsanwalt und informierte ihn über den Vorfall. Gemäss seinen ersten Informationen habe der Bruder von Roland Gisler den Auftrag gehabt, Server der JI abzuholen und zu entsorgen. Die Entsorgung sei aber nicht geschehen, womit Roland Gisler in den Besitz von Daten der JI gekommen sei. Falls der Sachverhalt zutreffe, gebe es, so der betroffene Staatsanwalt, «ein gröberes Problem».[671] Die Oberstaatsanwaltschaft veranlasste daraufhin bei der Staatsanwaltschaft Zürich-Sihl die Aufnahme von Ermittlungen und leitete ein Strafverfahren wegen Gewalt und Drohung gegen Beamte ein.[672]

Im Rahmen dieses Strafverfahrens erwuchs der Verdacht, dass sich Daten der JI in den Händen von Personen befanden, die keinen Zugriff darauf haben sollten.[673] Obwohl Roland Gisler angab, im Besitz verschiedener Daten der JI zu sein, deutete zu Beginn vieles daraufhin, dass die Daten nicht, wie ursprünglich angenommen, direkt von der JI stammten, sondern über verschiedene, insbesondere auch öffentliche Quellen durch Roland Gisler gesammelt und zusammengetragen worden waren.[674] Andreas Eckert, der damals als Oberstaatsanwalt für die Staatsanwaltschaft Zürich-Sihl zuständig war, erfuhr gemäss eigenen Angaben wohl im Rahmen einer Geschäftsleitungssitzung im November 2020 von den Vorfällen. Zu jenem Zeitpunkt handelte es sich aus seiner Sicht weder um einen besonders aufsehenerregenden Fall noch um einen

---

671 E-Mail des Leitenden Oberstaatsanwalts «Datenleck JI» vom 9. November 2020 an den Leitenden Staatsanwalt der Staatsanwaltschaft Zürich-Sihl; Kantonspolizei, Abschliessender Bericht über das kriminalpolizeiliche Ermittlungsverfahren «Aktion EGANO», Abfluss und unrechtmässige Verwendung von vertraulichen Daten der Justizdirektion des Kantons Zürich vom 2. September 2022.

672 Protokoll der Befragung von Mathias Eberli vom 31. Januar 2025, S. 7.

673 Protokoll der Befragung von David Zogg und Mathias Eberli vom 3. Mai 2024, S. 7.

674 Protokoll der Befragung von Mathias Eberli vom 31. Januar 2025, S. 3–4.

Schlüsselfall.[675] Als er ab März 2022 die Funktion als Leitender Oberstaatsanwalt übernahm, fand demzufolge – anders als bei Schlüsselfällen, die bei der Übergabe besprochen wurden – keine besondere Information statt.[676] Es entzog sich damit seiner Kenntnis, dass die Generalsekretärin der JI, Jacqueline Romer, im Rahmen dieses Verfahrens den Bericht der Administrativuntersuchung (siehe Kapitel 12.3) am 11. Mai 2022 dem zuständigen polizeilichen Sachbearbeiter übermittelt hatte.

12.1.2 Strafverfahren der Staatsanwaltschaft II des Kantons Zürich

Die Staatsanwaltschaft II des Kantons Zürich führte ein Strafverfahren gegen Roland Gisler wegen Widerhandlungen gegen das Betäubungsmittelgesetz und weiterer Delikte. Mit Urteil vom 24. März 2021 wurde Roland Gisler erstinstanzlich teilweise schuldig gesprochen. Sowohl die Staatsanwaltschaft als auch Roland Gisler erhoben daraufhin Berufung.[677]

Das Verfahren der Staatsanwaltschaft II des Kantons Zürich ist insofern von Bedeutung, als Roland Gisler im Rahmen der dazugehörigen Berufungsverhandlung vom 4. November 2022 vor dem Obergericht des Kantons Zürich Aktenstücke an Medienschaffende und Behördenvertreter weitergab. Diese seien, so sagte er, über seinen Bruder zu ihm gelangt, der in früheren Jahren von der JI mit der Entsorgung von Datenträgern beauftragt worden war. Die abgegebenen Unterlagen wiesen eine gewisse Sensitivität auf, wobei zum damaligen Zeitpunkt jedoch unklar war, aus welcher Quelle sie stammten.[678] Damit wurde dieser veritable Datensicherheitsvorfall erstmals öffentlich bekannt.

12.2 Kenntnisnahme durch die Direktion der Justiz und des Innern (JI)

Die Direktionsvorsteherin der JI, Jacqueline Fehr, gab an, am Montag, 9. November 2020, nachdem am Vortag ein Staatsanwalt an seiner Privatadresse aufgesucht worden war (siehe Kapitel 12.1.1), erstmals vom damaligen Leitenden Oberstaatsanwalt telefonisch und später per E-Mail über den Datensicherheitsvorfall informiert worden zu sein.[679] In diesem Zusammenhang erhielt auch die Generalsekretärin der JI, Jacqueline Romer, als Empfängerin der E-Mail, Kenntnis vom Datensicherheitsvorfall.[680] Die stellvertretende Generalsekretärin, Susanna Stähelin, gab an, ebenfalls zu jenem Zeitpunkt in Kenntnis gesetzt worden zu sein.[681] Die Generalsekretärin informierte unverzüglich auch den Leiter der Hauptabteilung Digital Solutions, Urs Kaderli, über den

---

675 In folgenden Situationen wird ein Fall als Schlüsselfall qualifiziert: (a) für die Wirtschaft und den Finanzplatz Zürich besonders massgebendes Verfahren mit hohem volkswirtschaftlichen Schaden oder von anderweitiger aussergewöhnlicher Dimension, (b) in der Bevölkerung und in den Medien besonders Aufsehen erregende Kapitalverbrechen, Unfälle oder Katastrophen, (c) politisch und gesellschaftlich besonders relevante Verfahren (z. B. Organisierte Kriminalität, Korruption), (d) Verfahren von besonderer juristischer Tragweite (materiell- oder prozessrechtliche Leitentscheide), oder (e) Straftaten gegen oder durch Personen, die in der Öffentlichkeit stehen (Weisungen der Oberstaatsanwaltschaft für das Vorverfahren (WOSTA), Ziffer 8.5.1).

676 Protokoll der Befragung von Andreas Eckert vom 28. Februar 2025, S. 7.

677 Urteil des Obergerichts des Kantons Zürich vom 4. November 2022 (SB210320-O); Urteil des Bundesgerichts vom 19. September 2024 (BGer 7B_829/2023).

678 Protokoll der Befragung von Andreas Eckert vom 28. Februar 2025, S. 8.

679 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 30; E-Mail «WG: Datenleck IT» des Leitenden Oberstaatsanwalts an Jacqueline Fehr und Jacqueline Romer vom 9. November 2020.

680 Weitergeleitete E-Mail des Leitenden Oberstaatsanwalts «Datenleck JI» vom 9. November 2020 an Jacqueline Fehr und Jacqueline Romer; Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 20.

681 Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 9.

Vorfall. Er habe davon aber auch von Fredi Steiner, dem früheren Leiter der JI-Informatik, erfahren, der in dieser Sache bereits mit dem verfahrensleitenden Staatsanwalt der Staatsanwaltschaft Zürich-Sihl in Kontakt gestanden war.[682]

Die Direktionsvorsteherin, Jacqueline Fehr, führte gegenüber der PUK Datensicherheit aus, dass die Frage, wer und wie über diesen Vorfall zu informieren sei, bereits Gegenstand des ersten Austausches mit der Staatsanwaltschaft vom 9. November 2020 gewesen sei. Noch am selben Tag habe sie mit der JI-Informatik Kontakt aufgenommen und sie um eine Einschätzung gebeten, ob es weitere Hinweise auf den Vorfall gebe oder ob ähnliche Probleme noch bestünden. Die mündliche Stellungnahme habe sie noch am selben Tag erhalten.[683] Urs Kaderli, Leiter der Digital Solutions, DigiSol, wie die Hauptabteilung JI-Informatik seit dem 1. Juli 2021 offiziell heisst, versicherte, dass ein so gearteter Vorfall nicht mehr möglich wäre, da die Sicherheitsüberprüfung und die Entsorgung zu jenem Zeitpunkt bereits anders geregelt waren.[684]

Am 12. November 2020 informierte die Direktionsvorsteherin der JI den Leiter Kommunikation, Benjamin Tommer, und ging nach eigenen Aussagen die nächsten Schritte an.[685] Neben der Einleitung der Administrativuntersuchung (siehe Kapitel 12.3), wie sie auch vom Leitenden Oberstaatsanwalt angeregt worden war, habe sie von der Digital Solutions eine schriftliche Stellungnahme zur aktuellen Sicherheitssituation ausarbeiten lassen.[686] Sie beinhaltete ein Memorandum des ehemaligen Leiters der JI-Informatik, Fredi Steiner, zum früheren Umgang mit der Informationssicherheit, namentlich der Entsorgung, sowie eine tabellarische Zusammenstellung der technologischen Entwicklung innerhalb der JI im Zeitraum 1995–2016 zu Beschaffungen, Entsorgungen und eingeführten Sicherheitslösungen.[687]

Am 19. November 2020 wurden zwischen der Staatsanwaltschaft Zürich-Sihl und der JI die Zuständigkeiten hinsichtlich Strafverfahren, Administrativuntersuchung und Aufarbeitung der Situation betreffend Datensicherheit geklärt. Dabei ging es auch um den Informationsfluss und die Kommunikation. Insbesondere beschloss man, die GPK zu diesem frühen Zeitpunkt noch nicht zu informieren. Zum Vorgehen bezüglich der Information der Datenschutzbeauftragten enthält die ausführliche Traktandenliste der Sitzung, in welcher zwischen dem Oberstaatsanwalt und der JI besprochen wurde, wer für welche Bereiche zuständig ist, keine Angaben.[688]

Am 20. November 2020 informierte der Leiter der Digital Solutions, Urs Kaderli, den kantonalen Informationssicherheitsbeauftragten (ISIK), Philipp Grabher, über den Vorfall und die vorgesehene Administrativuntersuchung. Letzterer nannte ihm Namen von möglichen Autorinnen und Autoren für eine Administrativuntersuchung.[689] Anschliessend habe man sich mehrmals auf verschiedenen Stufen – auch auf Stufe

---

682 Protokoll der Befragung von Urs Kaderli vom 1. November 2024, S. 18.

683 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 30.

684 Protokoll der Befragung von Urs Kaderli vom 1. November 2024, S. 18.

685 Weitergeleitete E-Mail von Jacqueline Fehr an den Leiter Kommunikation und den Leiter Digital Solutions «WG: Fall G: Empfehlung (Administrativ-)Untersuchung» vom 12. November 2020.

686 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 30; E-Mail von Jacqueline Fehr vom 12. November 2024 an ihre Mitarbeitenden, inkl. E-Mail-Verkehr mit LOSTA «Fall G: Empfehlung (Administrativ-)Untersuchung».

687 Protokoll der Befragung von Urs Kaderli vom 1. November 2024, S. 18, Direktion der Justiz und des Innern, Digital Solutions, Memorandum «Mögliches Datenleck IT JI» von Fredi Steiner vom 10. November 2020 und Timeline «Technologieentwicklung Klient bei DigiSol».

688 Direktion der Justiz und des Innern, Generalsekretariat, Fall R.G. Daten-Missbrauch, Traktanden 19.11.20: Klärung sowie Koordination Aufgaben und Rollen/Zuständigkeiten.

689 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 30; Weitergeleitete E-Mail des Leiters DigiSol an die Generalsekretärin und deren Stv. vom 20. November 2020.

Direktionsvorsteherin – mit dem ISIK ausgetauscht und dann die offenen Themen, wie bspw. die Information der Datenschutzbeauftragten, angepackt.[690] Die Meldung an die Datenschutzbeauftragte folgte schliesslich am 30. November 2020 über deren offizielles Formular.[691]

Bezüglich der allgemeinen Kommunikation gegen innen und aussen führte der Kommunikationsbeauftragte der JI, Benjamin Tommer, gegenüber der PUK Datensicherheit aus, dass im Rahmen des Datensicherheitsvorfalls vor kommunikativen Massnahmen die direkt betroffene Einheit, Digital Solutions, jeweils informiert wurde. Die Mitarbeitenden der Direktion habe man mehrmals, wohl als der Vorfall dann mediale Wellen schlug, mit Mailings bedient. Im Rahmen von Sitzungen habe man die Kommunikation diskutiert, wobei es seitens Direktionsleitung keine Vorgaben gegeben habe. Gemäss Aussagen des Kommunikationsbeauftragten wussten sie, abgesehen von den Hinweisen der Staatsanwaltschaft, nichts über das Ausmass des Vorfalls und die Qualität der Daten. Aus diesem Grund und auch um negative Auswirkungen auf die informierten Personen zu vermeiden, hätten sie sich aktiv dafür entschieden, nicht öffentlich zu informieren. Die zurückhaltende Kommunikation der Direktion sei massgeblich davon geprägt gewesen, dass das man dem Beschuldigten nicht in die Hände spielen und damit das Strafverfahren gefährden wollte. [692]

12.3 Durchführung der Administrativuntersuchung

Die Direktionsvorsteherin, Jacqueline Fehr, sagte gegenüber der PUK Datensicherheit, dass sie die Generalsekretärin am 12. November 2020 mit der Einleitung einer Administrativuntersuchung beauftragt habe. Dabei habe sie darauf hingewiesen, dass der kantonale Informationssicherheitsbeauftragte (ISIK) in die Untersuchung einzubeziehen und die Abgrenzung zum Strafverfahren sicherzustellen sei.[693] Die beiden leitenden Fragen waren in ihren Augen, ob es Handlungsbedarf gebe und was man machen müsse, um sich gut aufzustellen.[694]

Am 2. Dezember 2020 erteilte das Generalsekretariat Maria Winkler und Sarah Bischof von IT & Law Consulting GmbH Zürich den Auftrag, eine Administrativuntersuchung durchzuführen.[695] Gemäss den Auftragnehmerinnen waren sie mit einer Sachverhaltsabklärung nach den Prinzipien des Verwaltungsverfahrens beauftragt, wobei die Ergebnisse in einem Schlussbericht festzuhalten waren. Es war, erstens, die Frage zu klären, ob die JI, insbesondere die JI-Informatik, im massgeblichen Zeitraum angemessene technische und organisatorische Massnahmen implementiert hätten, um die Datensicherheit zu gewährleisten. Hierbei waren neben dem Umgang mit der Speicherung und der Archivierung der Daten insbesondere die Sicherstellung der Löschung der Daten und die Entsorgung der Datenträger sowie der Beizug von externen Dienstleistern im Fokus. Zweitens war zu untersuchen, ob die Datensicherheit aktuell gewährleistet sei. Die Administrativuntersuchung umfasste den Zeitraum zwischen 2000

690 Protokoll der Befragung von Urs Kaderli vom 1. November 2024, S.17–19.

691 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 20.

692 Protokoll der Befragung von Benjamin Tommer vom 27. September 2024, S. 7–13.

693 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 30; Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 20–21; E-Mail «Antwort: Fall G: Empfehlung (Administrativ-)Untersuchung» von Jacqueline Fehr an den Leitenden Oberstaatsanwalt vom 12. November 2020.

694 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 32.

695 Direktion der Justiz und des Innern, Generalsekretariat, Auftrag betreffend Datenmissbrauch – Administrativuntersuchung vom 2. Dezember 2020.

und 2014 sowie den aktuellen Stand.[696] Die Autorinnen waren gemäss Auftrag verpflichtet, innert zwei Monaten einen Zwischenbericht vorzulegen, und durften die Untersuchung der Staatsanwaltschaft nicht beeinträchtigen.[697]

Im Rahmen der Untersuchung stellten die Autorinnen nach eigenen Aussagen relativ schnell fest, dass kaum Belege und Unterlagen für den Zeitraum von 2000–2014 vorhanden waren. Dies lag nach ihren eigenen Mutmassungen daran, dass bei der Räumungsaktion im Jahr 2019 (siehe Kapitel 11.2) viele Akten vernichtet worden seien. Dies wiederum führten sie auf das Fehlen von Vorgaben zurück, wie die Akten vorgängig hätten digitalisiert werden müssen. Weiter führten die Autorinnen aus, dass die Rücksichtnahme auf das laufende Strafverfahren die Administrativuntersuchung eingeschränkt habe. Aus diesem Grund hätten sie sich verstärkt mit der aktuellen Situation und deren Beurteilung auseinandergesetzt, insbesondere mit der Frage, ob zum aktuellen Zeitpunkt noch Risiken bestünden, die zu beheben seien, und welche Massnahmen sie hierfür empfehlen würden.[698]

Die Direktionsvorsteherin, Jacqueline Fehr, erklärte bei der Befragung durch die PUK Datensicherheit, darauf gedrängt zu haben, möglichst schnell einen Zwischenbericht mit Informationen über zu ergreifende Sofortmassnahmen zu erhalten.[699] Die Autorinnen legten ihren Bericht am 29. Januar 2021 vor.[700] Darin stellten sie fest, dass beim Generalsekretariat der JI seit ca. 2016 zahlreiche Massnahmen ergriffen worden seien, um die Verwaltung der Informationen sowie den Zugriff auf diese zu regeln. Auch seien im Bereich der Informationssicherheit zusätzliche Massnahmen umgesetzt worden. Ebenfalls sei eine hohe Sensibilität der interviewten Personen für Aspekte der Informationsverwaltung, der Informationssicherheit und des Datenschutzes festgestellt worden. Es bestehe jedoch Handlungsbedarf in Bezug auf den Erlass von Organisationsvorschriften, die für die gesamte Direktion verbindlich seien, auf die Kontrolle der Einhaltung von Vorschriften sowie bezüglich der Aktualität von Unterlagen. Die Autorinnen arbeiteten sodann 13 Empfehlungen aus. Bei vier Empfehlungen wiesen sie der Umsetzung eine hohe Priorisierung zu.[701]

Die Direktionsvorsteherin, Jacqueline Fehr, kam auf Basis des Zwischenberichts zum Schluss, dass das Risiko in der aktuellen Situation nicht mehr bestehe und keine Sofortmassnahmen zu ergreifen seien. Daher sei der Vorfall auf der Prioritätenliste nach unten gerutscht und zu einem ordentlichen Geschäft erklärt worden.[702] Die Anspannung und Besorgnis, welche die Anfangsphase geprägt habe, sei einer «wahnsinnigen Erleichterung» gewichen. Sie glaube, sie habe «das dann innerlich schlicht von der Agenda gestrichen».[703] Auch gemäss den Ausführungen des Kommunikationsbeauftragten hätten die Zwischenresultate eine gewisse Entwarnung gegeben und der Schlussbericht sei nur noch mit wenig Spannung erwartet worden. Die Thematik sei

---

696 Protokoll der Befragung von Maria Winkler und Sarah Bischof vom 25. Oktober 2024, S. 8–9.

697 Protokoll der Befragung von Maria Winkler und Sarah Bischof vom 25. Oktober 2024, S. 8, 15.

698 Protokoll der Einvernahme von Maria Winkler und Sarah Bischof vom 25. Oktober 2024, S. 10–11.

699 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 32.

700 Protokoll der Einvernahme von Maria Winkler und Sarah Bischof vom 25. Oktober 2024, S. 15; IT & Law Consulting GmbH, Administrativuntersuchung bei der Direktion der Justiz und des Innern des Kantons Zürich im Zusammenhang mit dem Umgang von Informationen und Datenmissbrauch, Zwischenbericht vom 29. Januar 2021.

701 IT & Law Consulting GmbH, Administrativuntersuchung bei der Direktion der Justiz und des Innern des Kantons Zürich im Zusammenhang mit dem Umgang von Informationen und Datenmissbrauch, Zwischenbericht vom 29. Januar 2021.

702 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 32.

703 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 37.

dann «unter den Radar» der Kommunikationsabteilung geraten, die auch nicht mehr involviert gewesen sei, weil es gemäss der Administrativuntersuchung keinen unmittelbaren Handlungsbedarf gegeben habe.[704]

Die Autorinnen schlossen die Administrativuntersuchung in der Folge mit dem Schlussbericht vom 30. März 2021 ab.[705] Dieser hielt fest, dass im Jahr 2019 bei der JI-Informatik grosse Mengen physischer Akten vernichtet worden seien, ohne dass diese vorher digitalisiert oder systematisch dokumentiert worden wären. Daher seien die Vorgänge zur Datenlöschung und Aktenvernichtung zwischen 2000 und 2014 nicht mehr nachvollziehbar. Als Ursache wurden fehlende standardisierte Prozesse bei der Vergabe an externe Dienstleister, eine ungenügende Wahrnehmung der Datenschutzverantwortung durch die JI und eine unzureichende Kontrolle der Dienstleister genannt. Diese Probleme basierten nach Ansicht der Autorinnen vor allem auf fehlenden organisatorischen Vorgaben und mangelhafter Aufsicht der Jl.

Zur Vermeidung ähnlicher Vorfälle empfahlen die Autorinnen verbindliche Organisationsvorschriften, systematische Kontrollen und die Aktualisierung der Informationsverwaltung.

- Um den Vollzug des IDG innerhalb der gesamten JI systematisch umzusetzen, sollte der Bereich Support, Führung und Recht [SFR] im Generalsekretariat der JI Organisationsvorschriften, Weisungen und Reglemente erlassen und intern die erforderlichen personellen Ressourcen zur Verfügung stellen, sodass die nötige Fachkompetenz aufgebaut und die Verantwortung für die Informationsverwaltung und den Datenschutz geregelt werden kann.
- Die Zugriffskonzepte sollten überprüft und gegebenenfalls angepasst werden.
- Ordnungsvorschriften zur Regelung der Verwendung von AGB oder Datenschutz- und Geheimhaltungsbestimmungen sollten erlassen werden.
- Direktionsweit verbindliche Vorgaben über die Durchführung von Sicherheitsprüfungen beim Beizug von externen Dienstleistern sollten erlassen und umgesetzt werden.

Insgesamt hielt der Schlussbericht fest, dass nach wie vor Handlungsbedarf bestehe, um die Umsetzung der gesetzlichen Vorgaben in der gesamten JI systematisch und flächendeckend sicherzustellen.[706]

Für den ehemaligen Datenschutzbeauftragten, Bruno Baeriswyl, war es noch bei seiner Befragung durch die PUK Datensicherheit unverständlich, wie die Administrativuntersuchung 2021 weiterhin solche Mängel feststellen konnte, zumal die wesentlichen Vorgaben schon in den gesetzlichen Grundlagen der 1990er-Jahre enthalten waren und auch weiter konkretisiert worden seien.[707]

Zum Schlussbericht führte die Direktionsvorsteherin der JI gegenüber der PUK Datensicherheit aus, dass sie ihn nach dessen Eingang am 31. März 2021 zusammen mit der Generalsekretärin geprüft habe. Der Schlussbericht habe keinen sofortigen Handlungsbedarf angezeigt. Zudem sei dessen Systematik für sie teilweise nicht nachvollziehbar gewesen. Von einer Veröffentlichung des Schlussberichts der Administra-

---

[704] Protokoll der Befragung von Benjamin Tommer vom 27. September 2024, S. 13–14.

[705] Protokoll der Einvernahme von Maria Winkler und Sarah Bischof vom 25. Oktober 2024, S. 15; IT & Law Consulting GmbH, Administrativuntersuchung bei der Direktion der Justiz und des Innern des Kantons Zürich im Zusammenhang mit dem Umgang von Informationen und Datenmissbrauch, Schlussbericht vom 30. März 2021.

[706] IT & Law Consulting GmbH, Administrativuntersuchung bei der Direktion der Justiz und des Innern des Kantons Zürich im Zusammenhang mit dem Umgang von Informationen und Datenmissbrauch, Schlussbericht vom 30. März 2021.

[707] Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 12.

tivuntersuchung habe man wegen des laufenden Strafverfahrens für lange Zeit abgesehen.[708] Auch sei eine Information der Gesamtregierung ausgeblieben, weil sich die Regierungsmitglieder nicht systematisch über Administrativuntersuchungen informieren, sofern diese vom Thema her nicht auch andere Direktionen betreffen.[709]

12.4 Exkurs: Administrativuntersuchungen im Allgemeinen

Im Rahmen ihrer Abklärungen war die PUK Datensicherheit mit der Aussage konfrontiert, dass sich die Mitglieder des Regierungsrates üblicherweise nicht gegenseitig über Administrativuntersuchungen informieren, sofern die anderen nicht davon betroffen seien. Sie liess sich daher im Rahmen ihrer Befragungen und mit einem Auskunftsersuchen an die Staatskanzlei über die allgemeine Praxis im Umgang mit Administrativuntersuchungen informieren.

Seit 2020 hat ausser der Sicherheitsdirektion und der JI keine Direktion eine Administrativuntersuchung durchgeführt. Während die JI in den letzten fünf Jahren einzig die Administrativuntersuchung zum Datensicherheitsvorfall in Auftrag gegeben hatte, führte die Sicherheitsdirektion zwei Untersuchungen zu organisatorischen Mängeln durch. Die übrigen Direktionen haben gemäss eigenen Angaben seit 2020 keine Sachverhalte mittels Administrativuntersuchungen überprüfen lassen.[710] Jene Regierungsratsmitglieder, die bereits Administrativuntersuchungen in Auftrag gegeben hatten, führten sinngemäss aus, dies sei stets dann notwendig, wenn etwas nicht in Ordnung sei. Zur Frage, ob die Durchführung einer Administrativuntersuchung den anderen Mitgliedern des Regierungsrats mitgeteilt werden müsse, wurde einerseits gesagt, dies könne unterschiedlich gehandhabt werden, und andererseits, eine Information erfolge nur dann, wenn es auch andere Direktionen betreffe. Eine systematische Information des Regierungsrats über laufende Administrativuntersuchungen gebe es nicht, wenn andere Direktionen vom Thema nicht betroffen seien.[711]

Schliesslich konnte die PUK Datensicherheit bei den Befragungen feststellen, dass die einzelnen Direktionsvorstehenden teilweise ein unterschiedliches Verständnis für den Begriff der Administrativuntersuchung und deren Umfang haben.[712]

12.5 Meldung an die Datenschutzbeauftragte

Die Datenschutzbeauftragte des Kantons Zürich, Dominika Blonski, erklärte gegenüber der PUK Datensicherheit, dass die Meldung zum Datensicherheitsvorfall am 30. November 2020 als Standardmeldung über das auf der Webseite zur Verfügung

---

[708] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 33–34, 38, 41.

[709] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 31.

[710] Schreiben «Weitere Auskünfte und Unterlagen, Administrativuntersuchungen» der Staatsschreiberin Kathrin Arioli an die PUK Datensicherheit vom 23. März 2025 inkl. Beilage «Liste Direktionen Anzahl durchgeführter Administrativuntersuchungen».

[711] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 31–33; Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S.19; Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 26; Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 25; Protokoll der Befragung von Carmen Walker Späh vom 13. Dezember 2024, S. 18–19, 21; Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 16; Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 26–27, 30.

[712] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 32; Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S.19; Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 26; Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 25; Protokoll der Befragung von Carmen Walker Späh vom 13. Dezember 2024, S. 18–19, 21; Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 16; Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 26–27, 30.

gestellte Formular eingegangen sei.[713] Grundsätzlich empfehle sie, einen Vorfall so schnell wie möglich zu melden, auch wenn zu diesem Zeitpunkt noch nicht alles bekannt sei. Viele Vorfälle würden erst nach drei bis vier Wochen gemeldet, da die betroffenen Stellen etwas Zeit benötigen, um sich zu organisieren. Die Zeitdauer vom Vorfall bis zur Meldung durch die JI sei ihr daher nicht speziell lang vorgekommen.[714]

Am 2. Dezember 2020 bestätigte die Datenschutzbeauftragte den Eingang der Meldung.[715] Seitens der JI wurde die Datenschutzbeauftragte laut ihren eigenen Aussagen zudem darüber informiert, dass die JI eine Administrativuntersuchung in Auftrag gegeben habe.[716] Sie habe daraufhin entschieden abzuwarten, welche Themen in Rahmen der Untersuchung aufkommen, und dann darauf zu reagieren. In der Zwischenzeit habe sie – wie die Autorinnen der Administrativuntersuchung auch – allfällige Sofortmassnahmen geprüft, zum damaligen Zeitpunkt aber keinen Anlass für solche gesehen.[717]

Am 10. Februar 2021, so die Datenschutzbeauftragte, habe sie sich nach dem Stand der Administrativuntersuchung sowie allenfalls getroffenen Sofortmassnahmen erkundigt. Gleichentags sei sie von der JI informiert worden, dass der Zwischenbericht Ende Januar 2021 eingegangen sei, keine Sofortmassnahmen zu treffen seien und der Schlussbericht Ende Februar vorliegen sollte. Sie habe daraufhin die JI gebeten, ihr den Schlussbericht zuzustellen, sobald dieser vorliege.[718]

Als keine Zustellung durch die JI erfolgt sei, habe sie sich am 28. Mai 2021 erneut zum Stand der Administrativuntersuchung erkundigt und um Zustellung des Schlussberichts gebeten. Diesen habe sie schliesslich am 31. Mai 2021 erhalten, also zwei Monate nach dessen Zustellung an die Direktion.[719]

Die Datenschutzbeauftragte erklärte, sie habe auf Grundlage des Schlussberichts das Ergebnis der Administrativuntersuchung sowie die festgehaltenen Massnahmen geprüft und beurteilt. Sie habe die Massnahmen als gut befunden und dies in ihrer Stellungnahme vom 15. September 2021 entsprechend festgehalten.[720] Darin empfahl die Datenschutzbeauftragte die Umsetzung der hoch priorisierten Massnahmen innert Jahresfrist und bat darum, über die Umsetzung mit geeigneter Dokumentation informiert zu werden. Weiter führte sie in ihrer Stellungnahme aus, sie habe keine Informationen darüber, wie viele Personen von der unbefugten Verarbeitung ihrer Personendaten betroffen waren. Vermutlich seien nur diejenigen Personen bekannt, deren Dokumente der Staatsanwaltschaft übergeben worden waren. Der Inhalt dieser Dokumente sei ihr nicht bekannt, weshalb sich der Grad der Beeinträchtigung der Grundrechte der Betroffenen nicht einschätzen lasse. Sie sei davon ausgegangen, dass die unbefugte Verwendung von Informationen durch den externen Dienstleister straf-

---

713 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 4–6; Teilprotokoll der GPK zur Anhörung von Dominika Blonski vom 26. Januar 2023, S. 2; siehe auch E-Mail «Meldung Datenschutzvorfall» der Datenschutzbeauftragten an die Generalsekretärin der JI vom 2. Dezember 2020 (inkl. der automatischen Meldungsbestätigung vom 30. November 2020).

714 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 10–11.

715 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 5; Teilprotokoll der GPK zur Anhörung von Dominika Blonski vom 26. Januar 2023, S. 2; E-Mail «Meldung Datenschutzvorfall» der Datenschutzbeauftragten an die Generalsekretärin der JI vom 2. Dezember 2020.

716 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 5; Teilprotokoll der GPK zur Anhörung von Dominika Blonski vom 26. Januar 2023, S. 2.

717 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 6.

718 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 6; Teilprotokoll der GPK zur Anhörung von Dominika Blonski vom 26. Januar 2023, S. 2.

719 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 6; Teilprotokoll der GPK zur Anhörung von Dominika Blonski vom 26. Januar 2023, S. 2.

720 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 6; Teilprotokoll der GPK zur Anhörung von Dominika Blonski vom 26. Januar 2023, S. 2.

rechtlich verfolgt werde und die betroffenen Personen möglicherweise von der Staatsanwaltschaft in diesem Rahmen informiert worden seien. Eine nachträgliche Benachrichtigung, so die Datenschutzbeauftragte, ermögliche es den Personen nicht, Vorkehrungen zum effektiven Schutz gegen die Folgen der unbefugten Datenbearbeitung zu ergreifen. In den übrigen Fällen, in denen die betroffenen Personen nicht bekannt seien, sei eine Information sowieso nicht möglich. Sie folgerte, dass daher eine öffentliche Bekanntmachung in dieser Situation als nicht sinnvoll zu erachten sei.[721]

Da eine Rückmeldung seitens der JI auf ihre Stellungnahme ausgeblieben war, erinnerte die Datenschutzbeauftragte mit Schreiben vom 13. Oktober 2022 die Generalsekretärin der JI daran und bat sie um Informationen zum Stand der Umsetzung der Massnahmen bis zum 30. November 2022. Am 28. November 2022 sei sie von der stellvertretenden Generalsekretärin, Susanna Stählin, zunächst telefonisch und danach per E-Mail informiert worden, dass die JI den Entschluss gefasst habe, die Empfehlungen etwas breiter anzugehen.

Die Kontaktaufnahme fällt zeitlich mit der Einreichung der Anfrage KR-Nr. 456/2022 (siehe Kapitel 13.2) zusammen. Dazu befragt, gab die Direktionsvorsteherin, Jacqueline Fehr, an, es sei vorstellbar, dass man dieses Dossier anlässlich der eingereichten Anfrage hervorgeholt und geschaut habe, was da noch zu tun sei.[722] Die Datenschutzbeauftragte führte aus, dass sie aufgrund dieser Kontaktaufnahme auf Ende Januar 2023 ein Anschlusstreffen mit der JI vereinbart habe.[723]

12.6 Mündliche Information an den Gesamtregierungsrat

Nachdem die Direktionsvorsteherin der JI, Jacqueline Fehr, am 9. November 2020 vom Datensicherheitsvorfall erfahren hatte, erwähnte sie an der Regierungsratssitzung vom 18. November 2020 anlässlich der Beratung eines Geschäfts betreffend die Vergabe von Unterhaltsreinigungen der kantonalen Verwaltungsbauten, dass die JI mit einem Datensicherheitsvorfall konfrontiert sei.[724]

Die PUK Datensicherheit zog die Unterlagen zur Regierungsratssitzung vom 18. November 2020 bei. Es ging daraus hervor, dass der Regierungsrat im Zusammenhang mit der Vergabe der Unterhaltsreinigung der kantonalen Verwaltungsbauten[725] von einer Aktennotiz zur Sicherheitsüberprüfung eines Reinigungsdienstleisters Kenntnis nahm.[726] In diesem Zusammenhang habe sich die Direktionsvorsteherin der JI erkundigt, ob das Reinigungspersonal sicherheitsüberprüft werde und ob, falls dies nicht der Fall sei, eine solche Überprüfung angezeigt wäre. Sie habe hinzugefügt, dass sie diese Frage stelle, weil sie gerade mit einem möglicherweise sehr schweren, möglicherweise aber auch sehr harmlosen Datensicherheitsvorfall konfrontiert sei. Sie sei von der Oberstaatsanwaltschaft informiert worden und der Vorfall werde nun untersucht.

---

721 Datenschutzbeauftragte des Kantons Zürich, Stellungnahme, Meldung der nicht fachgerechten Entsorgung von Rechnern und des potenziellen Datenmissbrauchs, 15. September 2021.

722 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 38.

723 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 7; Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 24; Teilprotokoll der GPK zur Anhörung von Dominika Blonski vom 26. Januar 2023, S. 2.

724 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 31.

725 RRB Nr. 1148/2020 vom 25. November 2020, Unterhaltsreinigung der kantonalen Verwaltungsbauten, wiederkehrende gebundene Ausgabe, Vergabe.

726 Baudirektion, Immobilienamt, Facilitymanagement, Aktennotiz vom 13. November 2020 «Sicherheitsüberprüfung Reinigungsdienstleister».

Gemäss Aussagen von Regierungsrätin Jacqueline Fehr erinnern sich aber nicht mehr alle Mitglieder des Regierungsrates gleichermassen an diese Mitteilung. Auch sie selbst bezeichnete es rückblickend als eine nur beiläufige Information. Gemäss ihren Aussagen war eine gezielte Information nicht angezeigt, da es sich beim Datensicherheitsvorfall um einen direktionspezifischen Vorfall gehandelt habe, der keine Sofortmassnahmen erforderte.[727]

Durch die Befragungen konnte die PUK Datensicherheit feststellen, dass nur wenige Mitglieder des Regierungsrates die Information über den Datensicherheitsvorfall mit dem Geschäft zur Vergabe eines Auftrags für Reinigungsarbeiten in Verbindung bringen konnten. Der Grossteil der Regierungsratsmitglieder gab an, erst zwei Jahre später, Ende November 2022, als der Vorfall öffentlich bekannt geworden sei, davon Kenntnis genommen zu haben.[728]

12.7 Erste Information an die Geschäftsprüfungskommission (GPK)

Die Direktionsvorsteherin der JI, Jacqueline Fehr, führte aus, dass sie den für die JI zuständigen Referenten der GPK am 1. März 2021, im Rahmen des Frühlingsgesprächs, mündlich und schriftlich über den Datensicherheitsvorfall informiert habe.[729] Auch der ehemalige Präsident der GPK, Beat Habegger, erklärte, dass der für die JI zuständige Referent, Kantonsrat René Isler, im März 2021 durch die Direktionsvorsteherin anlässlich des Referentengesprächs über den Datensicherheitsvorfall informiert worden sei.[730] Dem der PUK Datensicherheit vorliegenden diesbezüglichen Schreiben ist unter Ziffer 3 mit dem Titel «Baustellen» zu entnehmen, dass auf die Administrativuntersuchung und den Verdacht auf Datenmissbrauch hingewiesen wurde. Es wurde hierbei sowohl der Umfang der Administrativuntersuchung dargelegt als auch ausgeführt, dass im Zwischenbericht von Ende Januar 2021 keine Empfehlungen zu Sofortmassnahmen enthalten seien und dass der Schlussbericht mit Empfehlungen in der ersten Jahreshälfte 2021 vorliegen werde.[731]

Der ehemalige GPK-Präsident, Beat Habegger, erklärte, dass dieses Schreiben der GPK zur Kenntnis gebracht worden sei. Dem Protokoll der damaligen Kommissionssitzung seien jedoch weder Bemerkungen des Referenten noch Fragen der Kommission zu dieser Thematik zu entnehmen. Die GPK sei sich im März 2021 der Tragweite des Datensicherheitsvorfalls noch nicht bewusst gewesen. Dies wäre aber auch sehr schwer zu erkennen gewesen. Danach gab es laut dem ehemaligen GPK-Präsidenten zum Datensicherheitsvorfall keine proaktive Information seitens der Direktionsvorsteherin mehr.[732]

Gegenüber der PUK Datensicherheit gestand die Direktionsvorsteherin in Bezug auf die Kommunikation mit den Behörden Fehler ein und ergänzte, dass sie in der JI aus diesen Schlüsse gezogen hätten und diesbezüglich nun aufmerksamer seien.[733]

---

727 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 31–32.

728 Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S. 18; Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 24–25; Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 24; Protokoll der Befragung von Carmen Walker Späh vom 13. Dezember 2024, S. 19–20; Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 15; Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 24.

729 Protokoll der Kantonsratssitzung vom 9. Januar 2023, S. 7.

730 Protokoll der Befragung von Beat Habegger vom 27. September 2024, S. 7.

731 Schreiben «GPK – Referentengespräch; Antworten zu den Themen» vom 1. März 2021 von Jacqueline Fehr an die GPK und René Isler.

732 Protokoll der Befragung von Beat Habegger vom 27. September 2024, S. 7.

733 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 37.

12.8 Würdigung durch die PUK

Es wird eine Gesamtwürdigung der Kapitel 12 und 13 in Kapitel 13.16 vorgenommen.

13. Umgang mit dem Datensicherheitsvorfall nach dem öffentlichen Bekanntwerden

13.1 Abgabe von Informationen an Behörden und Medien anlässlich der Berufungsverhandlung vom 4. November 2022

Am 4. November 2022 machte Roland Gisler im Rahmen seiner Berufungsverhandlung vor dem Obergericht (siehe Kapitel 12.1.2) den Medien und den Mitgliedern der Behörden Unterlagen mit sensitiven Daten zugänglich. Er gab einen ganzen Ordner mit Akten ab und äusserte, dass noch weitere Daten vorhanden seien. Damit kam gemäss der Aussage des ehemaligen Leitenden Oberstaatsanwalts, Andreas Eckert, der Fokus auf den Datensicherheitsvorfall. Im Rahmen des Strafverfahrens der Staatsanwaltschaft Zürich-Sihl waren zwar Datenträger sichergestellt worden, aber erst der Vorfall vom 4. November 2022 habe sie aufgeschreckt und man sei so richtig auf den Datensicherheitsvorfall aufmerksam geworden. Die damals bereits laufende Untersuchung hatte sich stärker auf den Aspekt der Bedrohung konzentriert, der Aspekt der Datenentsorgung stand weniger im Fokus. Im Verlauf des Novembers thematisierte man die Vorfälle vom 4. November 2022 auch im Rahmen des Kaderdialogs zwischen der Direktionsvorsteherin der JI, ihrem Stab und der Geschäftsleitung der Oberstaatsanwaltschaft. Dabei stellte die Direktionsvorsteherin dem Leitenden Oberstaatsanwalt die Übermittlung des Berichts der Administrativuntersuchung in Aussicht.[734]

Die Oberstaatsanwaltschaft entschied am 5. Dezember 2022, den Teilaspekt der Datenentsorgung einer vertieften strafrechtlichen Prüfung zu unterziehen und diese Abklärung an die kantonale Staatsanwaltschaft III zu übergeben, die Erfahrungen und Kompetenzen im Umgang mit Wirtschaftsdelikten hatte und 2014 auch die Untersuchung bei der Informatik der JI rund um den Leiter Logistik, Finanzen & Controlling (LFC), Renato Widmer, geführt hatte.[735] Zwischen dem Vorfall vom 4. November 2022 und der Ausweitung der Untersuchung am 5. Dezember 2022 verging ein ganzer Monat. Währenddessen war der Leitende Oberstaatsanwalt davon ausgegangen, den Schlussbericht zur Administrativuntersuchung zeitnah zu erhalten, er erhielt diesen jedoch erst am 3. Dezember 2022. Gemäss seinen Angaben war der Vorfall vom 4. November 2022 und nicht die späteren Entwicklungen für die Ausweitung ausschlaggebend.[736]

In der Zwischenzeit hatte der Datensicherheitsvorfall jedoch bereits weitere Kreise gezogen und die Öffentlichkeit erreicht.

13.2 Bekanntmachung durch die Anfrage KR-Nr. 456/2022

Am 28. November 2022 wurde die Anfrage KR-Nr. 456/2022 «Vorgehen und Verantwortlichkeiten in der Justizdirektion bei der Entsorgung von Datenträgern» eingereicht. Erstunterzeichner war Valentin Landmann, der auch der Rechtsvertreter von Roland Gisler war. In der Anfrage schrieben die Kantonsratsmitglieder, dass bei der Erneuerung von Computerhardware in verschiedenen Bereichen der Justizdirektion zahlreiche Festplatten mit teils hochsensitiven, ungelöschten Daten falsch entsorgt worden und in der Folge ins Zürcher Drogen- und Sexmilieu gelangt seien. Die Festplatten hätten unter anderem vom Amtsgeheimnis geschützte Unterlagen und Daten, wie psychiatrische Gutachten, Gefährlichkeitsgutachten über verschiedene Beschuldigte, Handytelefonlisten von Polizeibeamten, Unterlagen aus der Planung des PJZ, Zuteilung von Räumen des PJZ sowie Unterlagen des Psychiatrisch-Psychologischen Dienstes, ent-

[734] Protokoll der Befragung von Andreas Eckert vom 28. Februar 2025, S. 10–14.

[735] Protokoll der Befragung von Andreas Eckert vom 28. Februar 2025, S. 9.

[736] Protokoll der Befragung von Andreas Eckert vom 28. Februar 2025, S. 8.

halten.[737] Die Ratsmitglieder wollten vom Regierungsrat wissen, wie der Umgang mit zu entsorgenden Datenträgern geregelt sei, wie der Vorfall bei der JI geschehen konnte und inwiefern die JI darüber einen Überblick habe, wie man auf diesen Vorfall reagierte, und ob bezüglich Organisation und Entsorgungsabläufen Massnahmen ergriffen worden seien. Als die Direktionsvorsteherin der JI, Jacqueline Fehr, die Anfrage in jener Woche im Versand des Kantonsrates sah, war sie zwar etwas erstaunt darüber, dass dieses Thema wieder aufkam, erfasste die Dimension des Ganzen aber noch nicht.[738]

Die Anfrage wurde an der Sitzung vom 8. Februar 2023, also erst einen Monat nach der Beantwortung der dringlichen Interpellation KR-Nr. 462/2022 (vgl. Kapitel 13.7) und erst nach dem Beschluss der GPK vom 26. Januar 2023, dem Kantonsrat einen Antrag auf Einsetzung einer PUK zu stellen, durch den Regierungsrat beantwortet und dem Kantonsrat zu Kenntnis gebracht.

Bezüglich der Entsorgung von Datenträgern verwies die Antwort des Regierungsrates auf das Gesetz über die Information und den Datenschutz (IDG), welches die Löschung bzw. die Vernichtung der Informationen regelt, die durch das zuständige Amt nicht archiviert werden, sowie auf die Besonderen Informationssicherheitsrichtlinien (BISR) und den Leitfaden «Umgang mit Wechseldatenträgern».

Zu den Umständen und dem Umfang des Verlusts der Datenträger resp. der Daten konnte aufgrund des laufenden Strafverfahrens keine Aussage gemacht werden.

Bei der Frage bezüglich der Reaktion der Verwaltung verwies der Regierungsrat auf die Meldung an den kantonalen Informationssicherheitsbeauftragten und die Datenschutzbeauftragte sowie auf die Eröffnung des Strafverfahrens durch die Staatsanwaltschaft. Auch hielt er fest, dass die Direktionsvorsteherin sich vergewissert habe, dass es im Bereich Informationssicherheit keine erkennbaren Risiken mehr gebe. Weiter wies er auf die in Auftrag gegebene Administrativuntersuchung hin, die zum Zeitpunkt der Beantwortung der Anfrage (aber nicht zum Zeitpunkt von deren Einreichung) veröffentlicht war.

Schliesslich wurde hinsichtlich Zuständigkeiten sowie Unbrauchbarmachung und Entsorgung der seit 2010 zertifizierte Ablauf für die Entsorgung erwähnt.

Die Beantwortung der Anfrage hielt zusammenfassend fest: «Ein Datensicherheitsvorfall, wie er sich damals ereignete, ist heute für die Direktion der Justiz und des Innern technisch und organisatorisch ausgeschlossen. Dies bestätigte auch die Administrativuntersuchung aus dem Jahr 2021.»[739]

13.3 Datensicherheitsvorfall in den Medien

Parallel zu diesen Entwicklungen erhielt die JI Kenntnis darüber, dass gewissen Medien Informationen zum Datensicherheitsvorfall vorlagen. Dennoch verzichtete die JI gemäss deren Leiter Kommunikation, Benjamin Tommer, angesichts des laufenden Strafverfahrens auf eine öffentliche Kommunikation.[740] Ab Freitag, 2. Dezember 2022, erhielt der Datensicherheitsvorfall aber eine grosse mediale Aufmerksamkeit.[741]

---

[737] Anfrage KR-Nr. 456/2022 vom 28. November 2022, Vorgehen und Verantwortlichkeiten in der Justizdirektion bei der Entsorgung von Datenträgen.

[738] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 38.

[739] RRB Nr. 181/2022 vom 8. Februar 2023, Anfrage (Vorgehen und Verantwortlichkeiten in der Justizdirektion bei der Entsorgung von Datenträgern).

[740] Protokoll der Befragung von Benjamin Tommer vom 27. November 2024, S. 9.

[741] So titelte die Zeitung Blick am 2. Dezember 2022 «Riesiges Datenleck bei Zürcher Justiz!» und beim Tages-Anzeiger war «Leck bei Justizdirektion: Sensible Daten landeten im Drogen- und Sexmilieu» zu lesen. Auch im Schweizer Radio SRF und im Online-Medium Inside-it gab es eine Meldung.

Daraufhin bestätigte die JI im Rahmen einer Medienmitteilung vom 2. Dezember 2022 den thematisierten Datensicherheitsvorfall. Es wurde ausgeführt, dass vermutlich Computer-Hardware durch einen ehemaligen Dienstleister nicht ordnungsgemäss vernichtet und gespeicherte Daten nicht gelöscht worden waren und dass möglicherweise auch sensitive Daten betroffen seien. Man verzichtete aber darauf, sich weiter dazu zu äussern.[742]

Über das Wochenende berichteten weitere Medien über den Vorfall.[743] Die Direktionsvorsteherin der JI und der Leitende Oberstaatsanwalt tauschten sich über das Wochenende intensiv aus. Denn ab dem Moment, als die Informationen durch die Medienberichterstattung öffentlich geworden seien, sei der Grund für die zurückhaltende Kommunikation, nämlich die Vermeidung der Gefährdung des Strafverfahrens, weggefallen. Im Rahmen dieses Austausches erhielt der ehemalige Leitende Oberstaatsanwalt am Samstag, 3. Dezember 2022, auch den Bericht der Administrativuntersuchung. Die JI habe sich dann für einen Point de Presse entschieden. Durch eine eigene Information sollten schwerwiegende Reputationsrisiken ausgeschlossen werden.[744] Der ehemalige Leitende Oberstaatsanwalt gab an, die Beteiligung am Point de Presse abgelehnt zu haben.[745]

13.4 Reaktion der Direktion der Justiz und des Innern (JI)

Nachdem der Datensicherheitsvorfall durch Roland Gisler im Rahmen der Gerichtsverhandlung vom 4. November 2022 und durch die Anfrage im Kantonsrat vom 28. November 2022 wieder aufgebracht worden war, habe sich die JI laut Aussagen der Direktionsvorsteherin, Jacqueline Fehr, entschieden, den «Stier an den Hörnern» zu packen und die Thematik breiter anzugehen.[746] Auch die stellvertretende Generalsekretärin, Susanna Stähelin, führte aus, dass aufgrund der Empfehlungen der Administrativuntersuchung, wohl in Kombination mit den politischen und medialen Entwicklungen, ein «Ruck» durch die Direktion bzw. die Managementebene gegangen und die Thematik ernst genommen worden sei.[747]

Im Zusammenhang mit der Anfrage KR-Nr. 456/2022 hatte die Direktionsvorsteherin bereits am 30. November 2022 den GPK-Präsidenten per E-Mail über den Vorfall informiert.[748] Die E-Mail war sowohl an Beat Habegger als auch an den Referenten der JI, René Isler, adressiert und verwies noch einmal auf das Frühjahrsgespräch 2021. Gleichzeitig wies die Direktionsvorsteherin in der E-Mail darauf hin, dass aktuell ein Strafverfahren laufe und sie keine Auskünfte erteilen könne.[749]

---

[742] Direktion der Justiz und des Innern, Medienmitteilung vom 2. Dezember 2022 «Datensicherheitsvorfall bei der Direktion JI in den Jahren 2006 bis 2012».

[743] Beispielsweise berichtete nun neben dem Blick und dem Tages-Anzeiger auch die Neue Zürcher Zeitung darüber.

[744] Protokoll der Befragung von Benjamin Tommer vom 27. September 2024, S. 9.

[745] Protokoll der Befragung von Andreas Eckert vom 28. Februar 2025, S. 15.

[746] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 33 f./S. 37; Protokoll der Kantonsratssitzung vom 9. Januar 2023, S. 7.

[747] Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 12–13.

[748] Protokoll der Befragung von Beat Habegger vom 27. September 2024, S. 7.

[749] E-Mail mit Betreff «Anfrage KR-Nr. 456/2022 – Information an GPK» vom 30. November 2022 von Jacqueline Fehr an Beat Habegger und René Isler.

13.5 Ausweitung des Strafverfahrens

Der Leitende Oberstaatsanwalt berief am Montag, 5. Dezember 2022, eine Geschäftsleitungssitzung ein. Im Hinblick auf die bevorstehende Kommunikation der JI ging es dabei auch darum, zu klären, inwieweit der Schlussbericht der Administrativuntersuchung aus Sicht der Staatsanwaltschaft vor der Herausgabe geschwärzt werden musste. An jenem Tag habe die Oberstaatsanwaltschaft entschieden, das Strafverfahren auszuweiten und die beiden Untersuchungen – jene der Staatsanwaltschaft Zürich-Sihl und jene der Staatsanwaltschaft III – zu Schlüsselfällen zu erklären, bei denen kein Untersuchungsschritt und keine Kommunikation ohne Rücksprache mit der zuständigen Oberstaatsanwältin oder dem zuständigen Oberstaatsanwalt unternommen werden dürfen. Gegenüber der PUK Datensicherheit räumte der Leitende Oberstaatsanwalt ein, dass der Aspekt der Datenentsorgung lange «etwas nebensächlich war» und man das intern wohl schon früher zu einem Schlüsselfall oder Medienschlüsselfall hätte erklären sollen.[750] Allenfalls wäre man dann früher auf die Administrativuntersuchung gestossen. Wäre sie 2021 schon bekannt gewesen, hätte man diesen Punkt vielleicht bereits früher vertieft angeschaut.[751]

13.15.1 Strafverfahren der Staatsanwaltschaft III des Kantons Zürich

In der Folge wurde die Staatsanwaltschaft III damit beauftragt – ergänzend zu den bisherigen Ermittlungsergebnissen der seit November 2020 durch die Staatsanwaltschaft Zürich-Sihl geführten Untersuchung gegen Roland Gisler (siehe Kapitel 12.1.1) –, den Teilaspekt der Datenentsorgung einer vertieften strafrechtlichen Prüfung zu unterziehen.[752] Am 6. Dezember 2020 informierte die Oberstaatsanwaltschaft öffentlich über die Ausweitung des Strafverfahrens.[753] Die Kommunikation zwischen der Oberstaatsanwaltschaft und der JI erfolgte mit Blick auf den von der JI auf denselben Tag angesetzten Point de Presse koordiniert.[754]

Diese ergänzenden Untersuchungen der Staatsanwaltschaft III richteten sich gegen eine unbekannte Täterschaft, was die Untersuchungsmöglichkeiten wesentlich einschränkte. Im Rahmen dieser Grenzen betrieb die Staatsanwaltschaft III einen grossen Aufwand, um zur Klärung der Fragen im öffentlichen Interesse beizutragen. Die PUK Datensicherheit koordinierte ihre Untersuchung mit der Staatsanwaltschaft III und konnte sehr von deren Vorarbeiten profitieren.

13.6 Point de Presse vom 6. Dezember 2022

Die Direktionsvorsteherin der JI, Jacqueline Fehr, informierte am 6. Dezember 2022 gemeinsam mit dem Leiter der Digital Solutions, Urs Kaderli, und der Autorin der Administrativuntersuchung, Maria Winkler, im Rahmen eines Point de Presse die Öffentlichkeit und stellte die Administrativuntersuchung in geschwärzter Form zur Verfügung.[755] Der Schlussbericht der Administrativuntersuchung wurde am selben Tag auch dem Regierungsrat zugestellt.[756]

---

750 Weisung der Oberstaatsanwaltschaft für das Vorverfahren (WOSTA) vom 14. Mai 2025.

751 Protokoll der Befragung von Andreas Eckert vom 28. Februar 2025, S. 9–15.

752 Oberstaatsanwaltschaft, Medienmitteilung vom 6. Dezember 2022 «Staatsanwaltschaft prüft mögliches strafrechtliches Fehlverhalten bei Datenentsorgung vertieft»; Protokoll der Befragung von Andreas Eckert vom 28. Februar 2025, S. 8–9.

753 Oberstaatsanwaltschaft, Medienmitteilung vom 6. Dezember 2022 «Staatsanwaltschaft prüft mögliches strafrechtliches Fehlverhalten bei Datenentsorgung vertieft».

754 Protokoll der Befragung von Benjamin Tommer vom 27. September 2024, S. 17.

755 Direktion der Justiz und des Innern, Point de Presse vom 6. Dezember 2022 «Konsequenzen aus dem Datensicherheitsvorfall bei der Direktion JI».

756 Protokoll der Kantonsratssitzung vom 9. Januar 2023, S. 7.

Am Point de Presse führte die Regierungsrätin detailliert aus, welche Schritte sie nach dem internen Bekanntwerden des Datensicherheitsvorfalls ergriffen hatte, und stellte den zeitlichen Ablauf vor. Es folgten Ausführungen zu den Erkenntnissen der Administrativuntersuchung sowie zum Stand der Informationssicherheit in der Direktion und im Kanton. Bezüglich der zeitweisen Nicht-Veröffentlichung des Schlussberichts der Administrativuntersuchung verwies sie auf die Stellungnahme der Datenschutzbeauftragten und sagte, dass sie auf deren Empfehlung von einer Veröffentlichung abgesehen habe. Zugleich äusserte sie rückblickend aber auch Zweifel an der eigenen Kommunikationsstrategie. Gegenüber den Journalistinnen und Journalisten gab Jacqueline Fehr an, dass die damalige Entsorgung «in höchstem Masse dilettantisch, unprofessionell und möglicherweise auch strafrechtlich relevant» gewesen sei. Nach ihrer Beurteilung sei das, was damals geschehen sei, unter keinen Titeln zu rechtfertigen. Sie räumte weiter ein, dass der Schlussbericht der Administrativuntersuchung der GPK bereits früher hätte zugeleitet werden sollen. Auch Fragen zu technischen Details, zur Dokumentation von Löschungen, zur Aufräumaktion 2019 sowie zu personellen Konsequenzen wurden beantwortet. Gegenüber einer parlamentarischen Untersuchung durch die GPK oder durch die Einsetzung einer Untersuchungskommission zeigte sich die Regierungsrätin offen. Sie wies hinsichtlich des Ausmasses des Datensicherheitsvorfalls aber ausdrücklich darauf hin, dass die den Medien zugespielten Unterlagen wohl auch aus anderen Quellen stammen könnten.[757]

13.7 Vertiefte Nachfrage durch die dringliche Interpellation KR-Nr. 462/2022

Am Montag, 5. Dezember 2022, reichten fünf Mitglieder des Kantonsrates die dringliche Interpellation KR-Nr. 462/2022 betreffend «Verantwortlichkeiten bei der Justizdirektion verlangen Aufklärung» ein. Die Fragen drehten sich namentlich um das Ausmass des Vorfalls, um die Administrativuntersuchung sowie um die Kommunikation der JI gegenüber der Geschäftsprüfungskommission und der Gesamtregierung.[758] Die Direktionsvorsteherin, Jacqueline Fehr, beantwortete in der Kantonsratssitzung vom 9. Januar 2023 die Fragen der dringlichen Interpellation.[759] Sie machte Angaben zur Administrativuntersuchung, zur Meldung an die GPK vom 1. März 2021 und zur umfassenden Information des Regierungsrates vom 21. Dezember 2022. Sie informierte, dass keine der Personen, die bei der Entsorgung eine aktive Rolle gespielt hatten, noch beim Kanton arbeite und dass die Staatsanwaltschaft bereits im November 2020 ein Strafverfahren eingeleitet habe und betroffene Personen in diesem Rahmen informiert würden. Zur ausgebliebenen öffentlichen Kommunikation hielt sie fest, das Ergebnis der Administrativuntersuchung sei nicht veröffentlicht worden, um das laufende Strafverfahren nicht zu gefährden. Sie gab weiter an, dass der Regierungsrat aktuell keinen Überblick über die Menge und Anzahl der Datenträger sowie über deren Inhalt habe. Abschliessend hielt sie fest, dass das Ausmass des Datenmissbrauchs erst nach dem Abschluss der strafrechtlichen Untersuchung abschätzbar sei. Sie könne jedoch bestätigen, dass sich die sachgerechten Datenträgerentsorgungen ab dem Jahr 2010 inzwischen wieder mit Zertifikaten belegen liessen.

---

[757] Direktion der Justiz und des Innern, Point de Presse vom 6. Dezember 2022 «Konsequenzen aus dem Datensicherheitsvorfall bei der Direktion JI».

[758] Dringliche Interpellation KR-Nr. 462/2022 am 5. Dezember 2022.

[759] Protokoll der Kantonsratssitzung vom 9. Januar 2023, S. 6–35.

Im Rahmen der folgenden Debatte kritisierten diverse Kantonsratsmitglieder die Kommunikation gegenüber dem Gesamtregierungsrat, der GPK und der Öffentlichkeit. Auch die Umstände der Aufräumaktion 2019 und die unsachgemässe Entsorgung von Papierakten (siehe Kapitel 13.8) gaben zu reden. Verschiedene Ratsmitglieder forderten die Einsetzung einer Parlamentarischen Untersuchungskommission.[760]

13.8 Eklat am Rande der Kantonsratssitzung vom 19. Dezember 2022

Zwischen der Einreichung der dringlichen Interpellation am 5. Dezember 2022 und deren Beantwortung im Kantonsrat durch die Justizdirektorin, ereignete sich am Rande der Kantonsratssitzung vom 19. Dezember 2022 ein Eklat. Roland Gisler deponierte während der Sitzung drei Kisten sowie einen Koffer mit Dokumenten und Harddisks der JI medienwirksam im Foyer des damaligen Kantonsratsprovisoriums in der Messe Zürich. Die dabei sichergestellten Papierakten und Datenträger flossen ebenfalls ins Verfahren der Staatsanwaltschaft III ein.[761] Nach der Sicherstellung liess die Staatsanwaltschaft III die Akten sichten. Dabei wurden folgende Kategorien von Unterlagen unterschieden (siehe als Beispiel Abbildung 6):[762]

- Kategorie 1: Interne JI-Akten ohne konkreten Personenbezug
- Kategorie 2: JI-Akten mit personenbezogenen Informationen über JI-Personal
- Kategorie 3: JI-Akten mit personenbezogenen Informationen über Dritte

Abbildung 6 Am 19. Dezember 2022 sichergestellte Akten, inkl. Behältnis

Quelle: Fotobogen Sicherstellungen, Beilage zum Nachtragsbericht vom 22. Mai 2024.

760 Protokoll der Kantonsratssitzung vom 9. Januar 2023, S. 9, 13–14, 21, 29, 31.

761 Oberstaatsanwaltschaft, Medienmitteilung vom 19. Dezember 2022 «Datensicherheitsvorfall: Staatsanwaltschaft stellt im Kantonsrat abgegebene Papierakten und Datenträger sicher»; Artikel der Zeitung Tages-Anzeiger «Auch die Sicherheitsdirektion ist vom Justiz-Datenleck betroffen» vom 23. Januar 2023 (und weitere).

762 Kantonspolizei, Polizeilicher Ermittlungsbericht, Nachtrag vom 22. Mai 2024 zur Sichtung der physischen Unterlagen; Schlussbericht zum Ermittlungsverfahren Memory vom 19. Dezember 2024, S. 17.

Bei den nicht-sensitiven internen Unterlagen der Kategorie 1 handelte es sich um RIS-Projektunterlagen. Auch die sensitiven internen Unterlagen der Kategorie 2 wiesen vorwiegend einen Bezug zur Entwicklung des Rechtsinformationssystems auf. Es handelte sich dabei beispielsweise um interne E-Mail-Korrespondenz. Bei der dritten Kategorie, der nur ein kleiner Teil zuzuordnen war, handelte es sich um Unterlagen aus Ämtern. So lagen aus dem Gemeindeamt beispielsweise Einbürgerungs- oder Eheschliessungslisten vor. Aus den Bewährungs- und Vollzugsdiensten stammten Listen zu Insassen oder Listen über Ab- und Zugänge und Versetzungen. Von der Staatsanwaltschaft existierten beispielsweise Untersuchungshaft-Listen oder Listen zu Verjährungsstichtagen. Bei den Unterlagen aus den Statthalterämtern handelte es sich um Korrespondenzen beschuldigter Personen.

Gemäss den Ermittlungen der Staatsanwaltschaft III standen die genannten Dokumente im Zusammenhang mit der RIS-Entwicklung und dienten in diesem Kontext als Vorlagen. Es handelte sich also explizit nicht um nachträglich ausgedruckte Unterlagen.[763] Die PUK Datensicherheit konnte sich im Rahmen der Sitzung vom 26. Januar 2025 selbst einen Eindruck über die Art der abgegebenen Akten verschaffen. Auch für sie war der Vorlagencharakter der Unterlagen ersichtlich.

13.9 Zweite Information an die Geschäftsprüfungskommission (GPK)

Nachdem der damalige GPK-Präsident, Beat Habegger, am 30. November 2022 von der Direktionsvorsteherin informiert worden war, traktandierte die GPK daraufhin den Datensicherheitsvorfall für die Sitzung vom 8. Dezember 2022 und lud die Direktionsvorsteherin ein. Im Vorfeld der Sitzung habe die GPK, so der damalige GPK-Präsident, zudem den Schlussbericht der Administrativuntersuchung erhalten.[764] Dieser sei der GPK nicht zeitnah nach dessen Eingang bei der JI übermittelt worden. Auf die Rückfrage durch die PUK Datensicherheit, ob die GPK es unterlassen habe, sich aktiv nach dem Schlussbericht und den weiteren Entwicklungen zu erkundigen, antwortete der GPK-Präsident, dies sei aufgrund der damals erhaltenen Informationen nicht angezeigt gewesen bzw. sei ein «überzogener Anspruch» an eine Aufsichtskommission des Kantonsrates. Dennoch müsse die GPK ihre Arbeit sauber erledigen, auch in den Referentengesprächen.[765]

In der Sitzung der GPK vom 8. Dezember 2022 räumte die Direktionsvorsteherin ein, dass es ein Fehler gewesen sei, dass die GPK den Bericht der Administrativuntersuchung nicht direkt nach dessen Abschluss erhalten habe, und entschuldigte sich dafür. Ebenso sagte sie gegenüber der PUK Datensicherheit, dass in diesem ganzen Geschäft «auf eine Art wie der Wurm drin war». Es sei «schief gegangen, was schief gehen konnte», und vermutlich habe sie, angesichts der Erleichterung darüber, dass keine Sofortmassnahmen notwendig waren, die Sache «sogar ein bisschen verdrängt».[766] Zur ausgebliebenen Information des Regierungsrates über die Administrativuntersuchung liess sie ergänzend verlauten, dass Administrativuntersuchungen nie anderen Direktionen zur Verfügung gestellt würden, sofern diese nicht betroffen seien.[767]

---

[763] Protokoll der Befragung von Mathias Eberli vom 26. Januar 2025, S. 8–10.

[764] Protokoll der Befragung von Beat Habegger vom 27. September 2024, S. 8–9, 10, 16–17.

[765] Protokoll der Befragung von Beat Habegger vom 27. September 2024, S. 19.

[766] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 37.

[767] Protokoll der GPK-Sitzung vom 8. Dezember 2022.

13.10 Missverständnis zwischen der Direktion der Justiz und des Innern (JI) und der Datenschutzbehörde bezüglich der Information der Öffentlichkeit

Im Rahmen des Point de Presse vom 6. Dezember 2022 hatte Jacqueline Fehr bezüglich einer Information der Öffentlichkeit zum Datenschutzvorfall ausgeführt, dass sie aufgrund der Stellungnahme der Datenschutzbeauftragten auf eine Veröffentlichung des Vorfalls verzichtet habe.[768]

Die Datenschutzbeauftragte erklärte gegenüber der PUK Datensicherheit in diesem Zusammenhang, nicht vorab über den Point de Presse informiert worden zu sein. Sie habe diesen online mitverfolgt und festgestellt, welch prominente Rolle sie in den Ausführungen eingenommen habe. In der Folge sei sie von der Zeitung «Blick» angefragt worden, ob sie auf die von Jacqueline Fehr gemachten Aussagen reagieren wolle.[769] Am 7. Dezember 2022 erschien ein Artikel im «Blick», worin sie angab, sich in ihrer Stellungnahme einzig zum Aspekt der Information der betroffenen Personen geäussert zu haben. Zur Publikation des Schlussberichts der Administrativuntersuchung habe sie keine Aussage gemacht.[770] Das erklärte sie dann auch im Rahmen der Sitzung der GPK-Subkommission vom 26. Januar 2023, wo sie den zeitlichen Ablauf der Geschehnisse und ihre Stellungnahme rund um den Datenschutzvorfall aufzeigte.[771]

Gegenüber der PUK Datensicherheit räumten sowohl die Datenschutzbeauftragte als auch die Direktionsvorsteherin ein, dass es sich hier um ein Missverständnis gehandelt habe, welches zwischen ihnen unterdessen geklärt worden sei.[772] Anlässlich eines Gesprächs im Januar 2023 zwischen der Datenschutzbeauftragten und der JI, in welchem es um die Umsetzung der Massnahmen aus der Stellungnahme der Datenschutzbeauftragten ging, habe die Direktionsvorsteherin der JI dann ausgeführt, dass die Thematik grundlegender aufgenommen werden soll. Die Datenschutzbeauftragte habe festgestellt, dass die Massnahmen bis dahin nicht in der gewünschten Form umgesetzt worden waren. Sie habe jedoch die Stossrichtung der JI begrüsst. Man habe sich dann darauf geeinigt, dass die Datenschutzbeauftragte quartalsweise einen Bericht über den Stand der Umsetzung erhalte, was in der Folge auch geschah.[773]

13.11 Ausbleibende Information an die Finanzkontrolle

Die JI teilte in ihrer Medienmitteilung vom 2. Dezember 2022 mit, dass die Finanzkontrolle von ihr unmittelbar nach Bekanntwerden des Datensicherheitsvorfalls über den Verdacht und die Administrativuntersuchung informiert worden sei.[774]

Der Leiter der Finanzkontrolle, Martin Billeter, und sein Stellvertreter, Daniel Strebel, führten im Rahmen der Befragung durch die PUK Datensicherheit aus, erst über die Medien auf den Datensicherheitsvorfall aufmerksam geworden zu sein, auch wenn dies teilweise anders berichtet wurde.[775] Aus dem E-Mail-Verkehr vom 4. und 5. Dezem-

---

[768] Direktion der Justiz und des Innern, Point de Presse vom 6. Dezember 2022 «Konsequenzen aus dem Datensicherheitsvorfall bei der Direktion JI».

[769] Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 8–10.

[770] Artikel der Zeitung Blick «Jacqueline Fehr redet endlich – die Datenschützerin widerspricht» vom 7. Dezember 2022.

[771] Protokoll der GPK-Subkommission Datenmissbrauchsvorfall vom 26. Januar 2023.

[772] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 42; Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 10.

[773] Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 7.

[774] Direktion der Justiz und des Innern, Medienmitteilung vom 2. Dezember 2022 «Datensicherheitsvorfall bei der Direktion JI in den Jahren 2006 bis 2012».

[775] Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 24.

ber 2022 zwischen der Direktionsvorsteherin und dem Leiter der Finanzkontrolle geht hervor, dass Jacqueline Fehr, da sie die entsprechende E-Mail nicht finden konnte, dann auch nicht mehr sicher war, ob sie die Finanzkontrolle wirklich über den Datensicherheitsvorfall informiert hatte, wie sie dies an verschiedenen Orten kundgetan hatte.[776] Daraufhin teilte ihr Martin Billeter mit, dass die Finanzkontrolle bis zu den Medienberichten keine Kenntnis von der genannten Angelegenheit gehabt habe. Weder die Direktionsvorsteherin noch die Generalsekretärin hätten die Finanzkontrolle informiert.[777]

13.12 Umfassende Information des Gesamtregierungsrates

Nach Auskunft der Staatsschreiberin, Kathrin Arioli, informieren die Direktionsvorsteherinnen und Direktionsvorsteher jeweils zu Beginn der Regierungsratssitzungen mündlich über Sachverhalte, die für die gesamte Regierung relevant sein könnten. Dies sei angesichts der medialen Berichterstattung zum Datensicherheitsvorfall auch so gemacht worden.[778] Die Direktionsvorsteherin der JI gab ihrerseits an, den Gesamtregierungsrat an der folgenden ordentlichen Sitzung nach dem Point de Presse am 21. Dezember 2022 anlässlich der dringlichen Interpellation KR-Nr. 462/2022 umfassend über den Datensicherheitsvorfall informiert zu haben.[779]

Im Rahmen dieser Sitzung erhielten die Mitglieder des Regierungsrates neben dem Interpellationstext auch den Schlussbericht der Administrativuntersuchung, die Stellungnahme der Datenschutzbeauftragten, die JI-Timelines zum zeitlichen Ablauf und der technischen Entwicklung sowie das Protokoll des Gesprächs mit dem Leitenden Staatsanwalt der Staatsanwaltschaft Zürich-Sihl.[780] Sowohl an dieser Sitzung als auch danach habe der Regierungsrat natürlich viel über diese Sache gesprochen.[781] Der Regierungsrat setzte an seiner Sitzung vom 21. Dezember 2022 auch einen thematischen Schwerpunkt auf die Informationssicherheit und das Strafverfahren und klärte dabei mit dem Leitenden Oberstaatsanwalt, ob eine ausserkantonale Staatsanwaltschaft mit den Abklärungen zum Datensicherheitsvorfall beauftragt werden sollte. Der damalige Oberstaatsanwalt führte dazu gegenüber der PUK Datensicherheit aus, dass der Regierungsrat solche Entscheide fälle, dass die Oberstaatsanwaltschaft jedoch stark im Prozess involviert gewesen sei. Er habe gespürt, dass der Regierungsrat die Untersuchung ausserkantonal geben wolle, habe aber dafür votiert, die Untersuchung durch den Kanton Zürich zu führen. Ausserkantonale Untersuchungen seien dann angezeigt, wenn Mitglieder des höheren Kaders von der Untersuchung betroffen sind. Das sei hier nicht der Fall gewesen. Aufgrund des Zeithorizonts der Untersuchung seien die Kadermitglieder nicht mehr bei der JI beschäftigt gewesen und es habe auch noch keinen hinreichenden Tatverdacht oder Tatverdächtige gegeben. Zudem besitze der Kanton Zürich die grösste Fachkompetenz in diesem Bereich. Wäre das Strafverfahren ausserkantonal gegeben worden, hätte die Verfahrensleitung vermutlich die Spezialisten des

---

776 E-Mail mit Betreff «Administrativuntersuchung AU» vom 4. Dezember 2022 von Jacqueline Fehr an Martin Billeter.

777 E-Mail mit Betreff «Administrativuntersuchung AU» vom 5. Dezember 2022 von Martin Billeter an Jacqueline Fehr.

778 Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 22.

779 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 39–40.

780 E-Mail von Kathrin Arioli vom 4. Dezember 2024, Anfrage: Unterlagen zu RR-Sitzungen.

781 Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 29.

Kantons Zürich für die Forensik beiziehen müssen.[782] Der Regierungsrat entschied in der Folge, dass es keinen Grund für eine ausserkantonale staatsanwaltschaftliche Untersuchung gebe.[783]

Aus den Befragungen der Regierungsrätinnen und Regierungsräte durch die PUK Datensicherheit geht hervor, dass für die meisten von ihnen ein früher Einblick in die Adminstrativuntersuchung nicht von Interesse war. Die Administrativuntersuchung wurde als interne Sache der JI gesehen, auch wenn einzelne angaben, dass die Ergebnisse auch für ihre Direktion von Interesse gewesen wären. Gemäss einer Aussage wäre dem Bericht zu einem früheren Zeitpunkt wohl kaum eine grosse Aufmerksamkeit zugekommen, da die Tragweite des Vorfalls erst durch die mediale Thematisierung Anfang Dezember 2022 entstanden sei.[784] Andere wiesen darauf hin, dass ab dem Zeitpunkt, als es Hinweise gegeben habe, dass auch andere Direktionen betroffen sein könnten, bzw. eine Aussenwirkung entstanden sei, eine Information gut gewesen wäre.[785] Gerade mit Blick auf die Abklärungen, die der Direktionsvorsteher, Mario Fehr, im Fall der Sicherheitsdirektion, die medial ebenfalls im Fokus stand, durchführen liess, wäre es hilfreich gewesen, wenn die Information frühzeitig vorhanden gewesen wäre.[786]

13.13 Massnahmen der Direktion der Justiz und des Innern (JI)

Von den insgesamt 13 Empfehlungen der Administrativuntersuchung vom 30. März 2021 wiesen vier eine hohe Priorisierung auf: So sollten die Zugriffskonzepte aktualisiert, spezifische Vorgaben zu Verträgen mit externen Dienstleistern erstellt, direktionsweite Vorgaben zu Sicherheitsprüfungen erlassen und die Umsetzung des IDG in der Direktion systematisch angegangen werden.[787]

13.13.1 Verzögerte Umsetzung der Empfehlungen der Administrativuntersuchung

Nach Ansicht der Direktionsvorsteherin, Jacqueline Fehr, fiel aufgrund der IKT-Organisation die Umsetzung mancher der insgesamt 13 Empfehlungen auch in die Zuständigkeit des kantonalen Informationssicherheitsbeauftragten (ISIK).[788] Das Generalsekretariat der JI ging in der Folge gemeinsam mit dem ISIK und der Digital Solutions, der JI-Informatik, durch die verschiedenen Empfehlungen und Massnahmen und entschied, was auf der kantonalen und was auf der direktionalen Ebene anzugehen sei.[789] Der PUK Datensicherheit liegt ein Dokument vor, das diese im April 2021 vorgenommene Zuteilung klärt.[790] Beispielsweise war bei der Aktualisierung der Informatikstrategie der JI die neue kantonale Informationssicherheitsstrategie zu berücksichtigen. Weiter sollten die notwendigen Schulungen der Mitarbeitenden zur Informationssicherheit im Rahmen der neuen kantonalen Sicherheitskultur realisiert werden. Im Be-

---

[782] Protokoll der Befragung von Andreas Eckert vom 28. Februar 2025, S. 18–19.

[783] Protokoll der Kantonsratssitzung vom 9. Januar 2023, S. 32.

[784] Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 26; Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S. 19; Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 22.

[785] Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 16.

[786] Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 26.

[787] IT & Law Consulting GmbH, Administrativuntersuchung bei der Direktion der Justiz und des Innern des Kantons Zürich im Zusammenhang mit dem Umgang von Informationen und Datenmissbrauch, Schlussbericht vom 30. März 2021, S. 34–37.

[788] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 33–34.

[789] Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 22–23.

[790] Direktion der Justiz und des Innern, Schlussbericht Befunde (Tabelle).

reich des Vertragswesens sollten sich die Vorgaben der JI, die noch zu erarbeiten waren, auf erweiterte kantonale Allgemeine Geschäftsbedingungen (AGB) stützen können. Das Zentrum für Cybersicherheit befasste sich 2024 mit Vertragsbausteinen für die Cloud-Nutzung. Im Rahmen dieser Diskussionen kam die Fachgruppe Informationssicherheit (FAGIS) zum Schluss, dass standardisierte Vertragsbausteine für alle Beschaffungen zu erarbeiten seien. Die bisherige Praxis mit drei AGB, die individuell ergänzt worden waren, sollte verbessert werden. So sollte es beispielsweise möglich sein, mit standardisierten Erweiterungen ein Audit-Recht oder die Form der Datenvernichtung nach Vertragsende vorzuschreiben oder Vorgaben an Subunternehmen weiterzureichen.[791]

Die Datenschutzbeauftragte, Dominika Blonski, forderte in ihrer Stellungnahme vom 15. September 2021, die hoch priorisierten Empfehlungen umzusetzen, und liess der Direktion Zeit für die Realisierung.[792] Basierend auf den kantonalen Vorgaben der BISR 5, 6 und 22,[793] erarbeitete die JI einen für alle Organisationen und Fachstellen verbindlichen Sicherheitsüberprüfungsprozess und setzte so eine Empfehlung um.[794] Nach Ablauf der Jahresfrist erkundigte sich die Datenschutzbeauftragte am 13. Oktober 2022 zum aktuellen Stand und bat um einen Zwischenbericht per Ende November 2022.[795] Am 28. November 2022 wurde sie durch die JI schliesslich informiert, dass man die Thematik grundlegender angehen wolle.[796] Die Datenschutzbeauftragte erklärte gegenüber der PUK Datensicherheit, sie habe festgestellt, dass zu jenem Zeitpunkt die Massnahmen noch nicht in der vorgesehenen Form umgesetzt worden waren. Von den als hoch prioritär bezeichneten Empfehlungen war zwar die Frage der Sicherheitsüberprüfungen angegangen worden, aber die Zugriffskonzepte waren damals noch nicht vorhanden. Zu jenem Zeitpunkt waren auch die organisatorischen Massnahmen zur verbesserten Umsetzung des IDG in der Direktion noch nicht weit fortgeschritten. Die nicht als prioritär bezeichnete Empfehlung, die JI-Informatikstrategie zu erneuern, war gemäss Aussage der Generalsekretärin, Jacqueline Romer, noch im November 2024 hängig. Inzwischen konnte das Gremium SDI die neue Informatikstrategie der JI als erste überabeitete direktionale Informatikstrategie abnehmen.[797]

Die Datenschutzbeauftragte betonte aber, dass sie die Absicht der JI, die Sache grundlegend angehen zu wollen, begrüsst habe.[798] Vonseiten der JI bestand der Wunsch, diese Fragen, in Ergänzung zur Administrativuntersuchung, strukturierter und systematischer über alle Organisationseinheiten der JI hinweg anzuschauen.[799]

---

791 Amt für Informatik, Kantonales Zentrum für Cybersicherheit, Präsentation «Vertragsbausteine der Informationssicherheit» vom April 2025 beim Legal Hub.

792 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 7.

793 Kanton Zürich, Steuerung Digitale Verwaltung und IKT, BISR 05 Personensicherheit vom 4. Mai 2021 und BISR 06 Richtlinie für Schulungsmassnahmen in Informationssicherheit vom 4. Mai 2021 sowie BISR 22 Richtlinie für Beziehungen zu externen Personen (insbesondere Liefernden) vom 4. Mai 2021.

794 Direktion der Justiz und des Innern, Generalsekretariat, DigiSol, Sicherheitsüberprüfungsprozess für Externe vom 3. Oktober 2022.

795 Datenschutzbeauftragte des Kantons Zürich, «Meldung der nicht fachgerechten Entsorgung von Rechnern und des potentiellen Datenmissbrauchs», Schreiben vom 13. Oktober 2022.

796 E-Mail «Zwischenbericht zur Umsetzung der Empfehlungen aus der Administrativuntersuchung bei der JI im Zusammenhang mit dem Umgang von Informationen und Datenmissbrauch» der stv. Generalsekretärin an die Datenschutzbeauftragte vom 28. November 2022.

797 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 12; Stellungnahme von Jacqueline Romer vom 7. November 2025.

798 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 7. Beispielsweise datiert das neue Zugriffskonzept der Abteilung Justizvollzug und Wiedereingliederung (JuWe) vom 28. Februar 2023.

799 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 22–23.

13.13.2 Umsetzung der Massnahmen aus dem KPMG-Bericht

Mit der öffentlichen und politischen Diskussion rund um den Datensicherheitsvorfall konfrontiert, wollte die Direktionsvorsteherin, Jacqueline Fehr, nach eigenen Angaben das Problem nun wirklich gründlich angehen und lösen und im Bereich des Datenschutzes und der Informationssicherheit eine Vorbildrolle einnehmen können.[800] Deshalb gab sie bei der Beratungsfirma KPMG, die mit der Funktionsweise der Verwaltung vertraut war, einen Bericht in Auftrag. Gemäss dem Vorwort des Berichts wollte sie mit der gründlichen Analyse sicherstellen, dass aus den Erfahrungen mit dem Datenvorfall die richtigen Schlüsse gezogen werden, und wissen, wo die Direktion insgesamt punkto Datenschutz und Informationssicherheit steht.[801] Von Mai bis Juli 2023 wurde in allen Organisationen der JI eine Erhebung zum Stand des Datenschutzes und der Informationssicherheit gemacht. Ziel war es, darauf basierend ein für die Direktion möglichst einheitliches Datenschutz- und Informationssicherheits-Regelwerk zu etablieren.

Im Bereich Verantwortlichkeit und Organisation stellte die KPMG fest, dass die JI durch eine Anpassung der Organisationsverordnung per Juli 2023 in allen Organisationseinheiten Verantwortliche für Datenschutz und Informationssicherheit ernannt hatte.[802] Als Folge des KPMG-Berichts schuf das Generalsekretariat per 1. Juli 2024 ein Kompetenzzentrum Business Support und Compliance (BSC), das allen Organisationseinheiten als Anlaufstelle dienen und die Umsetzung des Aktionsplanes vorantreiben sollte.[803] Im KPMG-Bericht stand weiter, dass keine direktionsweite Policy bestehe, die sämtliche relevanten Grundlagen zum Thema Datenschutz und Informationssicherheit enthalte. Gemäss dem Bericht besteht in der JI kein direktionsweites Risikomanagement in Bezug auf Datenschutz und Informationssicherheit. Im Informatikbereich sei ein Register für Risiken der Informationssicherheit erst im Aufbau. Weiter gab es laut Bericht in den Organisationseinheiten kaum Audits mit Fokus auf Datenschutz und Informationssicherheit. Schliesslich war im Bericht auch festgehalten, dass in der Direktion keine regelmässigen Datenschutz- und Informationssicherheitsschulungen für alle Mitarbeitenden stattfänden.[804] Auch gegenüber der PUK Datensicherheit gab die Generalsekretärin an, es fänden keine flächendeckenden Schulungen statt. Sie halte hier jedoch eine übergreifende Herangehensweise, die bei der gesamten Verwaltung ansetze, für zielführender.[805]

Diese Feststellungen des KPMG-Berichts sind erstaunlich; dies insbesondere mit Blick auf die Informatiksicherheitsverordnung vom 17. Dezember 1997, die schon damals u. a. festgehalten hatte, dass man Mitarbeitende über Sicherheitsmassnahmen informieren, diese beachten und für die notwendige Ausbildung sorgen müsse und dass auch die eigenen Sicherheitsmassnahmen periodisch durch unabhängige interne oder externe Stellen überprüft werden sollten. Vor diesem Hintergrund bezeichnete es der ehemalige Datenschutzbeauftragte, Bruno Baeriswyl, gegenüber der PUK Datensicherheit

---

[800] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 34, 43.

[801] Direktion der Justiz und des Innern, Generalsekretariat, Datenschutz und Informationssicherheit in der Direktion der Justiz und des Innern. Bericht und Aktionsplan vom 19. Dezember 2023.

[802] Direktion der Justiz und des Innern, Generalsekretariat, Datenschutz und Informationssicherheit in der Direktion der Justiz und des Innern. Bericht und Aktionsplan vom 19. Dezember 2023, S. 11–13.

[803] Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 10; Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 17.

[804] Direktion der Justiz und des Innern, Generalsekretariat, Datenschutz und Informationssicherheit in der Direktion der Justiz und des Innern. Bericht und Aktionsplan vom 19. Dezember 2023, S. 11–13, 16–18, 22–23, 32–33.

[805] Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 11.

«als Armutszeugnis», dass 2023 noch solche Feststellungen gemacht wurden. In seinen Augen sollten die vorgeschlagenen Massnahmen seit mindestens zehn Jahren selbstverständlich sein.[806]

13.13.3 Aufbau der Abteilung Business Support & Compliance

Gemäss der Leiterin des Kompetenzzentrums Business Support und Compliance (BSC), Susanna Stähelin, die ihre Tätigkeit am 1. Juli 2024 aufgenommen hatte, wurde auf der Management-Ebene erkannt, dass man das Thema des Datenschutzes und der Informationssicherheit organisatorisch fassen und klare Zuständigkeiten bestimmen musste. Nach Auskunft der Direktionsvorsteherin liegt die Zuständigkeit für die Informationssicherheit nun bei der Leiterin BSC, die mit den einzelnen Zuständigen der Amtsstellen in Verbindung steht.[807]

Das Kompetenzzentrum Business Support und Compliance hat eine beratende Rolle und keine Weisungsmöglichkeiten. Die aktuelle Leiterin geniesst laut eigenen Angaben eine starke Unterstützung und auch bei den Organisationseinheiten «ziehe man mit».[808] Sie habe aus Governance-Überlegungen den Informationssicherheitsbeauftragten der Direktion (ISID) aus der Informatik herausgelöst und im Kompetenzzentrum Business Support und Compliance (BSC) verortet. Bei den vertraglichen Grundlagen sowie der Sicherheitsüberprüfung habe das Kompetenzzentrum bereits Veränderungen bewirkt.[809] Manche Empfehlungen aus der Administrativuntersuchung befinden sich aber immer noch in der Umsetzung. So war beispielsweise die Überarbeitung der IKT-Strategie der JI im November 2024 noch nicht abgeschlossen.[810]

Die JI sah sich nach dem Datensicherheitsvorfall in der Pflicht, im Bereich der Informationssicherheit voranzugehen und eine Vorreiterrolle einzunehmen. Sie wollte etwa auch für die anderen Direktionen und die Staatskanzlei herausfinden, wie man diese Problematik am besten löse. Der Bericht wurde folglich im Regierungsrat und in der Generalsekretärenkonferenz traktandiert. Zudem informiert die Leiterin des BSC nach Aussagen der Direktionsvorsteherin und der Generalsekretärin regelmässig in Fachgremien über den diesbezüglichen Stand.[811]

Die JI machte den KPMG-Bericht zeitnah, am 3. Januar 2024, dem Regierungsrat zugänglich und dieser nahm in der Sitzung vom 10. Januar 2024 davon Kenntnis. Die Generalsekretärenkonferenz erhielt den Bericht am 10. Januar 2024 zugestellt und nahm davon in der Sitzung vom 20. Januar 2024 Kenntnis. Die IKT-Subkommission, die Geschäftsprüfungs- und die Finanzkommission des Kantonsrates wurden am 11. Januar 2024 über den Bericht informiert.[812] Die PUK Datensicherheit erhielt diesen Bericht anfänglich nicht. Nach einem schriftlichen Hinweis der GPK vom 19. Januar 2024 ging der Bericht bei der GPK am 22. Januar 2024 erneut ein – mit dem Hinweis, den Bericht an die PUK Datensicherheit weiterzugeben.

Im Rahmen der Befragung durch die PUK Datensicherheit entschuldigte sich die Direktionsvorsteherin dafür, den Bericht nicht auch der PUK Datensicherheit zugestellt zu haben, und beteuerte, dass dies nicht absichtlich geschehen sei. Der Zeitpunkt

---

806 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 12.

807 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 9.

808 Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 16–18.

809 Protokoll der Befragung von Susanna Stähelin vom 30. August 2024, S. 14.

810 Protokoll der Befragung von Urs Kaderli vom 1. November 2024, S. 12.

811 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 43–44; Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 14.

812 Direktion der Justiz und des Innern, Generalsekretariat, Memo betreffend Kommunikation KPMG – Bericht vom 21. Dezember 2023.

der Einsetzung sowie die Zuständigkeit der PUK Datensicherheit seien ihr nicht bekannt gewesen. Gemäss Memo zur Kommunikation sollte der Bericht an geeigneter Stelle ohne Begleitkommunikation auf die Webseite gestellt werden. Vier Tage nachdem die PUK Datensicherheit den Bericht am 22. Januar 2024 ebenfalls erhalten hatte, publizierte die Direktionsvorsteherin den Bericht auch auf ihrem persönlichen Blog. In ihren Augen war diese Publikationsform passend, da auch sie persönlich im Zentrum der politischen Auseinandersetzung gestanden habe und auf diese Weise für den Bericht auch etwas mehr Öffentlichkeit schaffen konnte.[813] Später wurde der Bericht vom Blog entfernt und auf der Webseite der JI aufgeschaltet.

13.13.4 Reaktion auf den Bericht in den anderen Direktionen und der Staatskanzlei

Der Eindruck, dass die JI mit dieser Untersuchung zu Datenschutz und Informationssicherheit auch für die anderen Direktionen voranging, liess sich im Rahmen der Befragungen der Regierungsmitglieder nicht bestätigen. So konnten sich nicht alle Regierungsmitglieder inhaltlich an den Bericht erinnern. Andere gaben an, dieser Bericht sei in ihrer Direktion respektive der Staatskanzlei mit Interesse studiert und Rückschlüsse für die eigene Organisation gezogen worden.[814]

13.14 Abklärungen in den anderen Direktionen

Für die PUK Datensicherheit war es eine zentrale Frage, wie die anderen Regierungsrätinnen und Regierungsräte auf den Datensicherheitsvorfall reagierten und welche Abklärungen sie tätigen liessen. Die Kommission stellte fest, dass sich Intensität und Tiefe der Abklärungen in den Direktionen und der Staatskanzlei wesentlich unterschieden. Die Aussagen werden nachfolgend zusammengefasst wiedergegeben.

– Die Staatsschreiberin, Kathrin Arioli, betonte, ihr sei sofort bestätigt worden, dass ein solcher Vorfall in der Staatskanzlei nicht passieren könne. Weiter habe sie sich nach Informationen zur früheren Entsorgung von Computern erkundigt. Da der Vorfall etwa 15 Jahre zurücklag, habe es in der Staatskanzlei niemanden mehr gegeben, der schon damals dort tätig war. Überdies seien angesichts der üblichen zehnjährigen Aufbewahrungsfrist keine Unterlagen mehr vorhanden gewesen. Inwieweit auch Unterlagen des Staatsarchivs hierzu untersucht wurden, entzieht sich der Kenntnis der PUK Datensicherheit. Die weiteren Abklärungen der Staatskanzlei brachten schliesslich zutage, dass ab 2010 eine Leistungsvereinbarung mit der Baudirektion für die Entsorgung der Geräte bestanden hatte.[815]
– Der Sicherheitsdirektor, Mario Fehr, hielt gegenüber der PUK Datensicherheit fest, dass er unmittelbar nach Bekanntwerden des Datensicherheitsvorfalls in der Sicherheitsdirektion eine Analyse in Auftrag gegeben habe. Für den Entsorgungsprozess über einen Dienstleister, der vom Generalsekretariat, vom Amt für Militär und Zivilschutz, vom Sozialamt und vom Sportamt gemeinsam genutzt wurde, liess man sich schriftliche Zertifikate geben. Die Vernichtung und Löschung in den übrigen Ämtern sowie die physische Zerstörung der Datenträger durch die KAPO habe man sich von den damals beteiligten Mitarbeitenden durch intensives Nachfragen

[813] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 44–45.

[814] Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 23; Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 26–27; Protokoll der Befragung von Carmen Walker Späh vom 13. Dezember 2024, S. 22; Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 17; Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 26; Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S. 20.

[815] Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 20–21.

bestätigen lassen. Des Weiteren sei auch die Herkunft der Daten, die mutmasslich aus dem Zuständigkeitsbereich der Sicherheitsdirektion stammten, geklärt worden: Bei den Akten der Kantonspolizei habe es sich um Akten gehandelt, die zur Staatsanwaltschaft übergegangen waren. Auch die Geräte der Statthalterämter, die teilweise noch mit Aufklebern der Sicherheitsdirektion versehen waren, seien damals bereits in der Zuständigkeit der JI gewesen. Der Sicherheitsdirektor gab an, tief zurückreichende, intensive Abklärungen getätigt zu haben.[816]

– Der Finanzdirektor, Ernst Stocker, gab der PUK Datensicherheit zu Protokoll, dass er sich, sobald er das erste Mal vom Datensicherheitsvorfall erfahren habe, bei den Verantwortlichen erkundigte, ob das auch in der Finanzdirektion passieren könne. Man habe ihm versichert, dies sei ausgeschlossen, da man über ein Entsorgungskonzept verfüge, welches die Prozesse klar festlege.[817]
– Die Volkswirtschaftsdirektorin, Carmen Walker Späh, erklärte der PUK Datensicherheit, sich beim Generalsekretär erkundigt zu haben, wie die Entsorgung innerhalb der Volkswirtschaftsdirektion abgelaufen sei. Der damit befasste IT-Leiter, der bereits vor ihrem Amtsantritt für die Volkswirtschaftsdirektion (VD) tätig gewesen sei, habe sehr viel Wert auf die Informationssicherheit gelegt und die Datenträger eigenständig zerstört. Da der Fall zeitlich weit zurücklag, war laut Aussagen der Direktionsvorsteherin das Bedürfnis der VD, die Geschichte aufzuarbeiten, nicht besonders gross. Sie habe sich jedoch versichern lassen, dass die VD aktuell gut aufgestellt sei.[818]
– Die Gesundheitsdirektorin, Natalie Rickli, gab der PUK Datensicherheit an, intern gefragt zu haben, wie die Gesundheitsdirektion aufgestellt sei und ob diese über den fraglichen Dienstleister Entsorgungen abgewickelt habe. Letzteres sei glücklicherweise nicht der Fall gewesen.[819]
– Der Baudirektor, Martin Neukom, sagte gegenüber der PUK Datensicherheit aus, er habe zeitnah abklären lassen, wie Entsorgungen in der Baudirektion (BD) abliefen. Er habe diesen Vorfall zum Anlass genommen, um zu prüfen, ob in der BD etwas Ähnliches hätte passieren können oder ob allenfalls etwas nicht gut laufe.[820] Der Statusbericht der BD zum Datenleck, der am 2. Februar 2023 in der Geschäftsleitung behandelt wurde und der PUK Datensicherheit vorliegt, beleuchtete u. a. die IT-Migrationen aus den Jahren 2004, 2010 und 2016, den Umgang mit Servern sowie den aktuellen Stand der Cyber-Security in der BD. Auf Basis dieser Informationen kam der Direktionsvorsteher zum Schluss, dass sich in der Baudirektion nichts Ähnliches zugetragen habe.
– Die Bildungsdirektorin, Silvia Steiner, gab an, bei Amtsantritt über den Ablauf der Entsorgungen in der Bildungsdirektion «ins Bild gesetzt worden» zu sein. Sie habe sich bereits damals – auch aufgrund ihrer beruflichen Vergangenheit als Staatsanwältin – über die Sicherheitskonzepte der Bildungsdirektion informieren lassen. Angesichts des Vorfalls habe sie nochmals nachgefragt, ob das auch in der Bildungsdirektion passieren könnte bzw. hätte passieren können. Sie habe überdies auch versucht, in Erfahrung zu bringen, ob ihre eigenen persönlichen Daten betroffen gewesen seien.[821]

---

816 Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 24–25.

817 Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 25.

818 Protokoll der Befragung von Carmen Walker Späh vom 13. Dezember 2024, S. 20–21.

819 Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 15.

820 Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S. 19.

821 Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 7, 24.

13.15 Einstellung des Strafverfahrens

Die Staatsanwaltschaft III führte ein umfangreiches Strafverfahren gegen Unbekannt durch. Sie stellte das Strafverfahren am 8. September 2025 aber ein, weil «allfällige tatbestandsmässige Handlungen sich trotz aufwendiger Ermittlungen weder innerhalb der Direktion noch ausserhalb einer bestimmten Person zurechnen [liessen]. Teilweise waren allfällige zu untersuchende Vorwürfe auch bereits verjährt».[822]

13.16 Würdigung durch die PUK

Ungenügende Kommunikation

Die PUK Datensicherheit stellt fest, dass die Direktionsvorsteherin, Jacqueline Fehr, und die Generalsekretärin der JI, Jacqueline Romer, umgehend erste Schritte einleiteten, nachdem sie vom Datensicherheitsvorfall erfahren hatten. Nach der Information ihrer engsten Mitarbeitenden entschieden sie sich, rasch eine Administrativuntersuchung einzuleiten. Die Meldung an die Datenschutzbeauftragte erfolgte später. Auf eine Information der GPK wurde vorerst verzichtet. Die GPK wurde dann aber über ihren JI-Referenten anlässlich des Frühjahrsgesprächs in Kenntnis gesetzt. Es reicht aus Sicht der PUK Datensicherheit nicht aus, eine Information dieser Tragweite ausschliesslich in einem solchen Rahmen zu platzieren. Die PUK Datensicherheit hätte erwartet, dass die Direktionsvorsteherin der JI die GPK von sich aus und aktiv über diese Sachverhalte informierte. Allgemein erachtet die PUK Datensicherheit eine formellere Information der GPK bei Vorfällen, die rasche Abklärungen bis hin zu einer Administrativuntersuchung auslösen, als notwendig.

Die PUK Datensicherheit erwartet deshalb, dass der Regierungsrat den Aufsichtskommissionen über die laufenden Administrativuntersuchungen in den Direktionen und der Staatskanzlei, die über personalrechtliche Abklärungen von geringer Tragweite hinausgehen, in geeigneter Form Bericht erstattet. Hierfür ist der Gesamtregierungsrat von den Direktionen und der Staatskanzlei über laufende Administrativuntersuchungen in Kenntnis zu setzen.

Weiter stellt die PUK Datensicherheit fest, dass auch die Kommunikation, insbesondere gegenüber den Behörden, nicht genügend funktionierte. Entgegen anderslautenden Äusserungen der Direktionsvorsteherin der JI blieb eine Information der Finanzkontrolle aus. Die Datenschutzbeauftragte musste sich ein zweites Mal zum Stand der Abklärungen erkundigen und erhielt den Bericht der Administrativuntersuchung erst einen Monat nach dessen Eingang bei der JI. Weiter erhielt auch der Leitende Oberstaatsanwalt, der Anfang November 2022 im Rahmen eines Kaderdialogs vom Bericht erfahren hatte, diesen erst im Dezember 2022. Die GPK wiederum erhielt den Administrativbericht erst im Rahmen des öffentlichen Bekanntwerdens des Vorfalls im Dezember 2022. Die PUK Datensicherheit anerkennt aber, dass die Direktionsvorsteherin diese Fehler rasch eingeräumt und sich entschuldigt hat.

Durch alle diese Defizite verzögerten sich nicht nur die Abklärungen der Staatsanwaltschaft III, sondern auch die Abklärungen der Datenschutzbeauftragten sowie allfällige weitere interne Abklärungen der anderen Direktionen. Rückblickend musste auch die Direktionsvorsteherin, Jacqueline Fehr, einräumen, dass im eigenen Verantwortungsbereich Fehler unterliefen, insbesondere im Hinblick auf die zeitgerechte Kommunikation. Für die PUK Datensicherheit ist es durchaus plausibel, dass sich die fehlende Kommunikation auch damit erklären lässt, dass die Thematik bei den verant-

[822] Oberstaatsanwaltschaft, Medienmitteilung vom 12. September 2025 «Datensicherheitsvorfall bei der Direktion JI: Staatsanwaltschaft stellt Verfahren ein».

wortlichen Personen der JI aus dem Fokus geriet, als die grösste Anspannung vorbei war und sich Erleichterung darüber einstellte, dass weder eine unmittelbare Gefahr bestand noch Sofortmassnahmen nötig waren. Das zeigt sich für die PUK Datensicherheit auch darin, dass die Nachverfolgung der Massnahmen aus der Administrativuntersuchung just dann wieder aufgenommen wurde, als das Thema durch die parlamentarische Anfrage an die Öffentlichkeit gelangt war. Generell kann die PUK Datensicherheit feststellen, dass schliesslich eine umfassende Information und Diskussion zur Frage der allgemeinen Informationssicherheit und zum Datensicherheitsvorfall stattgefunden hat.

Es zeigt sich, dass gerade im Umgang mit weiteren kantonalen Stellen, wie den Aufsichtskommissionen oder der Datenschutzbeauftragten, keine klar definierten Prozesse vorliegen. Die Kommunikation mit den Behörden und der Regierung sei, so der Kommunikationsbeauftragte der JI, Benjamin Tommer, Aufgabe der Direktionsleitung.[823] Die PUK Datensicherheit regt hier an, entsprechende Prozesse zu erarbeiten.

Die PUK Datensicherheit kritisiert auch die fehlende respektive verzögerte Kommunikation gegenüber dem Regierungsrat. Es scheint zwar so, dass sich die Regierungsmitglieder lediglich über Administrativuntersuchungen informieren, die auch andere Direktionen betreffen, und sich manche Regierungsmitglieder folglich nicht daran gestört haben. Angesichts der Tatsache, dass Administrativuntersuchungen, die sich mit organisatorischen Mängeln befassen, relativ selten sind und wohl oft auch Erkenntnisse für die eigene Organisation mit sich bringen können, ist es aus Sicht der PUK Datensicherheit unabdingbar, dass die anderen Regierungsmitglieder jeweils auch davon erfahren. Nur so lässt sich feststellen, ob den Problemen systematische Ursachen zugrunde liegen. Es braucht eine formalisierte gegenseitige Information zu Administrativuntersuchungen in den Direktionen und der Staatskanzlei.

Verhaltene gemeinsame Reaktion des Regierungsrates

Die PUK Datensicherheit hat wenig Verständnis dafür, dass sich die befragten Regierungsmitglieder kaum für die Vorgänge in anderen Direktionen interessierten und mehrfach geäussert wurde, dass die einzelnen Regierungsmitglieder vornehmlich ihre Direktionen im Griff haben müssten. Für die PUK Datensicherheit ist die Vorstellung nicht angemessen, dass in einer Kollegialbehörde die Auffassung vorherrscht, dass Probleme möglichst innerhalb der eigenen Direktion zu lösen seien. Die PUK Datensicherheit kritisiert diesen extremen Fokus auf das eigene «Gärtchen» und den Umstand, dass die Direktionen und die Staatskanzlei bisweilen als einzelne Königreiche funktionieren und bei kleinsten Änderungen einen Machtverlust befürchten. Sie fordert hier mit Nachdruck eine intensivere Zusammenarbeit und gemeinsame Verantwortung.

Strafverfahren der Staatsanwaltschaft

Schliesslich hält die PUK Datensicherheit fest, dass die Frage, ob das Strafverfahren ausserkantonal geführt werden soll, im Rahmen der Regierungsratssitzung vom 21. Dezember 2022 diskutiert und geprüft wurde. In Abwägung der Interessen und in Kenntnis, dass der Leitende Oberstaatsanwalt an der Sitzung umfassend zu dieser Thematik informiert hatte, entschied der Regierungsrat in der Folge, den Fall nicht ausserkantonal zu geben. Für die PUK Datensicherheit ist dieser Entscheid auch vor dem Hintergrund, dass das Know-how für forensische Abklärungen wohl einzig bei der Kantonspolizei Zürich vorhanden ist, schlüssig und nachvollziehbar.

---

[823] Protokoll der Befragung von Benjamin Tommer vom 27. September 2024, S. 7, 19.

Die PUK Datensicherheit anerkennt die grossen Anstrengungen, welche die Staatsanwaltschaften unternommen haben, um diese Fragen im öffentlichen Interesse zu klären. Der Austausch und die Koordination mit der Oberstaatsanwaltschaft und der Staatsanwaltschaft waren sehr gut und zielführend. Die Vorarbeiten der Staatsanwaltschaft III und der Staatsanwaltschaft Zürich-Sihl waren eine wesentliche und äusserst wertvolle Grundlage für die Arbeit der PUK Datensicherheit. Dank gelungener Koordination konnte sie auf diesen Vorarbeiten aufbauen.

Anfrage KR-Nr. 456/2022

Die genauen Hintergründe der kantonsrätlichen Anfrage KR-Nr. 456/2022, die den Datensicherheitsvorfall publik machte, sind der PUK Datensicherheit nicht bekannt und waren gemäss ihrem Auftrag auch nicht Gegenstand der Abklärungen. Diese konzentrierten sich auf die Verantwortlichkeiten für den Datensicherheitsvorfall sowie auf die frühere und aktuelle kantonale Informationssicherheit. Die Rolle von Valentin Landmann, der gleichzeitig als Rechtsvertreter von Roland Gisler und Erstunterzeichner der Anfrage fungierte und den Datensicherheitsvorfall öffentlich machte, bleibt für die PUK Datensicherheit unklar und über weite Strecken nicht nachvollziehbar.

Massnahmen der JI im Rahmen der Umsetzung des KPMG-Berichts

Die PUK Datensicherheit begrüsst es, dass die JI mit einer eigenen vertieften Abklärung, dem zusätzlichen KPMG-Bericht, Transparenz über die aktuelle Situation im Bereich der Informationssicherheit und Datenschutz geschaffen und ihre Bemühungen in diesem Bereich wesentlich intensiviert hat. Gleichzeitig stellt die PUK Datensicherheit ernüchtert fest, dass gewisse Empfehlungen aus dem Bericht zur Administrativuntersuchung – beispielsweise die Aktualisierung der Zugriffskonzepte, der Entwurf spezifischer Vorgaben zu Verträgen mit externen Dienstleistern und die systematische Umsetzung des IDG in der Direktion – innert Jahresfrist noch nicht umgesetzt waren. Auch sind der PUK Datensicherheit keine eigenen Auditaktivitäten der Digital Solutions in den Organisationseinheiten der JI bekannt.

Es irritierte die PUK Datensicherheit, dass ihr der KPMG-Bericht ein halbes Jahr nach ihrer Einsetzung nicht ebenfalls zugestellt wurde. Die Direktionsvorsteherin gab als Begründung an, ihr sei der Zeitpunkt der Einsetzung und die Zuständigkeit der PUK Datensicherheit nicht bekannt gewesen. Dem ist entgegenzuhalten, dass der Direktionsvorsteherin mit Schreiben vom 2. November 2023[824] persönlich die Aufnahme der Untersuchungstätigkeiten der PUK Datensicherheit mitgeteilt worden war. Die PUK Datensicherheit bedankt sich für die Entschuldigung der Direktionsvorsteherin, kritisiert aber gleichzeitig das Vorgehen. Es gilt auch hier die Kommunikation gegenüber den Behörden deutlich zu verbessern.

Die PUK Datensicherheit erachtet hingegen die Absprache und Koordination der direktionalen Anstrengungen zur Umsetzung des KPMG-Berichts mit dem kantonalen Informationssicherheitsbeauftragten (ISIK) im Hinblick auf die laufenden kantonalen Entwicklungen als sehr sinnvoll. Auch die Bestrebungen des Generalsekretariats der JI, die eigenen Erkenntnisse im Rahmen der Generalsekretärenkonferenz zu teilen, sind im Sinne einer von der PUK Datensicherheit gewünschten gesamtheitlichen Herangehensweise.

---

[824] Schreiben der PUK Datensicherheit betreffend «Aktenzustellung» an Jacqueline Fehr vom 2. November 2023.

Ausbleibende koordinierte Herangehensweise

Insgesamt vermisst die PUK Datensicherheit jedoch eine gesamtkantonale Sicht. Sowohl der Schlussbericht der Administrativuntersuchung als auch der KPMG-Bericht enthalten aus Sicht der PUK Datensicherheit Schlussfolgerungen, die für den gesamten Kanton, alle Direktionen und die Staatskanzlei von Interesse sein müssten. Im Umgang mit den Feststellungen zeigt sich für die PUK Datensicherheit die fehlende direktionsübergreifende und gesamtkantonale Perspektive, denn es hat sich herausgestellt, dass der Regierungsrat nach den Feststellungen des KPMG-Berichts nicht als Gesamtgremium tätig wurde.

Es ist für die PUK Datensicherheit unerklärlich, dass jede Direktion und die Staatskanzlei für sich ihre Schlüsse daraus gezogen haben, ohne auf Regierungsebene gemeinsam die Frage anzugehen, wie Compliance im Bereich der Informationssicherheit und des Datenschutzes im gesamten Kanton erreicht werden könnte. Hier sieht die PUK Datensicherheit ganz klar den Regierungsrat als Kollegialbehörde in der Pflicht, die Umsetzung der Empfehlungen, beispielsweise im Bereich der vertraglichen Vorgaben, der Personensicherheitsprüfung oder des Risikomanagements, auf der kantonalen Ebene und einheitlich anzugehen.

Auch blieb eine Untersuchung aus, wie es in der gesamten kantonalen Verwaltung um den Datenschutz und die Informationssicherheit steht, ähnlich dem BDO-Bericht aus dem Jahr 2016 zur damaligen IT-Situation. Somit fehlt für die PUK Datensicherheit auch heute die Transparenz darüber, wie gut die vom Datensicherheitsvorfall nicht direkt betroffenen Direktionen und die Staatskanzlei im Bereich der Informationssicherheit tatsächlich aufgestellt sind.

Für die PUK Datensicherheit zeigen die Auskünfte, die sie von den anderen Direktionen und der Staatskanzlei zu den von ihnen getroffenen Massnahmen eingeholt hat, dass der Datensicherheitsvorfall von vielen Regierungsmitgliedern als ausschliessliches Problem der JI wahrgenommen wurde. Zwar sahen sich auch andere Direktionen veranlasst, Nachforschungen zur eigenen Entsorgungspraxis in der Vergangenheit anzustellen. Dennoch hat die PUK Datensicherheit den Eindruck erhalten, dass die anderen Direktionen und die Staatskanzlei kaum Interesse an der Thematik gezeigt haben. Man war vielmehr einfach froh, dass die eigene Direktion nicht von einem solchen Vorfall betroffen gewesen war. Hier bleibt aber festzuhalten, dass die organisatorischen Vorkehrungen in den anderen Direktionen in etwa jenen der JI entsprochen haben und sie damit nicht vor einem ähnlichen Vorfall gefeit gewesen wären.

14. Heutiges kantonales System der Informationssicherheit

14.1 Geltendes Regelwerk

14.1.1 Beitrag der IKT-Strategie zur Informationssicherheit

Die IKT-Strategie von 2018, auf der die aktuelle kantonale IKT-Organisation basiert, bewirkte auch Veränderungen im Bereich der Informationssicherheit. Im Rahmen der Strategie beschloss der Regierungsrat, die IKT-Sicherheit übergeordnet anzugehen (siehe dazu Kapitel 10.3.4). Mit dem RRB Nr. 625/2019 gab er das diesbezügliche Projekt «IKT-Sicherheit» frei, welches die Grundlagen für ein zeitgemässes Informationssicherheitsmanagement schaffen sollte und den Aufbau eines Security Operations Centers (SOC) zur Überwachung der IKT-Sicherheit und zur Steigerung der Widerstandsfähigkeit gegenüber Cyber-Angriffen umfasste. Hierzu und für den Aufbau einer Sicherheitsorganisation innerhalb des Amtes für Informatik (AFI) bewilligte der Regierungsrat vier zusätzliche Stellen. Mit dem gleichen Beschluss löste er auch die Projekte zu einem verwaltungsweit einheitlichen digitalen Arbeitsplatz (DAP), einem zentralisierten Identitäts- und Zugriffsmanagement (IAM) sowie einer einheitlichen Kommunikations- und Kollaborationslösung aus.[825]

Aus Sicht der Finanzkontrolle führten die Schaffung des AFI und der Aufbau von diesbezüglichen Zuständigkeiten innerhalb des AFI zu einer merklichen Verbesserung im Bereich der Informationssicherheit.[826]

14.1.2 Allgemeine Informationssicherheitsrichtlinie vom 3. September 2019 (AISR 1.0)

Vorgeschichte

Wie in Kapitel 10.2 ausgeführt, stiess die geringe Regelungstiefe der Verordnung über die Informationsverwaltung und -sicherheit (IVSV) im Bereich der Informationssicherheit beim ehemaligen Datenschutzbeauftragten, Bruno Baeriswyl, auf Kritik. Deshalb führte der Regierungsrat die Regelung mit der Allgemeinen Informationssicherheitsrichtlinie (AISR) für die kantonale Verwaltung genauer aus und setzte sie 2020 gemeinsam mit der Verordnung in Kraft.[827] Die AISR dient mit den Besonderen Informationssicherheitsrichtlinien (BISR) dazu, die Grundprinzipien der Vertraulichkeit, Verfügbarkeit und Integrität der Informationen zu gewährleisten.[828]

Im Rahmen des langwierigen Erarbeitungsprozesses der AISR legte der frühere Informatik-Sicherheitsbeauftragte (I-SiBe), Renzo Mühlebach, die einzelnen Entwicklungsstufen der Fachgruppe Informatiksicherheit (FAGIS) vor und holte dazu jeweils die Stellungnahmen der Datenschutzbehörde ein.[829] Neben der direktionalen Zuständigkeit für die Umsetzung des Gesetzes über die Information und den Datenschutz (IDG) waren diese Arbeiten gemäss der Direktionsvorsteherin der JI, Jacqueline Fehr, ein weiterer Impuls, der die Aufmerksamkeit für das Thema «Informationssicherheit» schärfte. Auch im Rahmen der Vorberatung der AISR durch das Gremium «Steuerung digitale Verwaltung und IKT» (SDI) wuchs das Bewusstsein für die diesbezüg-

[825] RRB Nr. 625/2019 vom 26. Juni 2019, Projekte im Programm zur Umsetzung der kantonalen IKT-Strategie (Freigabe, zusätzliche Ausgabe, Stellenplan).

[826] Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 12.

[827] RRB Nr. 795/2019 vom 3. September 2019, Allgemeine Informationssicherheitsrichtlinie (AISR) (Erlass).

[828] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 7.

[829] Protokoll der Befragung von Renzo Mühlebach vom 21. Juni 2024, S. 9.

lichen technischen, organisatorischen und kulturellen Dimensionen.[830] Das SDI diskutierte auf Basis der Vorarbeiten des Gremiums «Operative Informatiksteuerung» (OIS) auch die direktionsinterne Umsetzbarkeit.[831]

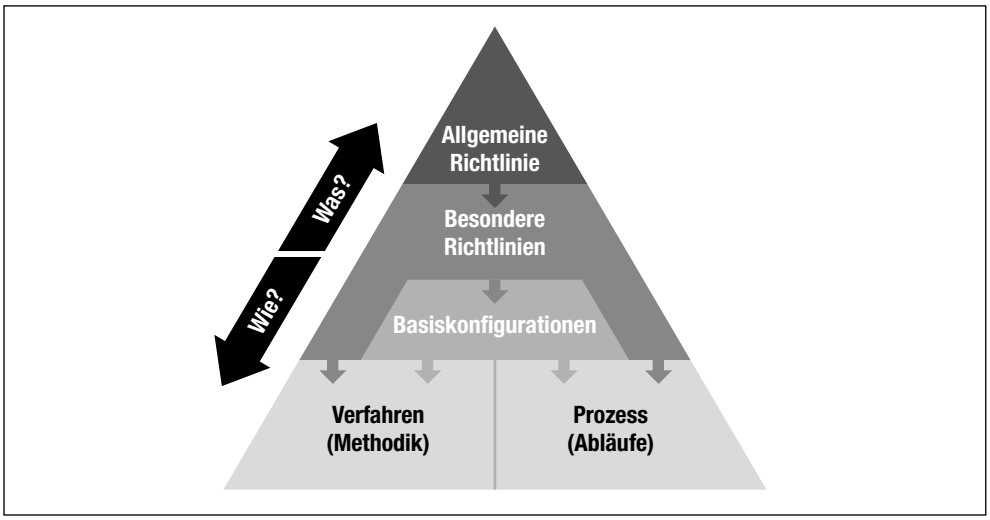
Wichtigster Gegenstand der AISR 1.0 war die IKT-Sicherheit. Obwohl es für die Umsetzung der Informationssicherheit die gesamte Organisation brauchte, nahm die AISR 1.0 vor allem die Informatikleiter in die Pflicht. In den Befragungen durch die PUK Datensicherheit gaben verschiedene Regierungsrätinnen und Regierungsräte an, mit dem RRB Nr. 795/2019 betreffend AISR die Informationssicherheit gefördert zu haben.

AISR als Spitze des kantonalen Informationssicherheits-Managementsystems (ISMS)

Die AISR legt die direktionsübergreifende Organisation fest und steht an der Spitze des kantonalen Regelwerks. Darunter folgen die Besonderen Informationssicherheitsrichtlinien (BISR), welche die kantonalen Regelungen für spezifische Bereiche enthalten. Schliesslich erstreckt sich das Regelwerk über die Basiskonfigurationen zu den konkret gelebten Prozessen, Normierungen und Aufzeichnungen in den Direktionen und der Staatskanzlei.[832]

Die AISR gilt, im Gegensatz zur früheren Informatiksicherheitsverordnung (ISV), nur für die Mitarbeitenden der kantonalen Verwaltung und führt die Vorgaben aus Gesetz und Verordnung (§ 7 IDG und § 12 IVSV) aus. Sie zeigt auf, wie das gesamtkantonale Regelwerk zur Umsetzung der Informationssicherheit – das Informationssicherheits-Managementsystem (ISMS) – aufgebaut ist (siehe Abbildung 7).[833] Mit der AISR legt der Regierungsrat den Rahmen fest und das Gremium SDI steuert mit den BISR die Schutzanforderungen für verschiedene Teilbereiche. Mit Basiskonfigurationen werden diese Anforderungen in der Informatik technisch umgesetzt.

Abbildung 7 Aufbau des Regelwerks gemäss AISR 1.0



Quelle: AISR des Regierungsrates für die kantonale Verwaltung vom 3. September 2019, S. 6.

830 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 8.

831 Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 12.

832 Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 16.

833 Ein ISMS ist gemäss ISO/IEC 27001:2022 die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit ganzheitlich, effektiv und nachhaltig zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Neben der gesamtkantonalen Organisation der Informationssicherheit bezeichnet die AISR auch die für die Erarbeitung der einzelnen BISR zuständigen Stellen und führt die Grundzüge dieser Regelungen, wie etwa Vorgaben zur Verschlüsselung, zum Umgang mit externen Personen oder Informationsrisiken, aus.[834]

Organisation der Informationssicherheit

- Der *Regierungsrat* trägt die Gesamtverantwortung für die Informationssicherheit in der kantonalen Verwaltung und nimmt Berichte des SDI zu AISR-Verbesserungen, aber auch zu Informationssicherheitsvorfällen, zum Notfallmanagement oder bewilligten Abweichungen von den BISR entgegen.
- Das Gremium *«Steuerung Digitale Verwaltung und IKT»* (SDI) berät die AISR vor und erlässt die BISR. Es befasst sich bei Bedarf mit Fragen, Entscheidungen und Regelungen zur direktionsübergreifenden Informationssicherheit. Letzteres geschieht im Auftrag des Regierungsrates oder auf Basis von Anträgen der SDI-Mitglieder oder der Fachgruppe IKT-Sicherheit (FAGIS). Das Gremium SDI nimmt die Berichte der Fachstellen entgegen und berichtet zusammenfassend an den Regierungsrat. Das SDI ist jedoch nicht ausschliesslich für die Informationssicherheit zuständig. Im Rahmen der IKT-Strategie und der Strategie «Digitale Verwaltung 2018–2023» kommen dem Gremium SDI weitere Aufgaben zu: Es steuert die Umsetzung dieser Strategien direktions- und fachübergreifend und wirkt für den Regierungsrat als vorberatendes Gremium.[835]
- Der *kantonale Informationssicherheitsbeauftragte*[836] (ISIK) fungiert gemäss der AISR 1.0 als zentrale Ansprechperson für alle Fragen der IKT-Sicherheit, koordiniert die diesbezüglichen Bestrebungen und leitet die Fachgruppe Informationssicherheit (FAGIS). Seine Kompetenzen in den spezifischen Feldern sind in der AISR und den BISR festgelegt. Namentlich ist er verpflichtet, über die bewilligten Ausnahmen und gemeldete Informationssicherheitsvorfälle zu informieren.
- Auf der Ebene der Direktionen oder der Staatskanzlei ist der jeweilige *Informationssicherheitsverantwortliche der Direktion (ISID)* für die Umsetzung zuständig. Er hat die Basiskonfigurationen festzulegen. Auf dieser Grundlage haben die *Informatik-Verantwortlichen der Direktion und der Staatskanzlei (IVAD)* wiederum die Verfahren und Prozesse im Bereich der IKT-Sicherheit festzulegen.
- Die *Fachgruppe Informationssicherheit (FAGIS)* bestand gemäss der AISR 1.0 aus dem ISIK und den acht ISID sowie einer Verbindungsperson der KAPO, die gemäss RRB Nr. 780/2017 nicht Teil der kantonalen IKT ist. Mit der AISR 2.0 vom 16. April 2025 nehmen nun zusätzlich eine Vertretung der Datenschutzbehörde sowie eine Verbindungsperson zur IKT-Grundversorgung Einsitz. Die FAGIS hat für eine ausreichende Regelungsdichte auf der Stufe der Gesamtverwaltung zu sorgen und koordiniert die Anliegen aus den verschiedenen Teilen der kantonalen Verwaltung.

Gemäss der Vorsteherin der JI, Jacqueline Fehr, ist die heutige Governance der Informationssicherheit klar: Der Regierungsrat sei für die AISR und damit für das Dispositiv der gesamtkantonalen Organisation verantwortlich. Die Hauptverantwortung für die Umsetzung der kantonalen Vorgaben in den einzelnen Direktionen und die Bereitstellung der dafür nötigen Ressourcen sieht sie aber bei den Direktionsvor-

---

[834] Allgemeine Informationssicherheitsrichtlinie des Regierungsrates für die kantonale Verwaltung vom 3. September 2019.

[835] Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 10; RRB Nr. 392/2018 vom 25. April 2018, Steuerung Digitale Verwaltung und kantonale IKT, Vertretungen und Konstituierung.

[836] Durch den engen Blick auf die IKT-Sicherheit werden in der AISR 1.0 noch die Begriffe IKT-Sicherheitsbeauftragte/r des Kantons Zürich und IKT-Sicherheitsbeauftragte/r der Direktion oder Staatskanzlei sowie die Fachgruppe IKT-Sicherheit erwähnt.

steherinnen und Direktionsvorstehern. Diese trügen technisch – sofern es nicht in den Bereich des AFI falle –, organisatorisch und kulturell die Verantwortung für die Informationssicherheit.[837] Mit Blick auf die Gesamtverantwortung des Regierungsrates führte die Staatsschreiberin, Kathrin Arioli, aus, dass der Regierungsrat auf Antrag der Finanzdirektion und nach Vorberatung durch das Gremium SDI über einen allfälligen AISR-Anpassungsbedarf berate. Grundsätzlich sei es aber jeder Direktion möglich, Antrag an den Regierungsrat zu stellen.[838]

Optimierungsbedarf bei der AISR 1.0

Obwohl sich bereits der erste kantonale Informatik-Sicherheitsbeauftragte (I-SiBe), Renzo Mühlebach, für ein breiteres Verständnis eingesetzt hatte (siehe Kapitel 10.1.2), ist in der AISR 1.0 explizit noch ausschliesslich von IKT-Sicherheit die Rede. Damit sind die organisatorischen Verantwortlichkeiten für die Informationssicherheit, die über die Informatik hinausgehen, ungenügend abgebildet. Für die Umsetzung der Informationssicherheit braucht es gemäss dem Informationssicherheitsbeauftragten (ISIK), Philipp Grabher, auch in den Direktionen und der Staatskanzlei Strukturen, die es erlauben, die gesamtkantonalen Prozesse darauf aufzubauen.[839]

- Dem Einkauf komme beispielsweise eine zentrale Rolle zu. Die Beschaffungsverantwortlichen würden die Lieferanten kennen, könnten diese hinsichtlich Informationssicherheit prüfen und eine Übersicht über die Lieferantenbeziehungen (Inventar) herstellen.
- Allgemein seien es die Direktionen und die Staatskanzlei selbst, die ihre Werte, die es zu schützen gilt, am besten kennen und erfassen können. Folglich müssten die Direktionen und die Staatskanzlei als gesamte Organisationen befähigt werden, die Informationssicherheit umsetzen zu können.
- Es seien also die Direktionsleitungen, welche die Voraussetzungen schaffen müssten, damit die Informationssicherheit in den Direktionen und Ämtern gelebt werden kann. Hierfür sollte die Informationssicherheit auch auf der Managementebene in der Direktion und dem Regierungsrat regelmässig Thema sein. Auch Fragen der richtigen Governance gehörten dazu, die im Informationssicherheitsbereich an Bedeutung gewonnen hätten und auch in internationale Standards einflössen.[840]

In Bezug auf die Organisation in der Direktion ist es gemäss dem Informationssicherheitsbeauftragten der Finanzdirektion zentral, dass die ISID nicht der Informatikleitung unterstellt sind. Denn in dieser Konstellation könnten die Interessen zur Aufrechterhaltung des Betriebs mit den Sicherheitsrisiken kollidieren.[841] Die Unterstützung durch die Leitungsfunktionen ist für den ISID der Finanzdirektion eine Bedingung für die erfolgreiche Umsetzung der Vorgaben.[842]

Alle genannten Aspekte sind in der AISR 1.0 aus dem Jahr 2019 nicht oder ungenügend enthalten. Diese bildet auch die neueren Entwicklungen rund um die Umsetzung der IKT-Strategie 2018 sowie die 2022 erlassene Cybersicherheitsstrategie nicht ab. Auch dazu, wie die Umsetzung der Informationssicherheit kontrolliert wird, hält sie wenig fest. Demgegenüber war in der früheren ISV der Prozess von der vorgängigen Risikoabschätzung über das Ergreifen von entsprechenden Massnahmen bis zur nachträglichen Kontrolle vorgezeichnet. Um eine Gesamtsicht der kantonalen Risikosituation

---

837 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 8.

838 Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 16.

839 Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 18.

840 Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 18.

841 Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 12.

842 Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 14.

zu haben und die Wirksamkeit beurteilen zu können, sind aus Sicht des ISIK direktionsübergreifende Audits nötig. Zusätzlich brauche es aber auch Kennzahlen, die das Risikomanagement, das heute in den Projekten über die Informationssicherheits- und Datenschutzkonzepte stattfindet, aggregieren. Vor diesem Hintergrund setzte der ISIK zusammen mit der FAGIS Anfang 2024 einen Prozess zur Erneuerung der AISR und der BISR in Gang.[843]

14.1.3 Umsetzung der IKT-Strategie

Als der heutige ISIK, Philipp Grabher, im März 2020 seine Stelle antrat, waren mit der IVSV und der AISR die neuen Grundlagen zwar bereit, die Informationssicherheitsorganisation bestand aber im Wesentlichen nur aus seiner Stelle. Im Juni 2020 setzte das Gremium SDI die ersten BISR fest, und mit dem Geschäftsorganisationskonzept, das im Rahmen des Projektes IKT-Sicherheit erarbeitet worden war, nahm auch die zukünftige Organisation der Informationssicherheit Form an. Mit RRB Nr. 1193/2020 bewilligte der Regierungsrat hierfür in den Direktionen und der Staatskanzlei sieben unbefristete ISID-Stellen und stellte zusätzliche Mittel für die Direktionen und die Staatskanzlei bereit.[844] Mit RRB Nr. 811/2021 richtete der Regierungsrat einen IT-Expertenpool Informationssicherheit ein, der die Direktionen und die Staatskanzlei mit Fachwissen unterstützen sollte.[845] Die Direktionen und die Staatskanzlei machten hiervon unterschiedlich Gebrauch. Obwohl damit die Möglichkeit bestanden habe, festgestellte Mängel zu beseitigen, seien diese Mittel nicht ausgeschöpft worden, gab der ISIK gegenüber der PUK Datensicherheit an.[846] In der Finanzdirektion sind sie aber beispielsweise genutzt worden, um die kritischen Schutzobjekte und deren Schutzbedarf in allen Ämtern zu identifizieren und eine Risikolandkarte aufzubauen.[847] In anderen Direktionen war man eher der Meinung, dass diese Ressourcen für den ISIK bereitstünden, und hat nichts abgeholt.[848]

14.1.4 Allgemeine Informationssicherheitsrichtlinie (AISR) vom 16. April 2025

Der Regierungsrat erliess die neue AISR am 16. April 2025 in Form einer verbindlich erklärten Richtlinie.[849] Eine stärkere rechtliche Verankerung fand nicht statt. Die AISR geht neu von einer gesamtheitlichen Betrachtung der Informationssicherheit aus und die Richtlinien (AISR und BISR) orientieren sich konsequent an der international anerkannten Normenreihe ISO/IEC 27000.

Gemeinsame kantonale Basis

Neu wird ein zweistufiger Governance-Ansatz gewählt, wonach zwischen einer gemeinsamen kantonalen Basis und der individuellen Umsetzung unterschieden wird. Die gemeinsame Basis umfasst neben der AISR und den BISR neu auch kantonal verpflichtende Informationssicherheitsstandards (ISST), welche angesichts besonderer Bedrohungslagen oder in stark verzahnten Themenfeldern die Umsetzung bestimmter BISR

---

843 Kanton Zürich, Finanzdirektion, Präsentation von Philipp Grabher «Vorgehen für die Überarbeitung der Informationssicherheitsrichtlinien» vom 22. Februar 2024.

844 RRB Nr. 1193/2020 vom 2. Dezember 2020, Informationssicherheit, Umsetzung in den Direktionen und der Staatskanzlei (Stellenpläne, gebundene Ausgabe).

845 RRB Nr. 811/2021 vom 14. Juli 2021, Rahmenverträge für Expertenpool Informationssicherheit (Vergabe).

846 Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 28.

847 Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 22.

848 Protokoll der Befragung von Roman Bolinger vom 15. März 2024, S. 16.

849 Allgemeine Informationssicherheitsrichtlinie des Regierungsrates für die kantonale Verwaltung vom 16. April 2025, Finanzdirektion, Faktenblatt Allgemeine Informationssicherheitsrichtlinie (AISR).

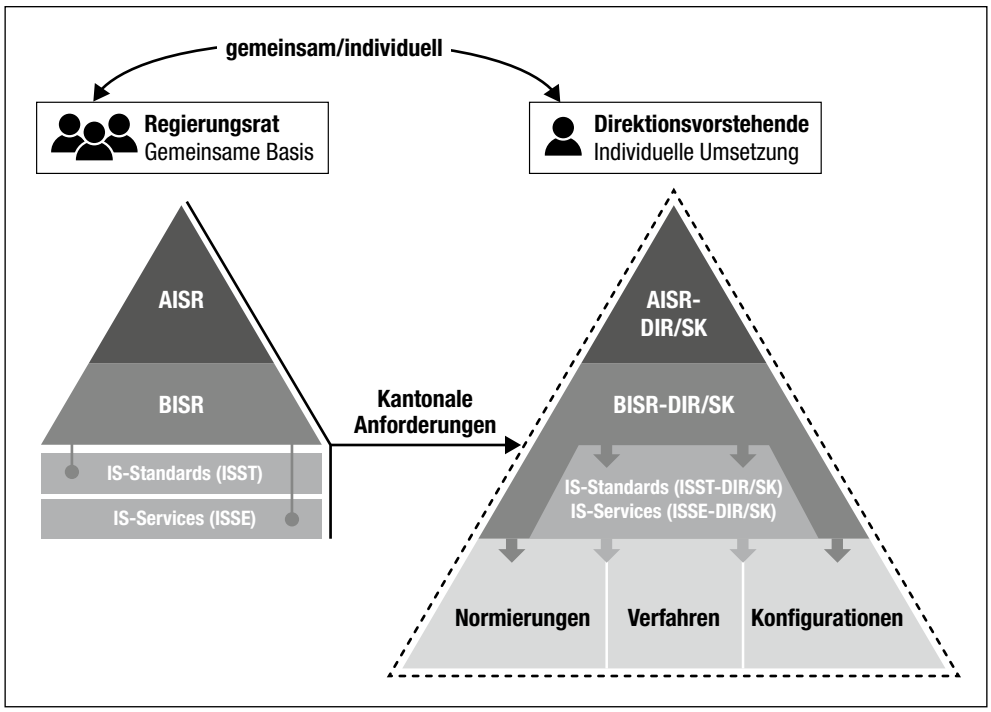
einheitlich und verbindlich regeln. Sie werden durch die Instanz erlassen, die für diesen BISR-Bereich zuständig ist,[850] und können durch die Direktionen und die Staatskanzlei nicht unterschritten werden. Weiter sind die gesamtkantonal bereitgestellten Informationssicherheitsservices (ISSE), also Dienstleistungen, die den Direktionen und der Staatskanzlei gesamtkantonal zur Verfügung gestellt werden, Teil der gemeinsamen Basis.

Verantwortung der Direktionen und der Staatskanzlei

Im RRB Nr. 438/2025 zum Neuerlass wird mit Verweis auf § 60 Abs. 1 lit. e der Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung (VOG RR)[851] die Verantwortung der Vorsteherinnen und Vorsteher der Direktionen und der Staatskanzlei für die Umsetzung der Informationssicherheit betont.

Folglich sind die Direktionen und die Staatskanzlei gemäss der neuen AISR, abgesehen von den Anforderungen der gemeinsamen Basis und unter Berücksichtigung der technischen Rahmenbedingungen, frei in der Ausgestaltung der operativen Umsetzung. Die Verantwortung der Direktionsleitung für die Informationssicherheit gemäss der neuen AISR zeigt sich nun beispielsweise explizit in der Verpflichtung, hierfür genügend Ressourcen bereitzustellen oder individuelle AISR der Direktionen und der Staatskanzlei (AISR-DIR/SK) zu erlassen. Die AISR-DIR/SK haben die Zuständigkeiten für das Regelwerk der Direktionen und der Staatskanzlei zu definieren (siehe Abbildung 8).

Abbildung 8 Aufbau des Regelwerks gemäss AISR 2.0



Quelle: AISR des Regierungsrates für die kantonale Verwaltung vom 16. April 2025, S. 9.

[850] Hier handelt es sich je nach Thema beispielsweise um das Zentrum für Cybersicherheit, das Personalamt oder das Immobilienamt.

[851] Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung vom 18. Juli 2007 (VOG RR; LS 172.11).

Wie dieses interne Regelwerk, das Informationssicherheits-Managementsystem (ISMS),[852] ausgestaltet wird, richtet sich jedoch nach dem Kontext der Direktionen und der Staatskanzlei. Es ist also möglich, dass dieses ISMS auf der Ebene der Ämter implementiert wird.

Diese Autonomie der Direktionen und der Staatskanzlei wirkt sich auch auf die Rolle der Informationssicherheitsbeauftragten der Direktionen und der Staatskanzlei (ISID) aus. Die Direktionsleitung definiert deren Aufgaben, Kompetenzen und Verantwortlichkeiten. Damit kann ein oder eine ISID weiterhin dem Informatikleiter unterstellt bleiben.

Überprüfung der Einhaltung

Bei der Überprüfung der Einhaltung der Zielvorgaben und der Berichterstattung brachte die neue AISR eine Stärkung. Das Gremium SDI legt neu Kennzahlen fest und die Direktionen und die Staatskanzlei haben sicherzustellen, dass diese erhoben und dem ISIK in der geforderten Form zur Verfügung gestellt werden.

Weiter ist intern, mindestens jährlich, risikobasiert mittels Stichproben zu überprüfen, ob die Vorgaben nach ISO-Norm eingehalten werden. Die Umsetzung der Informationssicherheit der gemeinsamen Basis wird ab 2027 alle vier Jahre nach ISO/IEC 27001 durch eine unabhängige Zertifizierungsstelle überprüft. Auch die Direktionen und die Staatskanzlei veranlassen gemäss AISR eine Überprüfung ihres ISMS. Schliesslich sind mit dem Regierungsrat und mit den jeweiligen Führungsorganen jährliche Steuerungsmeetings durchzuführen, in welchen der Stand der Informationssicherheit bewertet und Optimierungspotenzial diskutiert wird. Auf Basis dieser Steuerungsmeetings erstellt der ISIK zudem einen jährlichen Bericht, den das SDI dem Regierungsrat zur Kenntnis vorzulegen hat.

Ressourcen zur Umsetzung

Im Rahmen ihrer Befragungen erhielt die PUK Datensicherheit die Rückmeldung, dass für die Umsetzung der neuen AISR resp. BISR in den Direktionen und der Staatskanzlei auch zusätzliche Ressourcen notwendig seien. Sowohl die Vorsitzende des SDI, Kathrin Arioli, als auch Zuständige aus den Direktionen waren der Ansicht, dass man sich nicht zu etwas verpflichten solle, dass sich nicht einlösen lasse.[853] Der Regierungsrat schuf deshalb sieben auf zwei Jahre befristete Stellen, die mit Fachexpertinnen und -experten besetzt werden, welche die Umsetzung der Anforderungen der BISR sicherstellen sollen.[854]

14.1.5 Besondere Informationssicherheitsrichtlinien (BISR)

Die BISR[855] orientieren sich an der ISO/IEC-Norm 27002, welche Kontrollmechanismen für die Informationssicherheit beinhaltet. Die neue AISR weist alle Massnahmen der Norm den insgesamt 29 kantonalen BISR zu. Diese BSIR, von denen die meisten 2022 in Kraft traten, spezifizieren in den wichtigen Themenbereichen die Anforderungen. So befasst sich beispielsweise die BISR 6 mit Schulungen im Informationssicherheitsbereich, die BISR 8 mit der Handhabung von Speichermedien resp. deren Lö-

---

[852] Ein ISMS ist gemäss ISO/IEC 27001:2022 die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit ganzheitlich, effektiv und nachhaltig zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

[853] Protokoll der Befragung von Urs Kaderli vom 1. November 2024, S. 12, 28; Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 14, 28.

[854] RRB Nr. 438/2025 vom 16. April 2025, Allgemeine Informationssicherheitsrichtlinie (Neuerlass, Stellenpläne).

[855] Finanzdirektion, Faktenblatt Besondere Informationssicherheitsrichtlinien (BISR).

schung oder die BISR 22 mit den Beziehungen zu Lieferanten. Mit der Erneuerung der AISR wurde begonnen, auch die BISR zu überarbeiten. In den neuen BISR ist zusätzlich festgelegt, ob es sich um eine zwingende oder eine optionale Massnahme handelt und wer für die Umsetzung zuständig ist.[856]

Aus Sicht der Finanzkontrolle sind die BISR in den IT-Organisationen angekommen und bekannt. In der Umsetzung würden bei den Prüfungen jedoch immer wieder Lücken festgestellt.[857] Angesichts der Heterogenität der IT-Infrastruktur in den Direktionen und Ämtern lassen sich gemäss dem ISID der Finanzdirektion die zahlreichen Vorgaben nicht immer genau so, wie in der BISR vorgeschrieben, umsetzen. Ob die Mitarbeitenden die Ausnahmen, wie vorgesehen, beim ISID beantragen, sei fraglich.[858]

Konkretisierung der BISR in den Direktionen

Die Anforderungen der BISR in den verschiedenen Themenfeldern, konkret in den Verfahren und Prozessen zu berücksichtigen, ist Aufgabe der Direktionen und der Staatskanzlei. Wie sie dies regeln, hängt auch von ihrer spezifischen Infrastruktur sowie den personellen und finanziellen Ressourcen ab.[859]

Im Rahmen ihrer Abklärungen stellte die PUK Datensicherheit fest, dass hier Unterschiede bestehen. In der Finanzdirektion hat der ISID mit einem detaillierten Kontrollleitfaden konkretisiert, wie die allgemeinen Vorgaben der BISR in der Direktion umzusetzen sind. Der Leitfaden definiert für alle Aspekte konkrete Kontrollen und Nachweise.[860] Dieser Kontrollleitfaden ist auch in anderen Direktionen in Anwendung. Daneben gibt es aber auch Direktionen, die sich direkt auf die BISR abstützen.[861]

14.1.6 Kantonal verbindliche Leitfäden

Ergänzend zur AISR und zu den BISR gibt es auch weitere Nutzungsrichtlinien und Leitfäden, die sich an alle kantonalen Mitarbeitenden richten:
- Social Media Guidelines[862]
- Leitfaden Informationsklassifikation[863]
- Leitfaden Umgang mit Wechseldatenträgern[864]
- Allgemeine Nutzungsrichtlinie Microsoft 365 vom 1. Februar 2023[865]
- Merkblatt zur Nutzung von Online-KI-Generatoren vom 30. August 2023[866]
- Nutzungsrichtlinie Informationssicherheit[867]

Es lässt sich feststellen, dass die meisten dieser Leitfäden erst in jüngerer Zeit entstanden sind. So ist der Leitfaden zum Umgang mit Wechseldatenträgern vom 19. Dezember 2022 als Reaktion auf den Datensicherheitsvorfall zu sehen.

---

856 Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 21.

857 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 22.

858 Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 16, 18–19.

859 Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 29.

860 Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 17–19.

861 Protokoll der Befragung von Roman Bolinger vom 15. März 2024, S. 13.

862 Kanton Zürich, Social Media Guidelines, 2014.

863 Kanton Zürich, Leitfaden Informationsklassifikation, in Kraft seit 19. Dezember 2022.

864 Kanton Zürich, Leitfaden Umgang mit Wechseldatenträgern, in Kraft seit 19. Dezember 2022.

865 Kanton Zürich, Finanzdirektion, Amt für Informatik, Allgemeine Nutzungsrichtlinie Microsoft 365 vom 1. Februar 2023.

866 Staatskanzlei, Merkblatt zur Nutzung von Online-KI-Generatoren vom 30. August 2023.

867 Kanton Zürich, Nutzungsrichtlinie Informationssicherheit, in Kraft seit 29. Januar 2024.

14.1.7 Verbesserte Rahmenbedingungen durch die kantonale Cybersicherheitsstrategie

Angesichts wachsender Cyberrisiken, wie Cyberangriffen oder Cyberkriminalität, erliess der Regierungsrat, gestützt auf seine bisherigen Beschlüsse zur Informationssicherheit, eine Cybersicherheitsstrategie (heute Informationssicherheitsstrategie) und setzte sie auf den 1. Juli 2022 in Kraft.[868] Sie sieht in insgesamt neun Handlungsfeldern verschiedenste Massnahmen vor, wobei der Fokus in der ersten Phase auf folgenden vier Handlungsfeldern lag:

– Handlungsfeld 1: Bedrohungslage kennen
– Handlungsfeld 2: Verwaltung stärken
– Handlungsfeld 3: Umgang mit Vorfällen regeln
– Handlungsfeld 4: Betreiber kritischer Infrastrukturen sensibilisieren

Viele der Massnahmen im Handlungsfeld 2 zielen auf die Förderung der kantonalen Informationssicherheit. So schuf der Regierungsrat mit der Strategie eine Geschäftsstelle, eine Stelle für das kantonale Informationssicherheits-Risikomanagement sowie eine Stelle für die Sicherheits-Awareness. Diese Massnahmen haben die Informationssicherheit gestärkt und zentrale Schulungen und Awareness-Kampagnen sowie den Aufbau eines direktionsübergreifenden Risikomanagements ermöglicht. Letzteres soll gemäss dem ISIK künftig aufzeigen, wo auf den verschiedenen Ebenen (Regierungsrat, Direktion, Amt) Herausforderungen, Abweichungen und Verbesserungsbedarf bestehen.[869]

Organisatorisch fungiert der ISIK in seiner neuen Funktion als Cyber-Koordinator auch im Bereich der Cybersicherheit als zentrale Anlaufstelle und leitet das Kantonale Zentrum für Cybersicherheit (CCSC). Im neugeschaffenen Gremium Kerngruppe Cyber steht er als Mitglied u. a. mit den Leitungspersonen aus Strafverfolgung, Kantonspolizei und Kantonaler Führungsorganisation im Austausch.

Aus Sicht des Leiters der Digital Solutions der JI, Urs Kaderli, hat sich seit 2020 mit dem Aufbau des zentralen Programms zur Cybersicherheit auch das Bewusstsein für die Informationssicherheit verändert.[870] Die Direktionsvorsteherin der JI, Jacqueline Fehr, gab an, dass das Dispositiv der Cybersicherheit funktioniere und auch der Regierungsrat über die Cyberrisiken informiert werde.[871]

Mit der Umsetzung der Cybersicherheitsstrategie wird auch ein direktionsübergreifendes Angebot aufgebaut. Neben der Aktualisierung des Regelwerks geht es auf der Ebene der strategischen Cybersicherheit um das Risikomanagement, die Etablierung einer Sicherheitskultur, die kantonale Audittätigkeit (Assurance) und das Cyberkrisenmanagement. Gleichzeitig betreibt das CCSC im Bereich der operativen Cybersicherheit das Security Operations Center, das zentrale Identity und Access Management sowie die Public Key Infrastructure. Es hat eine Plattform für Bug-Bounty-Programme aufgebaut, welche helfen, Sicherheitslücken zu identifizieren.[872] Infolge des Fachkräftemangels konnten jedoch nicht alle bewilligten Stellen besetzt werden und die Umsetzung der Cybersicherheitsstrategie verzögert sich.[873] Gemäss der neuen AISR wird die

---

[868] RRB Nr. 676/2022 vom 4. Mai 2022, Cybersicherheitsstrategie (Festsetzung, Umsetzung, Stellenplan, Ausgabenbewilligung).

[869] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 18.

[870] Protokoll der Befragung von Urs Kaderli vom 1. November 2024, S. 8.

[871] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 24.

[872] Finanzdirektion, Amt für Informatik, Präsentation von Philipp Grabher, Stand Umsetzung Cybersicherheitsstrategie [z. H. SDI] vom 18. März 2024.

[873] Kanton Zürich Regierungsrat, Geschäftsbericht 2024, Teil II: Direktionen und Staatskanzlei, Leistungsgruppe 4620 IKT-Sicherheitsbeauftragter, S. 114–115.

Cybersicherheitsstrategie künftig als Informationssicherheitsstrategie weitergeführt. Der Regierungsrat verabschiedet diese Strategie neu alle vier Jahre und erteilt den Auftrag für ein kantonales Informationssicherheitsprogramm.

14.1.8 Von der IKT-Strategie zur IKT-Verordnung

Die IKT-Strategie umfasst mit dem Dreischichtenmodell wesentliche Elemente der heutigen etablierten Ausgestaltung des kantonalen IKT-Betriebs. Bereits im RRB Nr. 383/2018 war vorgesehen, hierzu Rechtsgrundlagen zu prüfen. Es sollen deshalb bestehenden Strukturen in einer neuen IKT-Verordnung geregelt werden, welche die IKT-Strategie ablöst.[874] In Bezug auf die zentrale Infrastruktur der Grundversorgung und ihrer Services gibt es gemäss dem ISIK aktuell Unklarheiten und Diskussionen, wer über die diesbezügliche Steuerung und Mindeststandards mitentscheiden darf. Es seien hier zentrale Entscheide notwendig, da sonst allenfalls die ganze Verwaltung einem Risiko ausgesetzt sein könnte.[875] Für die direktionsübergreifenden Angebote sind aus seiner Sicht die Governance, Steuerung und Verantwortung festzulegen.[876] Gemäss dem Normkonzept zur neuen Verordnung soll die Zuständigkeit für die technischen Basiskonfigurationen der Grundversorgung und der Kantonsapplikationen, also die technischen Einzelheiten zur Einhaltung der BISR-Anforderungen, neu beim Amt für Informatik (AFI) liegen. Es soll die Weisungskompetenz für Sicherheitsvorgaben der Grundversorgung erhalten.[877]

Gemäss dem Finanzdirektor ist es nun Zeit für die Verordnung, welche die Datensicherheit und die Grundversorgung in den zentralen Rechenzentren regelt.[878]

14.1.9 Ausblick: Herausforderungen durch Cloud-Lösungen

Mit dem RRB Nr. 542/2022 hat der Regierungsrat im März 2022 den Einsatz von Cloud-Lösungen, namentlich Microsoft 365, zugelassen.[879] Im RRB hält er fest, dass Microsoft als US-amerikanisches Unternehmen dem CLOUD Act untersteht und folglich von den US-amerikanischen Strafverfolgungsbehörden zur Offenbarung von spezifischen Daten aufgefordert werden kann. Der Regierungsrat führt weiter aus, dass Microsoft das Risiko eines sogenannten «Lawful Access», also die Herausgabe von Daten, mit verschiedenen Kontrollmechanismen minimiert. Auf Basis einer Risikobeurteilung kommt er zum Schluss, dass es höchst unwahrscheinlich sei, dass «US-Behörden über Microsoft auf vom Kanton Zürich im Rahmen von M365 in der Cloud gespeicherte Daten ohne Einwilligung des Kantons zugreifen können und werden». Durch die Umsetzung der AISR und der BSIR sowie weiterer rechtlicher, organisatorischer oder technischer Sicherheitsmassnahmen würden auch die meisten Risiken im Zusammenhang mit M365 wirksam vermindert. Zusätzlich schuf der Regierungsrat mit dem RRB Nr. 542/2022 auch die Stelle eines/einer kantonalen Cloud-Sicherheitsbeauftragte/n.

---

874 Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 16; Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 12.

875 Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 13–14.

876 Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 26.

877 Finanzdirektion, Amt für Informatik, Normkonzept IKT-Verordnung Kanton Zürich, Entwurf vom 28. Februar 2024.

878 Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 18.

879 RRB Nr. 542/2022 vom 30. März 2022, Einsatz von Cloud-Lösungen in der kantonalen Verwaltung (Microsoft 365), Zulassung.

Dass bei der Auslagerung in die Cloud wesentliche Risiken bestehen, zeigen die Leitfäden, welche die Datenschutzbeauftragte zu den Auslagerungen herausgegeben hat.[880] Diese Risiken müssen durch die verantwortlichen Organe sorgfältig angegangen werden, da sie für ihre Informationen verantwortlich bleiben. So gilt es beispielsweise, die Daten zu verschlüsseln, den Schlüssel beim öffentlichen Organ zu managen und vertragliche Absicherungen zu treffen.

Im Rahmen der Befragung durch die PUK Datensicherheit wies der ehemalige Datenschutzbeauftragte, Bruno Baeriswyl, deutlich darauf hin, dass für die öffentliche Verwaltung das Legalitätsprinzip ausschlaggebend sei. Bürgerinnen und Bürger müssten sich darauf verlassen können, dass ihre Daten gemäss dem Gesetz bearbeitet werden. Somit sei in den Bereichen, in denen das Gesetz ausschliesst, dass Informationen weitergegeben werden dürfen, auch keine Risikoabwägung möglich; Informationen dürften in keinem Fall herausgegeben werden. Es braucht seiner Meinung nach folglich klare Rahmenbedingungen für die Nutzung der Cloud-Lösung. Gewisse Daten dürfe man nicht oder nur verschlüsselt in die Cloud geben, und man müsse sich bewusst sein, wo welche Informationen genau liegen. Solche Einschränkungen könnten sich aber auch negativ auf die Funktionalität der Cloud-Lösung auswirken.[881]

Auch die Direktionsvorsteherin der JI, Jacqueline Fehr, sieht die korrekte Handhabung der Informationssicherheit im Umfeld von Cloud-Lösungen als grosse Herausforderung. Sie gab an, der Regierungsrat habe lange darüber diskutiert und sich dann trotz gewisser Zweifel für diesen Weg entschieden.[882]

Andererseits wurde gegenüber der PUK Datensicherheit auch die Ansicht geäussert, dass der Austausch und die Nutzung moderner Lösungen, wie Microsoft 365, durch die rechtlichen Vorgaben erschwert oder verhindert würden.[883]

14.2 Aktuelle Sicherheitsorganisation

Die PUK Datensicherheit hat sich im Rahmen ihrer Abklärungen grundlegend mit der Organisation im Bereich der Informationssicherheit befasst und dabei verschiedene Rollen und Gremien identifiziert, die hier eine wesentliche Rolle spielen. Sie hält fest, dass die politische und strategische Führung in den Bereichen Informationssicherheit und Cybersicherheit, aber auch in der IKT-Grundversorgung beim Regierungsrat und beim Gremium SDI liegt. Auf der Ebene der direktionsübergreifenden Strukturen lässt sich hingegen feststellen, dass zur Umsetzung der Digitalisierung, der Informationssicherheit und der Cybersicherheit unterschiedliche Gremien zentral sind (siehe hierzu Tabelle 17 und Tabelle 18). Es lassen sich aber immerhin erste Ansätze zu einer stärkeren Koordinierung beobachten. So fanden beispielsweise mit der Neuauflage der Allgemeinen Informationssicherheitsrichtlinie (AISR) im Jahr 2025 die Gremien und Services aus der Cybersicherheitsstrategie nun auch in der neuen Richtlinie Erwähnung. Zudem wird die Cybersicherheitsstrategie seither unter dem Namen Informationssicherheitsstrategie geführt.

---

880 Datenschutzbeauftragte des Kantons Zürich, Leitfaden «Bearbeiten im Auftrag» vom Oktober 2024; Leitfaden «Verschlüsselung der Daten im Rahmen der Auslagerung – unter Inanspruchnahme von Informatikleistungen und unter Berücksichtigung der Geheimnispflichten» vom November 2023; Leitfaden «Besondere datenschutzrechtliche Aspekte der Cloud Nutzung – unter Berücksichtigung des «CLOUD Act» vom November 2023; Leitfaden «Nutzung externer Cloud-Dienste» vom Oktober 2024.

881 Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 12–13, 18.

882 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 27.

883 Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 9, 17.

Tabelle 17 Zuständigkeiten für die Umsetzung der Informations- und Cybersicherheit

	Informationssicherheit	**Cybersicherheit**
Politische Führung	Regierungsrat	Regierungsrat
Strategische Führung	SDI (RRB Nr. 392/2018)[884]	SDI (RRB Nr. 392/2018)[885] Kerngruppe Cyber[886]
Direktionsübergreifende Strukturen	ISIK FAGIS CCSC[887]	Cyber-Koordinator [ISIK] CCSC
Umsetzung in DIR/SK und weiteren Stellen	Direktionen/Staatskanzlei ISID	Direktionen/Staatskanzlei Zusammenarbeit mit KFO[888]
Strategische Grundlage	*AISR/BISR*	*Informationssicherheitsstrategie (Cybersicherheitsstrategie)*
RRB-Nr.	129/2015 795/2019 438/2025 (Beilage)	676/2022 (Beilage, Umsetzung)

Tabelle 18 Zuständigkeiten für die Umsetzung der IKT-Strategie sowie der Strategie Digitaler Wandel an den Schulen der Sek II

	IKT-Programm	**Digitaler Wandel an den Schulen der Sek II**
Politische Führung	Regierungsrat	Regierungsrat
Strategische Führung	SDI (RRB Nr. 392/2018)[889]	SDI *(RRB Nr. 392/2018)*
Direktionsübergreifende Strukturen	OIS[890] Amt für Informatik	OIS Amt für Informatik
Umsetzung in DIR/SK	IKT-Verantwortliche	Mittelschul- und Berufsbildungsamt (MBA) Informationssicherheitsbeauftragte SEK II
Strategische Grundlage	*IKT-Strategie*	*Strategie Digitaler Wandel an den Schulen der SEK II (DiWaSek II)*
RRB-Nr.	383/2018 625/2019	259/2019 1178/2019

884 Staatsschreiberin (Vorsitz), Direktionsvorsteherinnen und Direktionsvorsteher aus FD, JI, und BI sowie Generalsekretäre aus VD, BD, DS.

885 Staatsschreiberin (Vorsitz), Direktionsvorsteherinnen und Direktionsvorsteher aus FD, JI, und BI sowie Generalsekretäre aus VD, BD, DS.

886 Amtschef AFI (Leitung) [in AISR wird der ISIK als Leiter genannt], Cyber-Koordinator, leitende Personen aus relevanten Verwaltungseinheiten (Staatsanwaltschaft, Polizei und Kantonale Führungsorganisation), Kommunikationsverantwortliche des kantonalen Zentrums für Cybersicherheit, ein Vertreter einer kantonalen kritischen Infrastruktur.

887 Kantonales Kompetenzzentrum Cybersicherheit unter der Leitung des ISIK.

888 Kantonale Führungsorganisation.

889 Staatsschreiberin (Vorsitz), Direktionsvorsteherinnen und Direktionsvorsteher aus FD, JI, und BI sowie Generalsekretäre aus VD, BD, DS.

890 Leiter AFI (Vorsitz), IKT-Verantwortliche der einzelnen Direktionen und der Staatskanzlei.

14.2.1 Rolle des kantonalen Informationssicherheitsbeauftragten (ISIK)

Verortung und Berichterstattung

Der heutige Informationssicherheitsbeauftragte (ISIK), Philipp Grabher, ist Leiter des kantonalen Zentrums für Cybersicherheit (CCSC), welches im AFI angesiedelt ist. Er ist somit dem Leiter des AFI unterstellt. Der ehemalige Datenschutzbeauftragte meinte dazu, dass man den ISIK so verorten sollte, dass er Möglichkeiten zur Kontrolle habe und Anliegen auch eskalieren könne.[891] Auch aus Sicht der Finanzkontrolle ist zu prüfen, ob der ISIK mit seiner Querschnittsfunktion nicht besser direkt dem Direktionsvorstand oder dem Regierungsrat berichten oder diesem direkt unterstellt sein solle, um auch direktionsübergreifend mehr Schlagkraft zu entwickeln.[892] Eine Stärkung der Position des ISIK erachtete der Regierungsrat gemäss Aussage des Finanzdirektors als nicht notwendig. Mit der Berichterstattung an das Gremium SDI, so der Finanzdirektor, hatte der Regierungsrat das Gefühl, «das sei wirklich auf Toplevel angesiedelt».[893] Mindestens einmal jährlich ist der ISIK auch im Regierungsrat.[894] Zudem habe er Zugang zum Gremium Operative Informatiksteuerung (OIS).[895] Bis anhin sah der Finanzdirektor im Austausch mit dem ISIK keine Anzeichen, dass die Regierung ihn nicht unterstütze.[896] Auch der ISIK gibt an, in seiner Amtszeit vonseiten SDI und Regierungsrat Unterstützung erfahren zu haben.[897]

Weisungsrecht

Als der Regierungsrat 2015 die Stelle des damaligen Informatik-Sicherheitsbeauftragten (I-SiBe) geschaffen hatte, stattete er diesen nicht mit einem Weisungsrecht aus (siehe Kapitel 10.1.4). Auch der aktuelle Informationssicherheitsbeauftragte (ISIK) verfügt über kein Weisungsrecht. Es ist für ihn folglich herausfordernd und mit langwierigen Diskussionen um Einigung verbunden, wenn er etwas zentral umsetzen möchte, das von den Direktionen nicht gutgeheissen wird. Ein Weisungsrecht würde dies vereinfachen.[898]

Die aktuellen Regierungsmitglieder sind auch heute davon überzeugt, dass ein Weisungsrecht für den ISIK nicht zielführend wäre. Im Rahmen der Befragungen haben die verschiedenen Regierungsrätinnen und Regierungsräte dazu diverse Gründe angeführt: [899]

– Dass eine einzelne Person diese Verantwortung für die gesamte Verwaltung übernehme und auf allen Ebenen durchgreifen könne, sei faktisch nicht möglich. Aufgrund der Komplexität und Vielfältigkeit der kantonalen Verwaltung, deren heterogene Teile wiederum mit weiteren Instanzen verbunden seien, bestehe eine Zurückhaltung gegen Kompetenzstrukturen, die quer zur Direktionsstruktur verlaufen und deren interne Prozesse übersteuern können.

---

[891] Protokoll der Befragung von Bruno Baeriswyl vom 7. Juni 2024, S. 19.

[892] Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 12–13.

[893] Protokoll der Befragung von Ernst Stocker vom 13. Dezember 2024, S. 13.

[894] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 15.

[895] Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 22; Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 10.

[896] Protokoll der Befragung von Ernst Stocker vom 13. Dezember 2024, S. 13.

[897] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 18.

[898] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 13, 29.

[899] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 20–22; Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S. 13; Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 9–10; Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 18; Protokoll der Befragung von Carmen Walker Späh vom 13. Dezember 2024, S. 18; Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 10–11; Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 18.

– Es wird bezweifelt, dass eine Weisungsbefugnis auch gegenüber den gewählten Regierungsrätinnen und Regierungsräten, die schliesslich die Verantwortung für die Informationssicherheit haben, funktionieren könne. Nach Meinung der befragten Regierungsrätinnen und Regierungsräte ist es aber wichtig, dass die Informationssicherheitsbeauftragten als Spezialisten eine starke Position haben, damit ihre Feststellungen gehört und ernst genommen werden. Dazu gehöre ein entsprechendes Reporting, ein leichter Zugang zu den Entscheidungsträgern und die Sensibilisierung der Vorgesetzten und Amtsleitungen.
– Auch wenn heute kein Weisungsrecht bestehe, seien die Direktionsvorsteherinnen und Direktionsvorsteher in der Pflicht und hätten ein ureigenes Interesse daran, Massnahmen zu ergreifen, um Sicherheitsvorfälle zu verhindern.
– Schliesslich wird darauf hingewiesen, dass eine Führung, welche die Mitarbeitenden und Vorgesetzten überzeuge und Verständnis für die Informationssicherheit schaffe, der nachhaltigerer Weg sei. Um die Umsetzung der Informationssicherheit zu fördern, müsse diese in der Kultur ankommen. Allgemein müsse eine Unternehmenskultur herrschen, die es erlaube, auf Fehler und Risiken hinzuweisen und Probleme anzusprechen.

14.2.2 Rolle der Informationssicherheitsbeauftragten der Direktionen und der Staatskanzlei (ISID)

Zwar gab es bereits vor dem RRB Nr. 1193/2020 in den Direktionen Personen, die mit der Informationssicherheit befasst waren, jedoch wurden erst mit diesem Beschluss diesbezügliche Stellen geschaffen. Dies, obwohl bereits der BDO-Bericht 2016 empfohlen hatte, die Fachgruppe IT-Sicherheit mit dezidierten IT-Sicherheitsfachleuten zu je mindestens 50 Stellenprozenten zu besetzen.[900]

Die Zurückhaltung des Regierungsrates erklärt sich die Direktionsvorsteherin der JI damit, dass der Kantonsrat bei Stellenschaffungen jeweils genau hinschaue und damals in der JI bereits eine Person diese Funktion innehatte.[901]

Aufgaben

Aus Sicht des ISIK ist es die Aufgabe der ISID, die Informationssicherheitsrisiken mit der Direktionsleitung und den Amtsleitungen zu behandeln. Sie müssen eine Informationssicherheitsstrategie für die Direktion entwickeln und die direktionsinterne Organisation definieren und damit festlegen, welche Aufgaben zentral innerhalb der Direktion und welche dezentral erledigt werden müssen. Wo notwendig, sind die BISR für die Direktion mit weiteren Regelungen zu konkretisieren.[902]

Der ISID der Finanzdirektion, Jörg Poell, der durch die PUK befragt wurde, sieht sich als Übersetzer der kantonalen Vorgaben, indem er diese messbar macht und in Absprache mit den Amtsleitungen diskutiert, welcher Soll-Zustand konkret zu erreichen ist. Schliesslich habe er Kontrollmechanismen zu etablieren, um zu sehen, ob die Massnahmen auch umgesetzt werden.[903] So erfasst der ISID beispielsweise die Überprüfungen des Schutzbedarfs oder die erstellten Informationssicherheits- und Datenschutzkonzepte (ISDS) in einem ISMS und nutzt diese Informationen wiederum für Kontrollen.[904] Als weitere Aufgabe seien die Mitarbeitenden zu schulen und zu sensibilisieren.

---

[900] BDO AG, Unabhängige Überprüfung der Informatik des Kantons Zürich, 31. Oktober 2016, S. 61.

[901] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 21.

[902] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 25.

[903] Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 6.

[904] Protokoll der Befragung von Roman Bolinger vom 15. März 2024, S. 11.

Verortung

Wie beim ISIK stellen sich auch bei den ISID-Stellen Governance-Fragen. Gemäss dem Vorsteher der Finanzdirektion hat man die Struktur der Umsetzung in der Finanzdirektion nun sauber gelöst. Man habe den ISID Ende 2023 aus dem AFI herausgelöst und direkt dem Generalsekretär unterstellt. Der ISID berichte nun direkt an den Generalsekretär und den Direktionsvorsteher.[905] Die Konfiguration kann aber je nach Direktion unterschiedlich ausfallen, da gemäss der neuen AISR die Direktionsleitungen die direktionsinternen Kompetenzen und Verantwortlichkeiten des ISID festlegen. Auf gesamtkantonaler Ebene sind lediglich die Aufgaben der ISID als Mitglieder der FAGIS definiert.

Fehlendes Weisungsrecht und begrenzte Mittel

Da die ISID heute gegenüber ihren Verwaltungseinheiten keine Weisungsbefugnisse haben, müssen sie die Amtsleitungen, auch mit Hinweis auf die bestehenden übergeordneten Regelungen, überzeugen. Wenn dies, etwa aus Ressourcengründen, nicht gelinge, sei es, so der ISID der Finanzdirektion, Jörg Poell, für die kantonale Verwaltung nicht ungefährlich.[906] Ohne Weisungsbefugnis können die ISID nur informieren, auf die Risiken aufmerksam machen und den Umgang mit diesen Risiken mit den Leitungspersonen besprechen.[907]

Gemäss dem ISID der Finanzdirektion standen ihm, als er 2022 seine Funktion antrat, kaum Mittel zur Verfügung. Mit dem von ihm erarbeiteten Kontrollleitfaden habe er nun ein Mittel, um die Umsetzung der BISR zu begleiten, falls auf der Ebene der Direktion keine weiteren Regelungen erlassen werden.[908]

Eine Stärkung der Position des ISID wäre beispielsweise möglich, in dem er gegenüber den Ämtern Mindestanforderungen zu Richtlinien vorgeben, gewisse Schulungen als verbindlich erklären oder auch unzureichende Kontrollmassnahmen oder ISDS-Konzepte, die den kantonalen Projektmanagement-Vorgaben nicht genügen, zurückweisen könnte.[909]

Berichterstattung

Bei der Informationssicherheit besteht nach Angaben des Baudirektors, Martin Neukom, die Gefahr, dass das Thema untergeht. Deshalb habe er mit dem ISID seiner Direktion ein jährliches direktes Reporting eingerichtet. Auch dem Finanzdirektor ist es wichtig, dass die Direktionsvorsteher oder Direktionsvorsteherinnen dem Thema einen hohen Stellenwert beimessen und so auch ein Signal an die Mitarbeitenden senden. Deshalb sei die Informationssicherheit immer wieder Thema in der Geschäftsleitungssitzung der Direktion.[910]

---

[905] Protokoll der Befragung von Ernst Stocker vom 13. Dezember 2024, S. 20; Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 6.

[906] Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 8–9, 12–14.

[907] Protokoll der Befragung von Roman Bolinger vom 15. März 2024, S. 16.

[908] Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 7–8.

[909] Amt für Informatik, Kantonales Zentrum für Cybersicherheit, ISID FD, Memorandum betreffend Vorschlag für die Überarbeitung des Geschäftsorganisationskonzepts zur Informationssicherheit vom 14. August 2023.

[910] Protokoll der Befragung von Martin Neukom vom 13. Dezember 2024, S. 7, Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 9.

14.2.3 Direktionsinterne Organisation der Informationssicherheit

Die Direktionen unterscheiden sich darin, inwieweit sie auch auf der Ebene der Ämter Informationssicherheitsbeauftragte (ISiA) eingerichtet und als solche bezeichnet haben.[911] Es kann sich um Personen handeln, die nur für diese Aufgabe zuständig sind, wie beispielsweise der Leiter «Sicherheit und Datenschutz» beim AFI, oder es sind Mitarbeitende in einer anderen Funktion, die diese Aufgabe ergänzend zu einem bestimmten Anteil an Stellenprozenten übernehmen. In manchen Direktionen gibt es auf der Ebene der Ämter keine Informationssicherheitsbeauftragten. Die Unterschiede sind hier sehr gross.[912] Generell unterscheiden sich die Direktionen darin, inwieweit die Vorsteherinnen resp. Vorsteher den Ämtern klare Vorgaben machen oder die Ämter eher koordinierend in deren Anstrengungen unterstützen.[913]

Gemäss dem ISIK, Philipp Grabher, braucht es auch in den Direktionen und Ämtern eine Organisation. Es sei nicht so, wie manche denken, dass mit der Umsetzung der kantonalen Informationssicherheitsstrategie, der Schaffung der zentralen Stelle und dem Aufbau des übergeordneten Regelwerks sowie den direktionsübergreifenden Dienstleistungen das Thema erledigt sei. Jede Direktion benötige, wie in der neuen AISR vorgeschrieben, eine eigene Informationssicherheitsstrategie, müsse ein Programm aufsetzen, selber Audits durchführen, die Wirksamkeit überprüfen und die Erkenntnisse mit den Leitungsebenen teilen.[914]

14.2.4 ISMS in den Direktionen

Als Folge der beschriebenen Heterogenität gibt es auch nicht zwingend in jeder Direktion ein ISMS, das die gesamte Direktion erfasst. Dies bedeutet gemäss dem ISID der Finanzdirektion aber nicht, dass überhaupt keine ISMS bestehen. So lägen beispielsweise auf der Ebene des Steueramtes sehr viele entsprechende Richtlinien und ein ISMS vor. Die Richtlinien auf der Ebene der Ämter gelte es auf der Stufe der Direktion zusammenzutragen, um jene Ämter zu unterstützen, die aufgrund ihrer Grösse kein eigenes ISMS betreiben könnten.[915]

14.2.5 Rolle des Gremiums SDI

Gemäss der AISR stellt das Gremium Steuerung und digitale Verwaltung (SDI) im Auftrag des Regierungsrates direktionsübergreifend sicher, dass die Informationen und die damit verbundenen Werte des Kantons angemessen geschützt sind. Das SDI beaufsichtigt die Tätigkeiten zur Informationssicherheit, bereitet die AISR vor und erlässt die BISR. Das Gremium sorgt dafür, dass die Informationssicherheit bei der Umsetzung der IKT-Strategie angemessen berücksichtigt wird, und steuert die Umsetzung der kantonalen Informationssicherheitsstrategie. Im Bereich der Überprüfung gibt das SDI die zu erhebenden Kennzahlen sowie den Plan zur kantonalen Audittätigkeit frei, nimmt die Berichte über den Stand, die Risiken und das Optimierungspotenzial zur Kenntnis und setzt den Regierungsrat darüber in Kenntnis. Neben dem Erlass der BISR hat das SDI gemäss der Vorsitzenden, Kathrin Arioli, eine beratende und koordinierende Funktion. Aus ihrer Sicht ist es richtig, dass die Kompetenz für den Erlass der grundlegenden Regelungen, wie der AISR oder der Verordnungen, beim Regierungsrat liegt. Bei gravierenden Mängeln müsse der Regierungsrat in diesen Regelwerken Anpassungen vornehmen.[916]

---

911 Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 6.

912 Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 8, 13–14.

913 Protokoll der Befragung von Philipp Grabher vom 15. März 2024, S. 31.

914 Protokoll der Befragung von Philipp Grabher vom 15. März 2024, S. 8, 19.

915 Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 9, 15.

916 Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 10–13.

Der ISIK gab an, das Gremium SDI halbjährlich über den Stand der Umsetzung der kantonalen Informationssicherheitsstrategie sowie die vom Zentrum für Cybersicherheit (CCSC) initiierte Initiative zur Lieferantenüberprüfung zu informieren.[917]

Aus Sicht der Direktionsvorsteherin der JI, Jacqueline Fehr, kommt dem SDI die Rolle zu, die Erfahrungen aus den Direktionen bei der Umsetzung wieder zusammenzuführen und die Richtlinien auf dieser Basis zu revidieren, wobei die Fäden natürlich beim ISIK zusammenlaufen, der für den Rückfluss der Informationen ins SDI sorgt.[918]

Die PUK Datensicherheit konnte bei der Befragungen der Regierungsrätinnen und Regierungsräte feststellen, dass auch der Gesamtregierungsrat das gemeinsame Vorgehen, namentlich die heutige direktionsübergreifende Organisation mit dem SDI für die strategische Ebene und dem Gremium der Operativen Informatiksteuerung (OIS) für die operative IKT-Koordination, diskutiert hat.[919] Die PUK Datensicherheit stellte auch fest, dass die Mitglieder des Regierungsrates unterschiedlich informiert sind, was sich teilweise durch die Mitgliedschaft bzw. Nichtmitgliedschaft im SDI erklären lässt.

14.2.6 Rolle der Fachgruppe Informationssicherheit (FAGIS)

Bereits mit dem «Organisationskonzept Informatiksicherheit» im Jahr 2015 richtete der Regierungsrat das Kompetenzzentrum IT-Sicherheit ein, welches damals aus der ISIK-Stelle und der Fachgruppe Informationssicherheit (FAGIS) bestand.[920]

Gemäss der neuen AISR besteht die FAGIS aktuell aus dem ISIK, den acht ISID, einer Vertretung der Datenschutzbehörde sowie einer Verbindungsperson zur KAPO und zum AFI. Nach Auskunft des ISIK nimmt auch die IKT-Sicherheitsbeauftragte des Projektes zur Digitalisierung der Schulen der Sek II daran teil. Die FAGIS berät das SDI, stellt dem Gremium Erkenntnisse zu kantonalen Informationssicherheitsrisiken zur Verfügung und beantragt ihm den Erlass oder die Anpassung der BISR, für deren Optimierung es fortlaufend sorgt. Des Weiteren nimmt die FAGIS Anliegen aus den Direktionen und der Staatskanzlei entgegen und kann Experten- und Fachgruppen einsetzen, um bestimmte Informationssicherheitsthemen zu behandeln.

Alle zwei Monate findet unter der Leitung des ISIK ein Austausch statt, an dem die Entwicklungen in den Direktionen und der Staatskanzlei, aber auch die Entwicklung der gesamtkantonalen Dienstleistungen vorgestellt und besprochen werden.[921] Daneben gibt es auch eine Zusammenarbeit gewisser ISID untereinander, die Themen, wie beispielweise Awareness-Kampagnen, gemeinsam angehen. Gemäss der BISR 6 vom 4. Mai 2021, Richtlinie für Schulungsmassnahmen in Informationssicherheit, sind Mitarbeitende regelmässig stufen- und funktionsgerecht zu sensibilisieren und zu schulen. Gemäss dem Leiter der Digital Solutions, Urs Kaderli, zogen jedoch bei der koordinierten Umsetzung nicht alle Direktionen gleich mit. Angesichts der Dringlichkeit habe die JI früher mit eigenen Schulungen begonnen, bevor dann mit der Cybersicherheitsstrategie (heute Informationssicherheitsstrategie) nach 2022 mit dem Aufbau kantonaler Schulungen begonnen werden konnte (siehe Kapitel 14.3.2).[922]

---

[917] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 26.

[918] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 13.

[919] Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 18–19; Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 18, Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 9, 13, 18; Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 17–18, Protokoll der Befragung von Carmen Walker Späh vom 13. Dezember 2024, S. 14–15; Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 8–9; Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S. 14–15.

[920] RRB Nr. 129/2015 vom 11. Februar 2015, Organisationskonzept für die Informatiksicherheit in der kantonalen Verwaltung (Genehmigung).

[921] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 23, 26.

[922] Protokoll der Befragung von Urs Kaderli vom 1. November 2024, S. 11, 14.

Gemäss den befragten ISID tauschen diese auch erarbeitete Dokumente oder Schulungsunterlagen aus oder teilen sich gewisse Arbeiten auf.[923] Falls im Rahmen des kantonalen Audits in mehreren Direktionen und der Staatskanzlei die gleichen Feststellungen gemacht werden, sei es auch im Sinne des Finanzdirektors, dass diese in der FAGIS gemeinsam besprochen und angegangen werden.[924] Der Sicherheitsdirektor, Mario Fehr, ist der Meinung, dass man auf die Meinung der FAGIS hören sollte und heute nicht mehr in der Position sei, Ratschläge von Informationssicherheitsbeauftragten nicht ernst zu nehmen. Die FAGIS könne mit gemeinsamen Handlungsrichtlinien, die dann auch gehört werden, an das Gremium SDI gelangen.[925]

Eine Verpflichtung der ISID, sich zu koordinieren, scheint aktuell aber nicht zu bestehen. Abgesehen vom Antragsrecht zur Weiterentwicklung der BISR hat die FAGIS keine Entscheid- oder Antragskompetenz.

14.2.7 Rolle des Gremiums Operative Informatiksteuerung (OIS)

Interessanterweise hat sich im Rahmen der Befragungen herauskristallisiert, dass gemäss der AISR zwar die FAGIS die Anstrengungen im Bereich der Informationssicherheit bündelt, wesentliche Vorentscheidungen über die Weiterentwicklung der Informatik jedoch im Gremium Operative Informatiksteuerung (OIS) gefällt werden. In diesem Gremium unter dem Vorsitz des Leiters des AFI, Hansruedi Born, sind alle Informatikverantwortlichen der Direktionen und der Staatskanzlei vereinigt. Gemäss Ziffer 20 der IKT-Strategie handelt es sich beim OIS um das Koordinations- und Konzeptgremium für verwaltungsweit relevante, fachtechnische IKT-Fragen. So prüft das OIS beispielsweise neue Fachapplikationen darauf, ob diese technisch, organisatorisch und finanziell strategiekonform sind oder ob bereits etwas Ähnliches besteht. Bei Bedarf wird diese Frage auf Basis der OIS-Einschätzung auch im SDI nochmals diskutiert. Die Prüfschritte erfolgen, bevor der Regierungsrat einen Beschluss über ein Digitalisierungsprojekt fällt.[926] Inwieweit im Rahmen dieser Prüfungen auch die Frage der Kompatibilität mit den kantonalen Anstrengungen im Bereich der Informationssicherheit geprüft werden und dazu auch die FAGIS oder der ISIK eingebunden werden, entzieht sich der Kenntnis der PUK Datensicherheit. Gemäss dem ISIK ist die Informationssicherheit an den Sitzungen des OIS regelmässiges Traktandum.[927]

Die Bedeutung des OIS zeigt sich ferner darin, dass gemäss dem Sicherheitsdirektor auch die Kantonspolizei, die nicht Teil der kantonalen IKT ist, ihre Projekte auf freiwilliger Basis durch das OIS prüfen lässt. Die KAPO koordiniere sich mit diesem Gremium, weil sie den gleichen Sicherheitsstandard anstrebe.[928] Gemäss der Bildungsdirektorin sollten auch direktionsübergreifende Anstrengungen zum koordinierten Umgang mit gleichlautenden Audit-Empfehlungen in diesem Gremium erfolgen.

In der AISR wird dieses für die kantonale Digitalisierung äusserst wichtige Gremium nicht abgebildet. Im Rahmen der Befragung wurde die Anregung eingebracht, dass die ISID die Möglichkeit haben sollten, ihre Anliegen bezüglich der Informationssicherheit direkter ins OIS einzubringen. Gemäss dem Sicherheitsdirektor, der diesen Hinweis gerne aufnahm, wäre es möglich, die ISID im Rahmen der einzelnen Projekte einzubinden oder die FAGIS als Gesamtgremium zu berücksichtigen.[929]

---

[923] Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 20; Protokoll der Befragung von Roman Bolinger vom 15. März 2024, S. 15.

[924] Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 19–20.

[925] Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 18.

[926] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 23.

[927] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 27.

[928] Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 13.

[929] Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 20.

14.3 Kantonale Angebote zur Informationssicherheit

14.3.1 Kantonale Audits

Das Projekt IKT-Sicherheit der IKT-Strategie zielte darauf ab, alle für ein kantonsweites Informationssicherheitsmanagement notwendigen Ressourcen und Prozesse festzulegen und diese zu auditieren. Vor diesem Hintergrund prüfte der kantonale Informationssicherheitsverantwortliche (ISIK) in Absprache mit der Projektleitung des IKT-Programms 2021 die Umsetzung der verschiedenen Vorgaben aus der AISR und den BISR.

Der Auditbericht vom 9. Dezember 2021 enthielt für die Direktionen, die Staatskanzlei und das Amt für Informatik zentrale Feststellungen und Empfehlungen.[930] Im Dezember 2022 beschloss der Regierungsrat, das Audit zu wiederholen, um die Umsetzung der bestehenden Abweichungen zu überprüfen.[931] Im August 2023 erhielten die Informationssicherheitsverantwortlichen in den Direktionen und der Staatskanzlei den entsprechenden Bericht.[932] Als weiteres Prüfthema nahm man den sicheren Umgang und die Entsorgung von Datenträgern auf.

Im zweiten Bericht ortete man Verbesserungspotenzial beim Inventar der schützenswerten Positionen und beim Schwachstellen- und Lieferantenmanagement. Die Feststellungen im Bereich des Schwachstellen-Managements sind gemäss dem ISID der Finanzdirektion auch dem Umstand geschuldet, dass der technische Betrieb von Applikationen aus den Direktionen ins AFI verschoben wurde oder zumindest auf dessen zentralen Rechenzentren laufe, die Applikationen aber durch die einzelnen Direktionen genutzt würden. Es sei ungenügend geklärt, wer für die diesbezüglichen Schwachstellen und die Kosten der Lizenzen zur Softwareaktualisierung zuständig sei.[933]

Der Auditbericht mit den Feststellungen zu den verschiedenen Prüfbereichen wurde im Gremium SDI sowie im Regierungsrat diskutiert.[934] Auch wenn eine interne Vergleichbarkeit zur Verbesserung beitragen könnte, wurde der im Audit enthaltene Vergleich der Direktionen und der Staatskanzlei untereinander, besonders das Rating, von den Mitgliedern des Regierungsrates nicht unbedingt begrüsst.[935] Die PUK Datensicherheit stellte im Rahmen ihrer Befragungen fest, dass bei den Regierungsratsmitgliedern keine gesamtkantonale Sicht auf die Auditergebnisse besteht. Vielmehr betonten sie, dass sie als Direktionsvorstehende vorrangig dafür zuständig seien, die Massnahmen in ihren Direktionen umzusetzen, und wollten oder konnten sich nicht zur Situation in den anderen Direktionen äussern.[936] Einzelne Mitglieder der Regierung kritisierten überdies, dass der ISIK im Rahmen der Administrativuntersuchung gesagt habe, die JI sei nach seinem Eindruck bezüglich Informationssicherheit weiter

---

930 Finanzdirektion, Amt für Informatik, Audit Informationssicherheit, Organisation ISMS, 9. Dezember 2021.

931 Finanzdirektion, Amt für Informatik, Kantonales Zentrum für Cybersicherheit, Aktennotiz an Regierungsrat, Informationssicherheit, Umsetzungstand in den Direktionen und der Staatskanzlei.

932 Finanzdirektion, Amt für Informatik, Audit Informationssicherheit Organisation ISMS, 31. August 2023.

933 Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 11.

934 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 14; Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 14.

935 Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 14; Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S. 12.

936 Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S. 12; Protokoll der Befragung von Carmen Walker Späh vom 13. Dezember 2024, S. 10; Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 11, 20; Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 16.

als andere Direktionen,[937] und relativierten diese Aussage.[938] Dass der Regierungsrat ein Bild von sich als kollegiales Gremium vermitteln und unbedingt vermeiden wollte, dass die einzelnen Direktionen vor der PUK Datensicherheit unterschiedlich dastehen und gegeneinander ausgespielt würden, zeigt sich auch in einem Dokument, das im Rahmen der Vorbereitung auf die PUK-Befragungen erstellt worden war.[939]

In Bezug auf die eigene Direktion führte der Baudirektor, Martin Neukom, aus, dass die Ressourcen für die Informationssicherheit dort zielgerichtet eingesetzt würden, wo die Risiken am höchsten seien.[940] In Kenntnis der Risiken ist folglich eine Priorisierung möglich. Eine derartige risikobasierte Vorgehensweise ist auf gesamtkantonaler Ebene wohl nicht möglich, solange eine rein direktionale Sicht auf die Auditergebnisse vorherrscht, wie es aktuell der Fall ist. Gemäss der Staatsschreiberin müsste vielmehr der ISIK dem SDI berichten, wenn irgendwo gravierende Mängel bestünden.[941]

Angesichts des heterogenen Umfelds verfolgt der ISIK deshalb einen zweistufigen Ansatz, wobei er auf der zentralen Steuerungsebene in ausgewählten Bereichen zentrale Dienstleistungen und kantonale Informationssicherheitsstandards (ISST) bereitstellt, um die Direktionen und die Staatskanzlei zu unterstützen. So können beispielsweise im Bereich der Sensibilisierung der Mitarbeitenden Synergien genutzt werden. Die Direktionen und die Staatskanzlei haben sich an die minimalen gesamtkantonalen Vorgaben zu halten, können aber auch darüber hinausgehen. Der Entscheid darüber, ob und wie die gesamtkantonalen Angebote genutzt werden sollen, liegt bei den Amts- und Direktionsleitungen respektive beim Regierungsrat. Sie haben abzuwägen, wie stark sie angesichts anderer Aufgaben, Risiken und Herausforderungen den Fokus auf die Informationssicherheit legen.[942] Die Aufgabe des ISIK ist es, allfälligen Handlungsbedarf aufzuzeigen. Der Entscheid über den Umgang mit den Risiken liegt bei der Direktions- oder Amtsleitung.[943]

14.3.2 Kantonale Schulungen

Die BISR 6 vom 4. Mai 2021 schreibt dem ISIK eine Rolle im Bereich der Schulungsmassnahmen zur Informationssicherheit vor. Im Rahmen der Cybersicherheitsstrategie schuf der Regierungsrat hierzu die Stelle für Sicherheitskultur. Gemäss dem ISIK hat das Kompetenzzentrum Informationssicherheit (CCSC) vor, jährlich zwei Kampagnen für alle kantonalen Mitarbeitenden zur Verfügung zu stellen. 2023 habe das CCSC beispielweise Schulungen zur sicheren Entsorgung von Datenträgern und zur Klassifizierung von Informationen gestartet. Daneben fänden zielgruppenorientierte Anlässe und Schulungen statt. Die Schulungen seien als kantonale Angebote nicht verpflichtend für die Direktionen und die Staatskanzlei. Aus Sicht des ISIK ist die Unterstützung der Direktions- und Amtsleitungen deshalb unabdingbar, damit die zur Verfügung gestellten Angebote von den Mitarbeitenden auch besucht werden.[944] Auf Antrag der SDI wurde im kantonalen Schulungsprogramm ein Schwerpunkt auf die Digitalisierung und die diesbezüglichen Fragestellungen aufgenommen.[945]

---

[937] IT & Law Consulting AG, Gesprächsnotizen/Protokoll in Sachen Kanton Zürich: Datenmissbrauch, Interview vom 14. Dezember 2020.

[938] Protokoll der Befragung von Natalie Rickli vom 13. Dezember 2024, S. 16; Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 13.

[939] Staatskanzlei, Rechtsdienst, Aktennotiz «PUK Datensicherheit Einzelfragen» vom 27. August 2024.

[940] Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S. 15.

[941] Protokoll der Befragung von Kathrin Arioli vom 22. November 2024, S. 14.

[942] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 10–11.

[943] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 19.

[944] Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 22–23.

[945] Protokoll der Befragung von Jacqueline Fehr vom 8. November 2024, S. 28.

Schulungen zur Informationssicherheit sind nun im kantonalen Weiterbildungsangebot enthalten und den Mitarbeitenden über die entsprechende Plattform zugänglich.

Schulungen in den Direktionen

Die PUK Datensicherheit liess sich von den Vertretern der Direktionen auch zu laufenden Schulungsmassnahmen informieren. Sie stellte fest, dass es auch hier Unterschiede gibt. Der Leiter der Digital Solutions der JI, Urs Kaderli, vermutet, dass es am politischen Willen fehle, alle kantonalen Mitarbeitenden hinsichtlich Awareness in gleicher Weise zu schulen.[946]

Kantonale Trainingslösung gegen Phishing

Im Rahmen der Befragung durch die PUK Datensicherheit wiesen verschiedene Befragte auf die kantonal implementierte Lösung zum Schutz vor Phishing hin. Dabei werden den Mitarbeitenden regelmässig E-Mails zugestellt, die sie nicht anklicken und als gefährlich melden sollten. Auf diese Weise findet eine Sensibilisierung statt. Gemäss der Finanzkontrolle war dies ein wichtiger Schritt, der bei der Sensibilisierung aller kantonalen Mitarbeitenden zu Verbesserungen geführt habe.[947] Die Trainingsplattform ist zwar in der kantonalen E-Mail-Lösung implementiert und mit dem digitalen Arbeitsplatz in der ganzen kantonalen Verwaltung ausgerollt. Die Funktion ist jedoch nicht automatisch aktiviert und muss durch die Endnutzer ausgelöst werden.[948]

14.3.3 Überprüfung der Lieferantenbeziehungen

Vor dem Hintergrund der Vorfälle beim Bund (Xplain) wurden auch im Kanton Zürich Risiken in der Lieferkette überprüft. Das kantonale Audit stellte fest, dass direktionsübergreifend Risiken in der Lieferkette bestünden. Das Zentrum für Informationssicherheit startete zeitnah ein Pilotprojekt, um die Widerstandsfähigkeit der kantonalen Lieferkette zu verbessern.[949] In der Folge gelangte der ISIK mit dem Vorschlag einer kantonalen Initiative zur systematischen Lieferantenüberprüfung via SDI[950] an den Regierungsrat.[951] Wie Regierungsrätin Jacqueline Fehr angab, hatte der Regierungsrat zu dieser Thematik einen Schwerpunkt gesetzt und sich auch im Rahmen einer Klausur eingehend damit befasst. Auch weitere Regierungsräte und Regierungsrätinnen machten auf die Bedeutung der Lieferantensicherheit aufmerksam.[952]

Nach einem ersten Überblick auf Basis von Security-Ratings, die öffentliche verfügbare Informationen auswerten, unterzog das kantonale Zentrum für Cybersicherheit (CCSC) mindestens drei Lieferanten pro Direktion einer vertieften Prüfung, indem es die Organisation und die Prozesse überprüfte. Insgesamt wurden auf diese Weise um die dreissig Lieferanten untersucht.[953]

---

946 Protokoll der Befragung von Urs Kaderli vom 1. November 2024, S. 16.

947 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 14.

948 Protokoll der Befragung von Roman Bolinger vom 15. März 2024, S. 17.

949 Kanton Zürich, Amt für Informatik, Amtsrapport Cybersicherheitsstrategie vom 23. Oktober 2023.

950 Kanton Zürich, Amt für Informatik, Präsentation «Cyberrisiken in der Lieferkette» des ISIK vom 18. Dezember 2023.

951 Finanzdirektion, Amt für Informatik, Kantonales Zentrum für Cybersicherheit, Aktennotiz an Regierungsrat betreffend Kantonale Initiative zur Bewertung der Cyber-Risiken in der Lieferkette der Verwaltung.

952 Protokoll der Befragung von Silvia Steiner vom 6. Dezember 2024, S. 22; Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 11; Protokoll der Befragung von Martin Neukom vom 6. Dezember 2024, S. 17.

953 Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 9, 12.

Bei der Datenbearbeitung durch Dritte stellte die Finanzkontrolle fest, dass in Verträgen zunehmend Anforderungen gestellt und auch eingehalten werden. Dies sei aber bisher noch nicht genügend etabliert. Weiter sei es heute, auch aufgrund der damit verbunden Kosten, oftmals nicht so, dass von Dienstleistern Auditberichte oder Zertifikate zu deren internen Kontrollprozessen verlangt werden.[954]

Aktuell unterstützt das Gremium SDI ein Vorhaben, mit dem das CCSC diese Prozesse weiterentwickeln möchte. Es soll ein einheitlicher Standard zur Überprüfung von Lieferanten definiert werden, der den Direktionen und der Staatskanzlei als Grundlage für eigene Lieferantenbewertungen dienen soll. Diese Informationen sollen schliesslich, in einer kantonalen Plattform zusammengeführt, Synergien für den gesamten Kanton schaffen.[955]

14.3.4 Kantonale Entsorgungsprozesse

Zentraler Entsorgungsprozess beim Amt für Informatik (AFI)

Die BISR 19 vom 19. Dezember 2022 zur Sicherheit von Informationssystemen schreibt vor, dass die Ausserbetriebnahme und fachgerechte Entsorgung von Informationssystemen nach einem dokumentierten Prozess zu erfolgen hat und Informationen auf den Speichermedien vor dem Austausch, der Entsorgung oder Wiederverwendung irreversibel gelöscht werden müssen. Ein kantonaler Leitfaden hält fest, wie welche Arten von Datenträgern korrekt gelöscht und vernichtet werden müssen.[956] Schliesslich gibt die kantonale HERMES-Projektmethodik vor, sich im Rahmen eines Projektes auch konzeptuell mit der korrekten Ausserbetriebnahme und Entsorgung zu befassen.

Das AFI hat einen zentralen Prozess aufgebaut, über den Wechseldatenträger und andere digitale Datenträger abgegeben werden können. Dabei wird über die Zusammenarbeit mit einem zertifizierten Unternehmen sichergestellt, dass die Daten sicher gelöscht werden.[957] Die Nutzung dieses Angebots ist allerdings freiwillig. Gemäss dem ISID der Finanzdirektion ist es also weiterhin möglich, dass die Ämter einen eigenen Dienstleister beauftragen oder Mitarbeitende beispielsweise USB-Sticks mittels Löschsoftware selbst löschen.[958]

Mit dem vollständigen Rollout des einheitlichen digitalen Arbeitsplatzes (DAP) in der ganzen kantonalen Verwaltung sind nun die Prozesse zur Ausserbetriebnahme von Clients beim AFI angesiedelt, womit ein zentraler Entsorgungsprozess besteht.[959] Die Rückgabe des Gerätes ist mit Seriennummer zu bestätigen und es lässt sich auch im kantonalen Serviceportal überprüfen, welches Gerät wann an das AFI zurückgegangen ist.[960]

In dieser Hinsicht sahen deshalb verschiedene Befragte seit der Migration zum AFI in diesem Bereich keinen Handlungsbedarf mehr.[961]

---

954 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 16–17.

955 Kanton Zürich, Amt für Informatik, Präsentation Vorhaben «Lieferantensicherheit» beim SDI vom 17. März 2025.

956 Kanton Zürich, Leitfaden: Umgang mit Wechseldatenträgern, in Kraft seit 19. Dezember 2022.

957 Protokoll der Befragung von Philipp Grabher vom 8. März 2024, S. 9, 21–23.

958 Protokoll der Befragung von Jörg Poell vom 15. März 2024, S. 20.

959 Protokoll der Befragung von Urs Kaderli vom 1. November 2024, S. 15.

960 Protokoll der Befragung von Roman Bolinger vom 15. März 2024, S. 17.

961 Protokoll der Befragung von Mario Fehr vom 13. Dezember 2024, S. 31; Protokoll der Befragung von Roman Bolinger vom 15. März 2024, S. 12; Protokoll der Befragung durch Martin Neukom vom 13. Dezember 2024, S. 16–17.

Lösung der Direktion der Justiz und des Innern

Für die Bedürfnisse der JI war der Prozess des AFI aufgrund der Erfahrungen des Datensicherheitsvorfalls ungenügend. Der Leiter der Digital Solutions, Urs Kaderli, gab an, er habe sowohl den Leiter des IKT-Programms als auch das Gremium OIS über seine Bedenken informiert. Es sei ihm wichtig gewesen, für alle ausgemusterten Geräte ein Lösch-Zertifikat zu erhalten und dieses – wie auch den Austrag – im eigenen Inventar festhalten zu können, so habe er selber die Übersicht. Da der Prozess beim AFI die Digital Solutions nicht überzeugte, wickelte sie die Ausmusterung über einen eigenen Prozess ab.[962] Die Digital Solutions habe jedes JI-Gerät zurückgeholt, es aus den Systemen gelöscht, sauber gewipt und dann mit Lieferschein dem Broker übergeben, der wiederum zu jeder Seriennummer ein Lösch-Zertifikat ausgehändigt habe. Für die Digital Solutions sei der Weg von der Direktion zum AFI und zum Broker zu wenig überwacht, weshalb sie sich aufgrund ihrer negativen Erfahrungen für diese Lösung entschieden habe.[963]

14.4 Koordination

14.4.1 Koordination bei der Umsetzung der verschiedenen Aspekte des Gesetzes über die Information und den Datenschutz (IDG)

Das Gesetz über die Information und den Datenschutz (IDG) macht Vorgaben in den Bereichen des Datenschutzes, der Informationsverwaltung und Archivierung, zum Öffentlichkeitsprinzip sowie zur Informationssicherheit. Im Rahmen ihrer Befragungen stellte die PUK Datensicherheit fest, dass die diesbezüglichen Zuständigkeiten innerhalb der Verwaltung bei unterschiedlichen Stellen angesiedelt sind und der Austausch nicht gewährleistet ist.

Die Verantwortung für die Umsetzung des IDG liegt gemäss § 60 Abs. 1 lit. e der Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung (VOG RR) bei den Direktionen und der Staatskanzlei. Die nach § 28 der Verordnung über die Information und den Datenschutz (IDV) eingesetzte Koordinationsstelle sowie die diesbezüglichen zentralen Ansprechpersonen in den Direktionen befassen sich, wie die PUK Datensicherheit festgestellt hat, lediglich mit dem Öffentlichkeitsprinzip.[964] Im Gegensatz zur Informationssicherheitsorganisation besteht innerhalb der kantonalen Verwaltung aktuell keine vergleichbare Organisation für den Datenschutz. Im Rahmen der Totalrevision des IDG sollen nun mit § 44c des Gesetzes über die Organisation des Regierungsrates und der kantonalen Verwaltung (OG RR) in jeder Direktion und der Staatskanzlei Datenschutzberatende eingeführt werden.

14.4.2 Koordination durch die Konferenz der Generalsekretärinnen und Generalsekretäre

Gemäss § 43 Abs. 1–3 OG RR bearbeitet die Konferenz der Generalsekretärinnen und Generalsekretäre (GSK) unter dem Vorsitz der Staatsschreiberin, Kathrin Arioli, Aufgaben, welche die allgemeine Verwaltung betreffen, sichert den Informationsfluss zwischen den Direktionen und unterstützt den Regierungsrat bei der Vorbereitung und Umsetzung von Beschlüssen.

---

962 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 14–15.

963 Protokoll der Befragung von Fredi Steiner vom 6. September 2024, S. 14–15.

964 Staatskanzlei des Kantons Zürich, Schreiben «Koordinationsstelle IDG der Staatskanzlei, zentrale Ansprechperson der Direktion» vom 21. Juli 2008 an die Direktionen des Regierungsrates.

Die GSK ist laut der Volkswirtschaftsdirektorin, Carmen Walker Späh, dazu angehalten, die Zusammenarbeit zwischen den Direktionen und der Staatskanzlei zu unterstützen. Sachverhalte, die auch andere Direktionen interessieren könnten, seien dort zu behandeln.[965] Für den Finanzdirektor, Ernst Stocker, müsste die GSK auch bei Auditergebnissen, die mehrere Direktionen in ähnlicher Weise betreffen, vorgeben, wie damit umzugehen ist.[966]

Gemäss der Generalsekretärin der JI, Jacqueline Romer, versucht die GSK, sich über gesamtkantonale Managementsaufgaben stärker abzusprechen und auch zu schauen, wo man voneinander profitieren könnte. Nach ihrer Erfahrung ist die Koordination im Vergleich zu kleineren Kantonen weniger ausgeprägt, in der aktuellen GSK sei der Wille dazu aber vorhanden.[967] Bei Querschnittsthemen werde versucht, sich über die Rahmenbedingungen und Eckwerte zu verständigen, diese gerade auch bei der Erarbeitung der neuen Strategie Digitale Verwaltung 2025+ noch besser abzustimmen und direktionsübergreifender zu klären. Aus diesem Grund habe sie die von der JI im Bereich Datenschutz & Information ergriffenen Massnahmen in der GSK vorgestellt und den kantonalen Entsorgungsprozess sowie die Cloud-Lösung dort traktandiert.[968]

Der Regierungsrat hat am 15. Januar 2025 mit dem Regierungsratsbeschluss RRB Nr. 45/2025 die neue Digitalisierungsstrategie 2025+ festgesetzt und im Juni 2025 mit dem Regierungsratsbeschluss RRB Nr. 635/2025 deren Umsetzung beschlossen.[969] Die neue Digitalisierungsstrategie hält im Wirkungsfeld «Transformation der Verwaltung» nun explizit das strategische Ziel fest, dass Prozesse konsequent angeglichen werden sollen, dass gemeinsame Lösungen eine Selbstverständlichkeit seien und dass die digitale Verwaltung ganzheitlich zu betrachten und übergreifend zu steuern sei. Auf Basis der vorliegenden Regierungsratsbeschlüsse ist für die PUK Datensicherheit zum Zeitpunkt der Berichtsredaktion nicht ersichtlich, inwieweit die Informationssicherheit im Rahmen der neuen Strategie Digitale Verwaltung 2025+ auch berücksichtigt wird. Es ist also unklar, ob die aufgezeigte direktionsübergreifende Herangehensweise auch für den Informationssicherheitsbereich gilt. Auf den ersten Blick ist davon auszugehen, dass die Informationssicherheit nicht zentraler Inhalt der Digitalisierungsstrategie ist, womit der gleiche Fehler, nämlich die Nichtberücksichtigung der Informationssicherheit, nochmals begangen würde.

14.5 Rolle weiterer Aufsichtsorgane

Sowohl die Finanzkontrolle als auch die Datenschutzbeauftragte nehmen in ihrem Bereich Prüfungen zur Informationssicherheit vor. Erstere legt einen klaren Fokus auf die Finanzen, während Letztere die Anwendung der Vorschriften des IDG beaufsichtigt, wovon die Informationssicherheit nur einen Teil ausmacht.

Die PUK Datensicherheit stellte im Rahmen der Befragungen fest, dass einige der befragten Personen in Anbetracht der Kontrolltätigkeit der Finanzkontrolle und der Datenschutzbeauftragten keinen Bedarf mehr für eigene interne Kontrollen sahen. Die bis ins Jahr 2020 von der Informatiksicherheitsverordnung (ISV) vorgesehenen internen Audits im Bereich der Informationssicherheit waren nicht systematisch umgesetzt worden.

---

965 Protokoll der Befragung von Carmen Walker Späh vom 13. Dezember 2024, S. 17.

966 Protokoll der Befragung von Ernst Stocker vom 6. Dezember 2024, S. 20.

967 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 11.

968 Protokoll der Befragung von Jacqueline Romer vom 1. November 2024, S. 14–15.

969 RRB Nr. 45/2025 vom 15. Januar 2025, Strategie Digitale Verwaltung 2025+ (Festsetzung); RRB Nr. 635/2025 vom 11. Juni 2025, Strategie Digitale Verwaltung 2025+, Umsetzung.

Die Datenschutzbeauftragte hielt dazu gegenüber der PUK Datensicherheit klar fest, dass interne Kontrollen notwendig seien und die Verantwortung für diese bei den öffentlichen Institutionen liege. Angesichts der Ressourcen der Datenschutzbehörden und der Anzahl der beaufsichtigten Institutionen sei eine solche Kontrolle auch gar nicht realisierbar.[970]

Auch die Finanzkontrolle machte gegenüber der PUK Datensicherheit klar, dass das Thema Informationssicherheit nicht primär im Fokus der Finanzkontrolle stehe und sie dort nicht relevant unterwegs sei, dies auch aufgrund der Aufgabenabgrenzung gegenüber der Datenschutzbeauftragten.[971]

14.5.1 Rolle der Datenschutzbeauftragten

Die Datenschutzbeauftragte nimmt, neben einem allgemeinen Monitoring zu den technischen Entwicklungen und dem diesbezüglich datenschutzrechtlich korrekten Umgang, auch konkrete Kontrollen nach § 35 IDG vor, bei denen sie von den öffentlichen Organen Auskunft über die bearbeiteten Daten verlangt. Nach Untersuchungen vor Ort werden Massnahmen vorgeschrieben und deren Umsetzung geprüft. Diese Kontrollen sind wichtig und die Datenschutzbehörde hat in den letzten Jahren ihre Anstrengungen im Bereich der Informationssicherheit intensiviert. Die Datenschutzbehörde hat aber auch die Aufgabe der Beratung, Information und Sensibilisierung.[972]

14.5.2 Rolle der Finanzkontrolle

Die Finanzkontrolle betonte im Rahmen der Befragung durch die PUK Datensicherheit, dass sie zwar Prüfungen im Bereich der Informatik mache, weil diese eine Nahtstelle zu den finanziellen Fragen darstelle, sie sehe dies jedoch nicht als ihre Kernaufgabe.[973] Auch aufgrund des sehr breiten Aufsichtsbereichs –Kernverwaltung, selbständige und externe Anstalten – könne die Finanzkontrolle nicht regelmässig relevante IT-Prüfungen vornehmen.[974] Die Berichte der Finanzkontrolle gingen zudem nur an den im Finanzkontrollgesetz definierten Adressatenkreis. Organisationen, wie beispielsweise das Personalamt, die für die gesamte kantonale Verwaltung Querschnittsfunktionen übernehmen, seien somit nicht über Mängel informiert, die in ihrem Bereich in den einzelnen Ämtern festgestellt werden. Auch der ISIK werde nicht zwingend über entsprechende Feststellungen der Finanzkontrolle in Kenntnis gesetzt. Es hänge massgeblich davon ab, ob innerhalb der Finanzdirektion eine entsprechende Weiterleitung erfolge.[975]

14.6 Rolle der parlamentarischen Aufsichtskommissionen

Den Aufsichtskommissionen des Kantonsrates kommt auch die Oberaufsicht über die Umsetzung der Informationssicherheit zu. Dabei sind sie einerseits auf entsprechende Informationen und Hinweise angewiesen; beim konkreten Datensicherheitsvorfall hat sich gezeigt, dass eine einmalige Information im Rahmen eines Referentengespräches nicht ausreicht. Andererseits sind diese Themen durch die Aufsichtskommissionen aber entsprechend zu beachten, aktiv zu begleiten und dem Kantonsrat in geeigneter Form zur Kenntnis zu bringen.

---

970 Protokoll der Befragung von Dominika Blonski vom 22. November 2024, S. 14–15.

971 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 8.

972 Protokoll der Befragung von Dominika Blonski vom 26. Januar 2024, S. 24; Stellungnahme von Dominika Blonski vom 10. November 2025.

973 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 18.

974 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 23.

975 Protokoll der Befragung von Martin Billeter und Daniel Strebel vom 5. Juli 2024, S. 21.

Aus Sicht der PUK Datensicherheit ist es angezeigt, dass die jeweils zuständigen Aufsichtskommissionen den Fragen der Informationssicherheit in ihrem Bereich ausreichend Bedeutung beimessen. Ein Beispiel hierzu ist die Informationssicherheit bei den Gerichten. Die PUK Datensicherheit selbst hat sich im Rahmen ihrer Abklärungen nicht damit befasst. Die Frage der Informationssicherheit ist jedoch insofern von Relevanz, als im Verlauf eines Strafverfahrens die gleichen Akten von der Kantonspolizei, die im Bereich der Informationssicherheit eigenständig ist, über die in der JI verorteten Staatsanwaltschaften schliesslich zu den Gerichten gehen. Folglich muss die Informationssicherheit in allen drei Kontexten in gleicher Weise gewährleistet sein.

14.7 Würdigung durch die PUK

Rechtliche und strategische Grundlagen

Die PUK Datensicherheit ist der Ansicht, dass die wesentlichen organisatorischen Zuständigkeiten auf Verordnungsstufe zu regeln sind, da sich die Verwaltung in ihrer Arbeitsweise an den rechtlichen Grundlagen orientiert. Bei der wichtigsten Grundlage der Informationssicherheit, der AISR, handelt es sich um eine vom Regierungsrat verbindlich erklärte Richtlinie und keine Verordnung. Die themenspezifisch wesentlichen Regelungen sind in den BISR geregelt.

Die PUK Datensicherheit sieht die konsequente Anlehnung an den internationalen Standard positiv. Angesichts der Fülle an BISR-Regelungen ist es aus ihrer Sicht jedoch unabdingbar, dass diese Regelungen weiter konkretisiert und fassbar gemacht werden. Dies hat aus Sicht der PUK Datensicherheit über alle Direktionen und die Staatskanzlei im Grundsatz koordiniert zu erfolgen.

Die PUK Datensicherheit stellt fest, dass sich die heutigen kantonalen Anstrengungen im Bereich der Informationssicherheit aus verschiedenen rechtlichen und strategischen Grundlagen speisen. So legt die AISR zwar die Ausgestaltung der kantonalen Informationssicherheit fest, wesentliche Impulse zu deren Weiterentwicklung gingen aber von der Cybersicherheitsstrategie aus. Schliesslich schaffte die aktuelle IKT-Governance mit dem Dreischichtenmodell und den dazugehörigen Gremien eine wesentliche Basis für die heutige Umsetzung der Informationssicherheit. Aus Sicht der PUK Datensicherheit bietet die laufende Überführung der IKT-Strukturen in eine Verordnung die Gelegenheit, auch die Verantwortlichkeiten im Bereich der Informationssicherheit im Einklang mit der neuen IKT-Verordnung festzuschreiben.

Neben diesen kantonalen Grundlagen existieren parallel auch die Informationssicherheitsbestrebungen der KAPO sowie der Digitalisierung der Schulen der SEK II. Die laufende digitale Transformation mit ihrer Vielzahl an Projekten basiert auf der Strategie Digitale Verwaltung 2018–2025, die mit der Strategie Digitale Verwaltung 2025+ eine Erneuerung erfahren hat. Die PUK Datensicherheit begrüsst es, dass die KAPO ihre IT-Projekte freiwillig dem Gremium Operative Informatiksteuerung (OIS) vorlegt und sich so mit den kantonalen Entwicklungen koordiniert. Aus Sicht der PUK Datensicherheit gilt es diese Praxis nun auch verbindlich festzulegen. Die Zusammenarbeit der KAPO mit dem OIS ist zu formalisieren.

Die PUK Datensicherheit fordert dazu auf, die strategischen Herausforderungen der Digitalisierung gesamtheitlich zu betrachten und angesichts der Vielzahl strategischer Grundlagen in diesem Bereich eine Klärung herbeizuführen, die Grundlagen zu vereinheitlichen und unter Berücksichtigung des Aspekts der Informationssicherheit

zusammenzuführen.[976] Denn für eine erfolgreiche Digitalisierung braucht es auch klare strategische Abwägungen und Grundlagen zur Informationssicherheit. So betont auch die Datenschutzbeauftragte in ihrem Jahresbericht 2024 die Notwendigkeit, sich angesichts des laufenden technologischen Wandels mit dessen Auswirkungen auf die Gesellschaft und die Grundrechte zu befassen.[977]

In Bezug auf die Strategie Digitale Verwaltung 2025+ begrüsst die PUK Datensicherheit einerseits ausdrücklich das Ziel der Generalsekretärenkonferenz (GSK), auf gemeinsame Lösungen hinzuwirken. Anderseits stellt sie fest, dass im Bereich der Informationssicherheit aktuell keine kantonalen Vorgaben, beispielsweise in der AISR, bestehen, welche eine Koordinierung der direktionalen Informationssicherheitsbestrebungen oder eine gemeinsame Erarbeitung von Prozessen vorsehen. Diese fehlende gemeinsame Herangehensweise widerspiegelt sich auch in der geringen Anzahl gesamtkantonaler Leitfäden. Es darf aus Sicht der PUK Datensicherheit nicht sein, dass die einzelnen Direktionen und die Staatskanzlei die BISR-Vorgaben entweder nicht konkretisieren oder unterschiedlich umsetzen. Damit die Umsetzung einheitlich erfolgt und keine Doppelspurigkeiten bestehen, ist zwingend eine arbeitsteilige, koordinierte Vorgehensweise vorzusehen.

Die neue AISR illustriert die weiterhin starken Autonomiebestrebungen in den Direktionen und der Staatskanzlei. Sie sieht vor, dass die Direktionen eigene AISR auf der Ebene der Direktion oder der Staatskanzlei erlassen. Die PUK Datensicherheit findet dieses zweistufige Vorgehen in der heutigen Form verfehlt und nicht zielführend. Es ist zu verwerfen. Dieses Vorgehen erinnert an die gescheiterte Umsetzung der Informatikstrategie 2008, welche die Direktionen und die Staatskanzlei dazu verpflichtet hatte, eigene Informatikstrategien zu erlassen. Dabei kam es zu starken Verzögerungen und schliesslich zum Scheitern der Informatikstrategie mit weitreichenden negativen Auswirkungen auch auf den Informationssicherheitsbereich. Das Silodenken mit Fokus auf die eigene Direktion muss gerade im Bereich der Informationssicherheit überwunden werden, wobei nötigenfalls auch die rechtlichen Grundlagen anzupassen sind, namentlich die Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung[978], die mit § 60 Abs. 1 lit. e die Zuständigkeit für die Regeln zur Umsetzung des IDG auf der Direktionsebene und nicht auf der kantonalen Ebene verortet. Hier sieht die PUK Datensicherheit deshalb den Gesamtregierungsrat und das SDI in der Pflicht, die Umsetzung der AISR eng zu begleiten und weitgehende kantonale Vorgaben zu machen.

Sicherheitsorganisation

Zwar wurde die Stelle des ISIK bereits 2015 geschaffen und die FAGIS hatte sogar schon länger bestanden. Das Kompetenzzentrum Informatiksicherheit, bestehend aus ISIK und FAGIS, führte aber lange Jahre eher ein Nischendasein. Die Informationssicherheit kam erst mit der Schaffung der ISID (RRB Nr. 1193/2020), dem Expertenpool «Informationssicherheit» (RRB Nr. 811/2021) und den Massnahmen der Cybersicherheitsstrategie (RRB Nr. 676/2022) in Schwung. Die PUK Datensicherheit an-

[976] Zum Zeitpunkt des Berichts der IKT-Subkommission der Geschäftsprüfungs- und der Finanzkommission zur Umsetzung der kantonalen IKT-Strategie und der Strategie Digitale Verwaltung 2019–2023 vom 23. März 2023 war noch unklar, wie sich die Koordination der IKT-Strategie und der Strategie Digitale Verwaltung 2018–2023 im Rahmen der Strategischen Initiativen weiterentwickelt (KR-Nr. 67/2023, S. 27).

[977] Datenschutzbeauftragte des Kantons Zürich, Tätigkeitsbericht 2024 «Welche Zukunft für den Datenschutz im Kanton Zürich?».

[978] Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung vom 18. Juli 2007 (VOG RR; LS 172.11).

erkennt, dass der Regierungsrat seit 2020 mit dem Erlass der AISR, der Bereitstellung von Ressourcen sowie der Umsetzung der Cybersicherheitsstrategie gewisse Anstrengungen unternommen hat und Verbesserungen sichtbar werden. Infolge des Fachkräftemangels verzögert sich der weitere personelle Ausbau des kantonalen Zentrums für Cybersicherheit jedoch. Das Versäumnis, dass der Regierungsrat 2015 den Weg zu einer kantonalen Sicherheitsorganisation nicht konsequent weitergegangen ist, lässt sich wohl nicht mehr wettmachen.

Direktionale Sicht auf die Informationssicherheit

Die PUK Datensicherheit muss ernüchtert erkennen, dass trotz der positiven Signale aus der Generalsekretärenkonferenz (GSK) in den Direktionen und der Staatskanzlei weiterhin starke Vorbehalte gegen eine zentrale Herangehensweise vorherrschen. So hat mit der neuen AISR eine Schwächung der kantonalen Rolle der ISID stattgefunden. Für die PUK Datensicherheit ist aber zentral, dass diese Positionen nicht der IT-Leitung unterstellt sind, und zwar in allen Direktionen und der Staatskanzlei. Vielmehr sind sie in der Nähe der Direktionsleitung oder der Generalsekretärinnen bzw. Generalsekretäre anzusiedeln. Überdies ist, wie in der neuen AISR vorgesehen, eine Berichterstattung über die Informationssicherheitsrisiken an die Leitung einzurichten. Weiter ist die Position der ISID gegenüber den Amtsleitungen mit einem Weisungsrecht im Bereich der Informationssicherheit zu stärken.

Die PUK Datensicherheit unterstützt das im Rahmen der neuen IKT-Verordnung angedachte Weisungsrecht für das AFI im Bereich der Grundversorgung ausdrücklich und fordert dessen Implementierung. Überdies hält es die PUK Datensicherheit für angezeigt, auch den ISIK im Bereich der direktionsübergreifenden Informationssicherheit mit einem Weisungsrecht auszustatten. Weiter müssen die organisatorische Unabhängigkeit des ISIK und dessen Kompetenzen so ausgestaltet sein, dass er seine Aufgabe in der gesamten kantonalen Verwaltung erfüllen kann. Es ist für die PUK Datensicherheit nicht nachvollziehbar, warum der Regierungsrat die Stärkung dieser zentralen Position mit einem Weisungsrecht als eine Schwächung sieht.

Aus Sicht der PUK Datensicherheit ist es beim wichtigen Thema der Informations- und Cybersicherheit nicht angebracht, auf dem eigenen Machtbereich zu beharren und eigenständige Lösungen zu forcieren. Desillusioniert stellt die PUK Datensicherheit fest, dass die einzelnen Regierungsrätinnen und Regierungsräte dem Erhalt des eigenen Einflussbereichs gegenüber der wichtigen gesamtheitlichen Betrachtung und Umsetzung der Informationssicherheit immer noch Priorität einräumen. Die PUK Datensicherheit kann sich vorstellen, dass vor diesem Hintergrund künftig auch eine gemeinsame Zuständigkeit für das Amt für Informatik (AFI) oder eine andere Verortung des AFI zu prüfen wären.

Schliesslich konnte die PUK Datensicherheit feststellen, dass dem Gremium FAGIS innerhalb der IKT-Governance keine wesentliche Rolle zukommt. Es ist vielmehr das Gremium OIS, bei dem die Fäden im operativen Bereich der Informatik direktionsübergreifend zusammenlaufen. Um die Informationssicherheit auch auf der Ebene der einzelnen Informatikprojekte zu stärken, ist es unabdingbar, dass die Stimme des FAGIS im Gremium OIS stärker Gehör findet. Für die PUK Datensicherheit muss geprüft werden, wie der Zugang der FAGIS zu diesem Gremium besser ausgestaltet werden kann.

Die heutigen Governance-Strukturen sind nach dem Eindruck der PUK Datensicherheit äusserst komplex ausgestaltet und speisen sich aus unterschiedlichen Quellen und Vorgaben. Sie sind für Aussenstehende, aber auch Mitarbeitende der kantonalen Verwaltung in dieser Art nur schwer nachvollziehbar. Für eine wirkungsvolle Umsetzung der Informationssicherheit fordert die PUK Datensicherheit eine Vereinfachung und Klärung der Strukturen.

Kantonale Dienstleistungen

Den Aufbau der kantonalen Dienstleistungen nimmt die PUK Datensicherheit positiv zur Kenntnis. Aus ihrer Sicht sind jedoch kantonal bereitgestellte Dienstleistungen für alle Direktionen verpflichtend auszugestalten. Dies bedingt jedoch, wie die PUK Datensicherheit beim kürzlich erfolgten Entsorgungsprozess von Datenträgern im Rahmen des DAP-Rollouts feststellen konnte, dass bei der Erarbeitung dieser gesamtkantonalen Prozesse auch die Bedenken der Direktionen und der Staatskanzlei berücksichtigt werden.

Interne Audits und externe Aufsicht

Die PUK Datensicherheit hegt starke Bedenken, dass durch die in der neuen AISR geregelte Autonomie der Direktionen und der Staatskanzlei vergleichbare Informationsgrundlagen in ausreichender Qualität bereitstehen, um die Informationssicherheitsrisiken aus einer gesamtkantonalen Sicht betrachten und entsprechend risikobasiert handeln zu können.

Die PUK Datensicherheit sieht hier das SDI in der Pflicht, dafür zu sorgen, dass auf Grundlage der in den Direktionen und der Staatskanzlei erhobenen Informationen eine gesamtkantonale Steuerung möglich ist. Nur mit einer gesamtkantonalen Sicht ist ein effizienter Ressourceneinsatz dort möglich, wo er aufgrund der Risiken angezeigt ist.

Dazu sind auch die Direktionen in der Pflicht, ihre eigenen Risiken mittels individueller Audits regelmässig zu eruieren. Die von der Finanzkontrolle und der Datenschutzbeauftragten vorgenommenen Prüfungen ersetzen eine solche selbständige Prüfaktivität keineswegs.

Risiken von Cloud-Lösungen für die Informationssicherheit

Die PUK Datensicherheit teilt die Bedenken der Datenschutzbehörde in Bezug auf die Cloud-Lösung M365 und sieht in der Tat hohe Risiken, dass – auch infolge der veränderten geopolitischen Situation – Daten von Einwohnerinnen und Einwohnern bzw. von Unternehmen im Rahmen des CLOUD Act gegenüber dem US-amerikanischen Staat offengelegt werden müssen. Diese Risiken sind sehr ernst zu nehmen, und der Regierungsrat hat vertieft zu prüfen, ob eine Ablösung von M365 anzustreben ist. Generell ist darauf zu achten, dass sich die Daten sowohl auf Servern im Inland befinden als auch individuell verschlüsselt und zudem wirkungsvoll vor fremdem Zugriff geschützt sind.

Vor dem Hintergrund dieser Risiken ist es unabdingbar, dass die Klassifizierung, Nutzung und Speicherung der Daten heute in allen Direktionen und der Staatskanzlei sorgfältig vorgenommen werden. Dabei ist die Allgemeine Nutzungsrichtlinie[979] zu beachten, welche die Nutzung und Speicherung von vertraulichen und geheimen Daten sowie von besonderen Personendaten auf der M365-Cloud explizit verbietet. Die Mitarbeitenden sind diesbezüglich stärker als heute durch die Direktionen und die Staatskanzlei zu sensibilisieren und zu unterstützen. Dabei sind klare, verständliche Regelungen festzulegen und kantonale Hilfsmittel, auch technischer Art, zu entwickeln.

Ergänzend dazu ist der Umgang mit Cloud-Lösungen stärker als bisher durch die Aufsichtskommissionen kritisch zu begleiten.

Stärkung der externen Aufsicht über die Informationssicherheit

In dieser Hinsicht stellte die PUK Datensicherheit fest, dass weder die Finanzkontrolle noch die Datenschutzbeauftragte aufgrund ihrer Ausrichtung sowie der Breite ihrer Zuständigkeit die Informationssicherheit regelmässig prüfen können. Bei der Finanz-

[979] Kanton Zürich, Finanzdirektion, Amt für Informatik, Allgemeine Nutzungsrichtlinie Microsoft 365 vom 1. Februar 2023.

kontrolle liegt der Fokus natürlicherweise auf den finanziellen Fragen. Der Datenschutzbeauftragten wiederum erlaubt es die Breite ihrer Aufsichtszuständigkeit, die auch die Gemeinden und zum Teil die Kirchen umfasst, die Entwicklung in den Direktionen und der Staatskanzlei nur mit einem risikobasierten Ansatz zu begleiten. Gemäss dem Entwurf für das totalrevidierte IDG soll die Datenschutzbehörde nun zusätzlich die Funktion der Öffentlichkeitsbeauftragten übernehmen.

Die externe Aufsicht über die Informationssicherheit ist aus Sicht der PUK Datensicherheit wesentlich zu stärken. Allenfalls ist hierfür – über die bestehenden Organe hinaus – eine externe Aufsicht über die Informationssicherheit in der kantonalen Verwaltung einzurichten. Ergänzend zur Weiterführung der externen Audits zur kantonalen Informationssicherheit, wie sie heute in der AISR vorgesehen sind, sieht die PUK Datensicherheit drei Möglichkeiten, um die Aufsicht im Bereich der Informationssicherheit zu stärken:

a) Die Verstärkung der Kontrollaktivität der Datenschutzbehörde im Bereich der Informationssicherheit und eine Neugestaltung der diesbezüglichen Berichterstattung gegenüber den Aufsichtskommissionen. Auf diese Weise wäre es auch mit dem heute risikobasierten Ansatz besser möglich, die Direktionen, die Staatskanzlei und die selbständigen öffentlich-rechtlichen Anstalten zu beraten und zu prüfen.
b) Die Stärkung der Ressourcen und Möglichkeiten der Finanzkontrolle für Prüfungen im Bereich der Informationssicherheit, die aktuell nicht zum Kerngeschäft der Finanzkontrolle gehört. Dazu müsste der bestehende gesetzliche Auftrag entsprechend erweitert werden. Allenfalls ist auch eine Erweiterung des Adressatenkreises der Berichterstattung der Finanzkontrolle zu prüfen, damit jene kantonalen Stellen, die direktionsübergreifend wirken, namentlich der ISIK und das Kompetenzzentrum Informationssicherheit, diese Informationen ebenfalls erhalten.
c) Die Schaffung einer neuen, unabhängigen Instanz zur Informationssicherheitskontrolle, welche die externe Aufsicht in diesem Bereich wahrnimmt und zuhanden der Aufsichtskommissionen berichtet.

Wesentliche Erkenntnisse und Informationen zur kantonalen Informationssicherheit sind den Aufsichtskommissionen in geeigneter Form zugänglich zu machen. Analog zur von der Finanzkontrolle vorgeschlagenen Berichterstattung über alle relevanten IT-Schlüsselprojekte[980] ist auch zu den Informationssicherheitsrisiken der Direktionen und der Staatskanzlei eine halbjährliche oder jährliche Berichterstattung einzurichten, die ebenfalls die Bedürfnisse der exekutiven Dienstaufsicht und der parlamentarischen Oberaufsicht erfüllt. Weiter ist vertieft zu prüfen, ob die Auditberichte sowie die internen Berichte der Datenschutzbeauftragten, ähnlich den Semesterberichten der Finanzkontrolle, den Aufsichtskommissionen zur Kenntnis gebracht werden sollen. Die PUK Datensicherheit erinnert die Aufsichtskommissionen des Kantonsrates dringend daran, die Umsetzung der Informationssicherheit im Rahmen der begleiteten Oberaufsicht engmaschig zu verfolgen. Dafür hat der Kantonsrat eine wirksame Oberaufsicht durch seine bisherigen Strukturen oder gegebenenfalls durch eine neu zu schaffende Aufsichtskommission für IT-Projekte und Informationssicherheit sicherzustellen.

[980] Finanzkontrolle Kanton Zürich, Bericht zur Aufsichtsprüfung bei der Direktion der Justiz und des Innern (JI) vom 10. Juni 2025, S. 5.

15. Stand der Informationssicherheit in den Direktionen und der Staatskanzlei

15.1 Einleitung

Im Rahmen ihrer Untersuchungen hatte die PUK Datensicherheit einerseits abzuklären, ob die Informationssicherheit in der kantonalen Verwaltung gewährleistet ist, und andererseits zu prüfen, ob die Datenvernichtung in der kantonalen Verwaltung generell ausreichend dokumentiert wird. Dazu verlangte sie am 22. Januar 2025 schriftlich Auskünfte von den Informationssicherheitsbeauftragten der Direktionen und der Staatskanzlei (ISID). Sie liess sich über die geltenden direktionsinternen Vorgaben, die Funktion und Tätigkeit des ISID sowie gezielt zu den Prozessen in Bezug auf die Sicherheits- und Lieferantenprüfung sowie die Ausserbetriebnahme von Geräten informieren. Abschliessend erkundigte sie sich nach den direktionsinternen Schulungs- und Audittätigkeiten.[981] Ergänzend zu diesen Auskünften stützte sie sich bei ihren Abklärungen auf die Erkenntnisse der kantonalen Audits aus den Jahren 2021 und 2023.[982]

15.2 Direktionsinterne Grundlagen

Im Bereich der Informatik, Informationsverwaltung und Informationssicherheit haben die Direktionen und die Staatskanzlei verschiedene eigene Weisungen erlassen.

Jene Weisungen und Richtlinien, die sich mit der Informationssicherheit im engeren Sinne befassen, stehen oftmals noch in einem engen Konnex zur Informatik und ersetzen teilweise diesbezügliche frühere Vorgaben (Tabelle 19). Ergänzend dazu bestehen auch strategische Grundlagen, die Informationssicherheitsvorgaben enthalten. Künftig sollen gemäss der neuen AISR alle Direktionen und die Staatskanzlei über eine eigene Allgemeine Informationssicherheitsrichtlinie (AISR-DIR/SK) verfügen. In der Finanzdirektion liegt der Entwurf für die Allgemeine Informationssicherheitsrichtlinie FD heute bereits vor.

Tabelle 19 Weisungen und Vorgaben zum Umgang mit Informatikmitteln und zur Informationssicherheit

SK	Weisung zum Umgang mit Informationen vom 16. März 2023[983] Richtlinie Integrale Sicherheit der Staatskanzlei des Kantons Zürich vom 10. Oktober 2023 Sicherheitsstrategie der Staatskanzlei 2024–2028 vom 13. August 2024
JI	Verordnung über die Datenbearbeitung der Direktion der Justiz und des Innern (LS 172.110.11)
DS	Weisung zum Umgang mit Informationen vom 24. Juni 2024
FD	Entwurf «Allgemeine Informationssicherheitsrichtlinie FD»
VD	Informationssicherheits-Weisung vom 12. Oktober 2021[984]

[981] Antwortschreiben des Beauftragten Integrale Sicherheit SK vom 17. Februar 2025; Antwortschreiben des ISID JI vom 19. Februar 2025; Antwortschreiben des ISID DS vom 20. Februar 2025; Antwortschreiben des ISID FD vom 20. Februar 2025; Antwortschreiben des ISID GD vom 20. Februar 2025; Antwortschreiben der ISID BI vom 20. Februar 2025; Antwortschreiben des ISID BD vom 17. Februar 2025.

[982] Finanzdirektion, Amt für Informatik, Audits Informationssicherheit Organisation ISMS vom 9. Dezember 2021 und vom 31. August 2023.

[983] Eine frühere Version lag mit der Weisung über die Nutzung von Informatikmitteln (Informatikweisung) vom 1. September 2017 vor.

[984] Volkswirtschaftsdirektion Informationssicherheits-Weisung vom 12. Oktober 2021. Frühere Versionen davon waren die Weisung zur Nutzung von Informatikmitteln (Informatikweisung) vom 1. Januar 2015, die Informatik-Weisung vom 12. März 2002 sowie jene vom 5. Juni 2000.

GD	Informatik-Sicherheit Benutzer Richtlinien vom März 2023 Substrategie FachApp-Security (Informationssicherheit bei Fachapplikationen)
BI	Richtlinien zur Nutzung der Informatik in der Bildungsdirektion Kanton Zürich vom 22. Januar 2019
BD	Informationssicherheit Kanton Zürich Nutzungsrichtlinie Baudirektion vom 28. März 2022[985]

Weitere direktionale Weisungen machen Vorgaben dazu, wie Informationen zu verwalten und die Geschäftsverwaltungssysteme (GEVER) zu nutzen sind (Tabelle 20).

Tabelle 20 Weisungen zum Umgang mit Informationen (Informationsverwaltung)

SK	Vorschriften über die Geschäftsverwaltung der Staatskanzlei vom 27. September 2016 (Auflage vom 17. März 2025)
JI	Vorschriften über die Geschäftsverwaltung der Direktion der Justiz und des Innern vom 10. Juli 2019
DS	–
FD	–
VD	–
GD	Weisung zur Nutzung M365 in der GD (derzeit in Umsetzung)
BI	Weisung zur Informationsverwaltung in der Bildungsdirektion vom 22. Februar 2024[986]
BD	Organisationsvorschriften zur Verordnung über die Informationsverwaltung und -sicherheit. Gültig ab 1. Juni 2022

Neueren Datums sind schliesslich die Weisungen und Vorgaben zur Klassifizierung von Informationen (Tabelle 21).

Tabelle 21 Vorgaben zur Klassifizierung von Informationen

SK	Leitfaden Klassifizierung von Informationen vom 16. März 2023
JI	Weisung Microsoft 365 (M365)
DS	Weisung zum Umgang mit Informationen vom 24. Juni 2024
FD	Leitfaden: Informationsklassifikation vom 19. Dezember 2022
VD	–
GD	Dokumente zur Informationsklassifikation auf der Intranetseite GD (Erläuterung vom 26. April 2024, Klassifikationsbeispiele GD vom 30. April 2024, Handhabung der verschiedenen Klassifikationsstufen vom 3. Mai 2024)
BI	Leitfaden Klassifizierung von Informationen in der Bildungsdirektion vom 27. Juni 2024
BD	Informationssicherheit Kanton Zürich Nutzungsrichtlinie Klassifizierung vom 16. Dezember 2024

Quelle: Obige Tabellen enthalten jene Dokumente, welche der PUK Datensicherheit im Rahmen der Befragung oder durch die ISID zur Kenntnis gebracht wurden oder auf der Intranetseite verfügbar waren.

Die letztgenannten Regelungen sind im Kontext der Allgemeinen kantonalen Nutzungsrichtlinie «Microsoft 365» vom 1. Februar 2023 zu sehen. Denn gemäss dem dazugehörigen RRB Nr. 542/2022 sind die Direktionen und die Staatskanzlei beauftragt, zu beurteilen, ob der Erlass einer ergänzenden organisationsspezifischen Regelung zu dieser Richtlinie, beispielsweise mit Bezug auf die verschiedenen Arten von Geschäften gemäss ihrem Ordnungssystem und im Hinblick auf die Nutzung von M365, notwendig ist.[987]

[985] Die Nutzungsrichtlinie ersetzte die Informatik-Weisung vom 1. Februar 2011.

[986] Eine frühere Version lag mit der Weisung zur Informationsverwaltung in der Bildungsdirektion vom 7. Mai 2020 vor.

[987] RRB Nr. 542/2022 vom 30. März 2022, Einsatz von Cloud-Lösungen in der kantonalen Verwaltung, (Microsoft 365), Zulassung.

Zusätzlich existieren auch auf der Ebene der Ämter weitere Vorgaben. Es besteht hier noch keine Einheitlichkeit. So schreibt beispielsweise der ISID der GD in seiner Antwort, dass mit dem geplanten Ausbau der Informationssicherheit auch Doppelspurigkeiten mit den Ämtern abgebaut und weitere Themen einheitlicher geregelt werden sollen.[988] Schliesslich gibt es je nach Aufgabe der Ämter auch zusätzliche Vorgaben des Bundes, die zu beachten sind.[989]

15.3 Sicherheitsorganisation

Dreh- und Angelpunkt der Informationssicherheit in den Direktionen und der Staatskanzlei sind die ISID. Hierzu hielt der Auditbericht 2021 fest, dass die Staatskanzlei und fünf von sieben Direktionen die direktionsinterne Stelle des ISID zeitnah besetzt hatten. Zwei ISID-Stellen waren zu diesem Zeitpunkt noch vakant, womit gemäss dem Audit eine fundamentale Voraussetzung für die Informationssicherheit noch nicht erfüllt war.[990] Bei der Finanz- und der Gesundheitsdirektion übten die Informatikleiter diese Aufgabe noch aus. Natürlich war die Gesundheitsdirektion damals durch die Corona-Pandemie stark belastet. Auch im Audit 2023 wurde noch festgestellt, dass die Rekrutierung inzwischen zwar angelaufen sei, aber bis dahin immer noch bisherige Mitarbeitende die ISID-Rolle in Teilfunktion übernehmen müssten.[991]

Mit Blick auf die Governance stellte die PUK Datensicherheit fest, dass die ISID innerhalb der Direktionen in unterschiedlichen Abteilungen und Hierarchiestufen angesiedelt wurden. Es kommt vor, dass die ISID-Stelle innerhalb der direktionseigenen Informatik vier oder fünf Stufen unterhalb der Direktionsleitung angesiedelt ist. Die Staatskanzlei oder die JI wiederum haben die ISID-Stelle bewusst ausserhalb der Informatik angesiedelt. Bei der Finanzdirektion und der Baudirektion ist der ISID direkt dem Generalsekretär unterstellt.

Auch bei der Berichterstattung bestehen Unterschiede. Zum Zeitpunkt der Befragung durch die PUK Datensicherheit im Dezember 2024 war noch nicht überall eine Berichterstattung über die Informationssicherheitsrisiken zuhanden der Direktionsleitung oder der Geschäftsleitung der Direktion implementiert. Nach Auskunft der ISID ist aktuell meist eine Berichterstattung an die Geschäftsleitung der Direktion respektive der Staatskanzlei oder gegenüber Strategiegremien eingerichtet. Weiterhin kommt es aber vor, dass ausschliesslich an den Generalsekretär berichtet wird. Dies wird mit der neuen AISR nicht mehr möglich sein. Teilweise kennen die Direktionen auch weitere Gremien, in denen unterschiedliche Personen u. a. bei Fragen der Informationssicherheit vernetzt sind.

- Abteilung Business Support & Compliance (JI)
- IKT-Strategiegremium (DS, VD)
- Security Board (BD)
- Vernetzungsgruppe des Generalsekretärs der GD mit den Digitalisierungsverantwortlichen der kantonalen Spitäler und Psychiatrien

---

988 Antwortschreiben des ISID GD vom 20. Februar 2025.

989 So namentlich die Vorgaben des SECO für das Amt für Arbeit der Volkswirtschaftsdirektion.

990 Finanzdirektion, Amt für Informatik, Audit Informationssicherheit Organisation ISMS vom 9. Dezember 2021, S. 7–8.

991 Finanzdirektion, Amt für Informatik, Audit Informationssicherheit Organisation ISMS vom 31. August 2023, S. 30.

15.4 Umsetzung der Informationssicherheit

15.4.1 Aufbau eines ISMS und Risikomanagements

Aus den Antworten der ISID geht hervor, dass für die meisten Informationssicherheitsbeauftragten der (weitere) Aufbau des Informationssicherheits-Managementsystems (ISMS), Schulungen, der Umgang mit Vorfällen, die Unterstützung der Informationssicherheit in den Projekten (Informationssicherheits- und Datenschutzkonzepte) sowie das direktionsinterne Risikomanagement wichtige Aufgaben darstellen. Die Befragungen der ISID im Rahmen der Informationsbeschaffungsphase vermittelten der PUK Datensicherheit ein Bild darüber, wie aufwendig es ist, alle schützenswerten Objekte zu identifizieren, deren Schutzbedarf zu eruieren, entsprechende Massnahmen zu erarbeiten und diese dann umzusetzen. Allgemein lässt sich sagen, dass die verschiedenen ISID in ihren Direktionen und der Staatskanzlei zwar mit Blick auf die ISMS einiges bewegt und Fortschritte erzielt haben, dass aber zur Umsetzung der Informationssicherheit in allen Direktionen noch Wesentliches geleistet werden muss. Dies zeigt sich auch darin, dass der Regierungsrat mit dem Erlass der neuen AISR auch Ressourcen für die Umsetzung der BISR gesprochen hat.

So besteht gemäss dem Auditbericht 2023 keine durchgängige Sicht auf die eingesetzten IKT-Infrastrukturelemente, wodurch auch eine abschliessende Klassifikation des Inventars in Bezug auf Kritikalität, Sicherheitsparameter oder Ausfallszeiten nicht sichergestellt werden könne. Weiterhin gelte es auch die Erarbeitung und Umsetzung von ISDS-Konzepten und Berechtigungskonzepten konsequent weiterzuführen. Der Auditbericht empfahl, die Informationssicherheit mit entsprechenden Sicherheitsmassnahmen, der Umsetzung der Prozesse und einem unterstützenden, standardisierten Kontrollkatalog zur effizienten BISR-Umsetzung zu verbessern.[992]

Die Antworten zeigen, dass die Direktionen und die Staatskanzlei keinen standardisierten Kontrollkatalog nutzen. In Bezug auf die eingesetzten Mittel stellte die PUK Datensicherheit fest, dass die Direktionen und die Staatskanzlei mit unterschiedlichen Applikationen und Tools arbeiten, die eine Übersicht zu den Risiken und Massnahmen erlauben sollen.[993]

15.4.2 Sicherheitsüberprüfungen

Aus den Antworten der ISID ging hervor, dass sich die Direktionen und die Staatskanzlei bei den Sicherheitsüberprüfungen auf die BISR 5 («Richtlinie für Personalsicherheit») und BISR 22 («Richtlinie für Beziehungen zu externen Personen, insbesondere Liefernden») abstützen. Sie machten nur vereinzelt weitere Angaben zu direktionsinternen Prozessen und Vorgaben. Der ISID der FD wies zusätzlich darauf hin, dass der Regierungsrat mit RRB Nr. 1462/2022[994] festgehalten habe, dass im Bereich der Personensicherheitsprüfungen eine Präzisierung der Rechtsgrundlagen abzuklären sei. Denn gemäss dem Informationssicherheitsgesetz des Bundes hat der Kanton Zürich eine mindestens gleichwertige Informationssicherheit zu gewährleisten.[995]

---

[992] Finanzdirektion, Amt für Informatik, Audit Informationssicherheit Organisation ISMS vom 31. August 2023, S. 4.

[993] So sind das Digital Security Control Center (DSC2), Governance, Risk und Compliance-Tools oder Security Dashboards in Anwendung. Weiter sollen Prozesslandkarten oder Statements of Applicability (SoA) aufgebaut werden.

[994] RRB Nr. 1462/2022 vom 9. November 2022, Ausführungsrecht zum Informationssicherheitsgesetz (Vernehmlassung).

[995] Art. 3 Abs. 2 des Bundesgesetzes vom 18.Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG, SR 128).

15.4.3 Lieferantenüberprüfungen

Aus den Antworten der ISID wird ersichtlich, dass sich die Überprüfung der Lieferanten von Fachapplikationen auf die BISR 20 («Richtlinie für die Sicherheit in Entwicklungs- und Unterstützungsprozessen»), BISR 21 («Richtlinie für die Sicherheit von Testdaten») und BISR 22 («Richtlinie für Beziehungen zu externen Personen, insbesondere Liefernden») stützen. Ergänzend gab der ISID der FD an, dass gewisse Ämter dezidierte Funktionen für das Lieferantenmanagement definiert hätten. In der Staatskanzlei würden auf Basis einer Risikoanalyse zur Leistungserbringung Anforderungskataloge genutzt, welche die Richtlinien konkretisierten, und in der Baudirektion würden Assessments zur Prüfung von Leistungserbringern implementiert. Darüber hinaus wurden aber keine konkreten direktionsinternen Prozesse zur Lieferantenüberprüfung angeführt.

15.4.4 Schulungen

In Bezug auf die Schulungen in den Direktionen und der Staatskanzlei ging hervor, dass Informationssicherheits-Schulungen, in Ergänzung zu den kantonalen Schulungen gemäss BISR 6 («Schulungsmassnahmen in Informationssicherheit»), nicht überall verpflichtend sind. So wird beispielsweise in der Sicherheitsdirektion oder in der Volkswirtschaftsdirektion auf der Ebene der Ämter festgelegt, inwieweit die Schulungen verpflichtend ausgestaltet werden. Die Baudirektion, die Bildungsdirektion, die Gesundheitsdirektion und die Staatskanzlei haben hingegen verpflichtende (Basis-)Schulungen oder E-Learning-Module implementiert. Bei der Finanzdirektion und der JI scheinen die Schulungen bisher nicht für alle Mitarbeitenden verbindlich zu sein.

15.4.5 Entsorgungsprozesse

Die Antworten der ISID zeigen, dass die Entsorgungsprozesse sich je nach Art der Geräte unterscheiden.

- Alle Geräte des Digitalen Arbeitsplatzes (DAP) können beim Amt für Informatik (AFI) abgegeben werden. Die Entsorgung der Geräte läuft dann über den beauftragten Dienstleister ab, welcher die Geräte erst in ein sicheres und überwachtes Lager übernimmt und dann innerhalb von 4–6 Wochen die Löschung gemäss dem klar definierten Standard durchführt oder vor Ort physisch schreddert, wenn eine Löschung nicht möglich ist. Ein Bericht verzeichnet alle Seriennummern der abgeholten Geräte und es können Löschberichte und Vernichtungszertifikate angefordert werden.
- USB-Speichersticks, externe Festplatten oder Smartphones werden in spezifischen Behältnissen gesammelt und im Auftrag des Immobilienamtes vernichtet.

Die Entsorgung der Server der Rechenzentren jener Direktionen, die noch über eine eigene Informatik verfügen, ist bisher nicht kantonsweit harmonisiert. Sie liegt in der Zuständigkeit der Direktion.

- In der JI erfolgt die fachgerechte Entsorgung von Datenträgern, die bei der JI im Einsatz standen, in Begleitung eines JI-Mitarbeitenden bei einem Entsorgungsdienstleister.[996]
- In der Gesundheitsdirektion werden die Datenspeicher der Server durch den Server-Manager intern mit einem Lösch-Algorithmus überschrieben. Die Festplatten und Bänder des kantonalen Labors werden physisch durch eine etablierte Firma geschreddert. Ihre Labor-Geräte werden mittels Löschsoftware gelöscht und diese Löschung mittels Zertifikats bestätigt.

[996] Direktion der Justiz und des Innern, Generalsekretariat, Digital Solutions, Sammlung und Entsorgung von Datenträgern, USB-Datensticks Handling vom 1. Januar 2023.

Separate Prozesse weist die Kantonspolizei auf:[997]
- Ihre Notebooks oder Deskop-Geräte bereitet die Firma Abraxas zur Entsorgung vor. Die mit der Entsorgung beauftragte Firma hat diese dann zu dokumentieren.
- Gewisse Geräte werden zur Entsorgung persönlich an die Firmen zurückgegeben, welche die vertraglich zugesicherte Entsorgung durchführen und ein Entsorgungsprotokoll erstellen.
- USB-Speichersticks und externe Datenträger werden in abgeschlossenen Behältnissen in einem gesicherten Raum gesammelt und durch die beauftragte Firma regelmässig zur Entsorgung abgeholt.

Insgesamt lassen sich damit die Entsorgungsprozesse des AFI, des Immobilienamtes, der direktionalen Informatikabteilungen in Bezug auf Serverkomponenten sowie die Prozesse der KAPO unterscheiden. Gemäss den vorliegenden Antworten scheint hier inzwischen eine Vereinheitlichung stattgefunden zu haben. Noch im Jahr 2023 stellte das kantonale Zentrum für Cybersicherheit (CCSC) in seinem Audit Folgendes fest:[998] «Die Entsorgung von Datenträgern wird in den Direktionen nicht einheitlich gelebt. Es besteht das Risiko, dass die sachgerechte Entsorgung nicht durchgängig gewährleistet werden kann. Aufgrund des fehlenden umfassenden IKT-Inventars ist die Entsorgung nicht durchgängig nachvollziehbar.» Überdies bestand bezüglich der prozessualen Nachvollziehbarkeit der Rücknahme der Datenträger durch das AFI noch Verbesserungsbedarf.

15.5 Direktionsinterne Audittätigkeit

Gemäss den schriftlichen Auskünften der ISID führten bisher weder die Direktionen noch die Staatskanzlei eigene interne Audits durch. Wie auch aus dem KPMG-Bericht hervorgeht, finden jedoch vereinzelt Penetrations- oder Sicherheitstests statt. In drei Direktionen ist zudem ein Kontrollframework in Anwendung, womit sich die BISR-Umsetzung nachprüfen lässt. Weiter findet durch die Beurteilung und Abnahme von Informationssicherheits- und Datenschutzkonzepten eine Prüftätigkeit statt. In den Antworten wird aber auf die Audits direktionsübergreifend genutzter Dienste und – allgemeiner – auf die Audittätigkeit des CCSC und die Kontrolltätigkeit der Finanzkontrolle sowie der Datenschutzbeauftragten verwiesen.

15.6 Würdigung durch die PUK

Grundlagen

Die PUK Datensicherheit stellt fest, dass in den Direktionen und der Staatskanzlei viele Weisungen erst in den letzten fünf Jahren entstanden sind. Zudem bestehen zwischen den Direktionen Unterschiede im Ausmass der diesbezüglichen Regelungen. Weiterhin wird Informationssicherheit teilweise stark im Kontext der Informatik-Sicherheit gesehen. Eine umfassende Policy, wie sie die KPMG bei der JI gefordert hat, scheint auch in den anderen Direktionen nicht vorzuliegen.

Sicherheitsorganisation

Hinsichtlich der Funktion der ISID-Stellen sieht die PUK Datensicherheit Handlungsbedarf. Auch im Wissen um den Fachkräftemangel ist es für die PUK Datensicherheit unverständlich, dass die für die Informationssicherheit so wesentliche ISID-Stelle nicht

---

997 Antwortschreiben des ISID DS vom 20. Februar 2025.

998 Finanzdirektion, Amt für Informatik, Audit Informationssicherheit Organisation ISMS vom 31. August 2023, S. 4.

überall zeitnah besetzt worden ist. Weiter hat sie Bedenken, dass die ISID dort, wo sie tief in der Hierarchie angesiedelt und dem Leiter der Informatik unterstellt sind, keine Wirkung entfalten können. Es sind hier zwingend kantonale Governance-Vorgaben notwendig, damit die ISID in allen Direktionen und der Staatskanzlei Wirkung entfalten können und die Direktionsleitungen regelmässig über die Informationssicherheitsrisiken informiert werden.

Umsetzung der Informationssicherheit

Die PUK Datensicherheit anerkennt die Leistung der ISID, welche in den letzten Jahren die Informationssicherheit in den Direktionen und der Staatskanzlei vorangetrieben haben. Zugleich sieht sie, dass zur wirkungsvollen Umsetzung der BISR-Vorgaben weitere und grosse Anstrengungen notwendig sind. Sie erachtet es als zwingend notwendig, die diesbezüglichen Herausforderungen gemeinsam und arbeitsteilig anzugehen. Was die unterschiedlichen Instrumente anbelangt, ist eine Koordinierung anzustreben, um eine gesamtkantonale Aggregierung der Risiken und Erkenntnisse zu erleichtern.

Auch geht für die PUK Datensicherheit aus den Antworten der ISID zu den Sicherheits- und Lieferantenüberprüfungen hervor, dass diese auf der gemeinsamen Basis koordiniert aufgebaut werden können und müssen. Die gegebenenfalls notwendige Präzisierung der rechtlichen Grundlagen zur Personensicherheitsüberprüfung[999] schafft die Chance, diese kantonal einheitlich und auf einem guten Niveau festzulegen. Bisher scheinen die meisten Direktionen keine eigenen systematischen, informationssicherheitsspezifischen Prüfungen ihrer Lieferanten vorgenommen zu haben. Hier gilt es die Erkenntnisse aus den kantonalen Lieferantenüberprüfungen zu konsolidieren und dann einheitliche Vorgaben und Prozesse für den gesamten Kanton zu definieren. Die PUK Datensicherheit ist weiter der Ansicht, dass auch die Schulungen in allen Direktionen und der Staatskanzlei verpflichtend auszugestalten sind.

Angesichts der Informationen zu den Entsorgungsprozessen erwartet die PUK Datensicherheit, dass diese nun kantonal einheitlich abgewickelt werden. Folglich ist in Zukunft auch eine Harmonisierung der bisher separat laufenden Prozesse der Kantonspolizei sowie der verbliebenen IKT-Abteilungen mit den kantonalen Prozessen anzustreben.

Audittätigkeit

Die PUK Datensicherheit weist dezidiert darauf hin, dass eigene interne Kontrollen und Auditprozesse notwendig sind, selbst wenn in gewissen Bereichen externe Kontrollen durch die Finanzkontrolle und die Datenschutzbeauftragte durchgeführt werden; Letztere sind lediglich als Ergänzung zu verstehen. Obwohl die frühere Informatiksicherheitsverordnung vom 17. Dezember 1997 eine direktionsinterne Kontrolle vorgeschrieben hat, scheint eine solche heute weder in den Direktionen noch in der Staatskanzlei implementiert zu sein und gelebt zu werden.

---

[999] Gemäss RRB Nr. 1462/2022 vom 9. November 2022, Ausführungsrecht zum Informationssicherheitsgesetz (Vernehmlassung), ist im Bereich der Personensicherheitsprüfungen eine Präzisierung der kantonalen Rechtsgrundlagen abzuklären, damit der Kanton Zürich auch in diesem Bereich eine dem Bund mindestens gleichwertige Informationssicherheit gewährleisten kann.

16. Stand der Informationssicherheit in den selbständigen öffentlich-rechtlichen Anstalten

16.1 Einleitung

Im Zusammenhang mit der Informationssicherheit hat die PUK Datensicherheit von den selbständigen öffentlich-rechtlichen Anstalten des Kantons Zürich schriftlich Auskünfte[1000] zu folgenden Themen eingeholt:
– Vorgaben und Regelwerke
– Informationssicherheitsorganisation
– Stand der Umsetzung des Information Security Management Systems (ISMS)
– Prozesse bei der Ausserbetriebnahme von Datenträgern und Löschung von Daten
– Schulungen und Weiterbildungen
– Audits und Kontrollaktivitäten
– Verbesserungs- oder Handlungsbedarf gemäss Audits und Kontrollaktivitäten
– Ergriffene Massnahmen nach Bekanntwerden des Datensicherheitsvorfalls

16.2 Umsetzung der Informationssicherheit[1001]

Vorgaben und Regelwerke

Die Auskünfte zeigen, dass die selbständigen öffentlich-rechtlichen Anstalten über Vorgaben und Regelwerke in Form von Weisungen, Reglementen und ähnlichen Dokumenten verfügen. Dabei wird ersichtlich, dass die Mehrheit der Anstalten eine oder mehrere Weisungen zu den Themen Informationssicherheit, Informationsklassifizierung, Umgang mit Informatikmitteln sowie Datenschutz eingeführt hat. Soweit zeitliche Angaben gemacht wurden, lässt sich jedoch feststellen, dass diese Weisungen und Reglemente in der Regel erst kürzlich erlassen wurden. Häufig orientieren sich die selbständigen öffentlich-rechtlichen Anstalten – insbesondere jene, die noch keine eigenen Regelwerke erarbeitet haben – an international anerkannten Standards, etwa jenen der ISO oder des NIST. Es zeigte sich zudem, dass nur wenige Anstalten in ihren Antworten explizit auf Vorgaben der übergeordneten Direktionen Bezug nahmen. Insbesondere die Elektrizitätswerke des Kantons Zürich (EKZ) und die Psychiatrische Universitätsklinik Zürich (PUK) haben auf die Eigentümerstrategie verwiesen, während andere Anstalten entsprechende Vorgaben auf Ebene der strategischen oder operativen Gesamtleitung erwähnt haben. Unabhängig davon haben sich sechs Anstalten ausschliesslich auf gesetzliche Vorgaben bezogen, ohne weiterführende Hinweise auf spezifische Anforderungen der Eigentümer zu geben.

[1000] Fragebogen Informationssicherheit bei den selbständigen öffentlich-rechtlichen Anstalten der PUK Datensicherheit vom 22. Januar 2025.

[1001] Antworten der Universität Zürich zum Fragebogen vom 12. Februar 2025; Antworten der Zentralbibliothek zum Fragebogen vom 20. Februar 2025; Antworten der Zürcher Hochschule für Angewandte Wissenschaften zum Fragebogen vom 20. Februar 2025; Antworten der Zürcher Hochschule der Künste zum Fragebogen vom 14. Februar 2025; Antworten der Elektrizitätswerke des Kantons Zürich zum Fragebogen vom 5. März 2025; Antworten der BVG- und Stiftungsaufsicht des Kantons Zürich zum Fragebogen vom 14. Februar 2025; Antworten der Integrierten Psychiatrie Winterthur – Zürcher Unterland zum Fragebogen vom 20. Februar 2025; Antworten des Kantonsspitals Winterthur zum Fragebogen vom 4. Februar 2025; Antworten der Psychiatrischen Universitätsklinik Zürich zum Fragebogen vom 20. Februar 2025; Antworten des Universitätsspitals Zürich zum Fragebogen vom 20. Februar 2025; Antworten der Gebäudeversicherung Kanton Zürich zum Fragebogen vom 18. Februar 2025; Antworten der Sozialversicherungsanstalt des Kantons Zürich zum Fragebogen vom 19. Februar 2025; Antworten der Zürcher Kantonalbank zum Fragebogen vom 18. Februar 2025.

Informationssicherheitsorganisation

Die Informationssicherheitsorganisation der Anstalten zeigt ein uneinheitliches Bild: Während bei einigen Anstalten bereits eine dezidierte Stelle für Informationssicherheit eingerichtet wurde, liegt die Zuständigkeit bei anderen weiterhin bei den jeweiligen Informatikverantwortlichen. Insbesondere im Bereich Bildung und Gesundheit verfügen beinahe alle selbständigen öffentlich-rechtlichen Anstalten über eine eigene CISO-Stelle. Zudem haben viele der selbständigen öffentlich-rechtlichen Anstalten Gremien gebildet, in denen Fragen der Informationssicherheit und des Datenschutzes behandelt werden. Diese Gremien werden teils von den Direktoren der Anstalten, teils von den Informatikverantwortlichen geleitet. Die Befugnisse der jeweils zuständigen Stellen innerhalb der Anstalten variieren deutlich. Nur wenige verfügen über Weisungs- oder Entscheidungsbefugnisse. Etwa ein Drittel der Stellen besitzt ein Prüfungsrecht, während die übrigen keine nennenswerten besonderen Befugnisse aufweisen.

Informationssicherheits-Managementsystem

Den Auskünften ist zu entnehmen, dass alle Anstalten entweder bereits ein Informationssicherheits-Managementsystem (ISMS) implementiert haben, sich derzeit in der Implementierungsphase befinden oder weitergehende Entwicklungen planen. Aktuelle Entwicklungen laufen hier u. a. bei den selbständigen öffentlich-rechtlichen Anstalten in den Bereichen Gesundheit und Bildung sowie bei der Gebäudeversicherung Kanton Zürich (GVZ). Es zeigt sich auch, dass die Umsetzung auf unterschiedlichen Zertifizierungen und Standards basiert. Die Mehrheit der Anstalten orientiert sich an der ISO-Zertifizierung.

Prozesse zur Entsorgung von Datenträgern und zur Löschung von Daten

Die dargelegten Prozesse zur Entsorgung von Datenträgern und zur Löschung von Daten zeigen, dass der Grossteil der selbständigen öffentlich-rechtlichen Anstalten mit externen Dienstleistern zusammenarbeitet und die Vernichtung bzw. Löschung zertifiziert erfolgt. Vereinzelt kommen bei der internen Weiterverwendung von Geräten spezielle Löschprogramme zum Einsatz. Im Unterschied dazu wickelt die Zürcher Kantonalbank (ZKB) den Prozess weitgehend intern ab bzw. lässt ihn durch eigene Mitarbeitende begleiten. Aus den Auskünften geht zudem hervor, dass nur wenige Anstalten bereits seit über 15 Jahren über entsprechende Prozesse verfügen. Einige Anstalten haben diese um 2014 eingeführt, parallel zur verstärkten Auseinandersetzung mit dem Thema auf Ebene der kantonalen Verwaltung. Andere dokumentieren die Vernichtung und Löschung von Datenträgern erst seit wenigen Jahren.

Schulungen und Weiterbildungen

Betreffend Schulungen und Weiterbildungen stellte die PUK Datensicherheit anhand der eingegangenen Auskünfte fest, dass – mit Ausnahme der Universität Zürich (UZH) und der Pädagogischen Hochschule Zürich (PHZH) – alle selbständigen öffentlich-rechtlichen Anstalten regelmässige Weiterbildungen im Bereich Informationssicherheit anbieten, wobei die Intervalle und die Definition von «Regelmässigkeit» zum Teil deutlich variieren. Die UZH und die PHZH befinden sich derzeit in der Entwicklung zusätzlicher Massnahmen in diesem Bereich. Bei gut der Hälfte der Anstalten sind Schulungen und Weiterbildungen für die Mitarbeitenden verbindlich vorgeschrieben. Eine Tendenz, welche Kategorien von Anstalten eine Verbindlichkeit vorsehen, ist nicht erkennbar. Die Rückmeldungen zeigen aber, dass in mehreren Anstalten derzeit Bestrebungen im Gange sind, die Verbindlichkeit solcher Massnahmen weiter zu erhöhen.

Audits und Kontrollaktivitäten

Aus den eingegangenen Auskünften geht hervor, dass alle Anstalten regelmässige interne und externe Audits und Kontrollaktivitäten durchführen. Acht Anstalten lassen – teils auch aufgrund bundesrechtlicher Vorgaben – unabhängige und relativ umfassende externe Audits durchführen. Andere Anstalten haben für verschiedene ihrer Applikationen und Systeme Penetrationstests oder Prüfungen durchführen lassen. Ganz vereinzelt hat sich aber auch gezeigt, dass sich die externen Prüfaktivitäten bisher lediglich auf die Prüfungen durch die Datenschutzbeauftragte oder die Finanzkontrolle beschränkt haben. Eine Ausnahme ist die Zentralbibliothek (ZB), die angegeben hat, keine entsprechenden Audits implementiert zu haben.

Die Mehrheit der Anstalten hat aus Sicherheits- und Vertraulichkeitsgründen darauf verzichtet, detaillierte Listen mit identifiziertem Verbesserungs- oder Handlungsbedarf aus Audits und Kontrollaktivitäten zu übermitteln. Bei jenen Anstalten, die entsprechende Angaben gemacht haben, konnten – soweit durch die PUK Datensicherheit beurteilbar – keine Auffälligkeiten festgestellt werden.

Reaktion auf den Datensicherheitsvorfall

Ein Grossteil der selbständigen öffentlich-rechtlichen Anstalten gab an, bereits regelmässige Überprüfungen der Informationssicherheit und der damit verbundenen Prozesse durchzuführen. Daher wurden nach Bekanntwerden des Datensicherheitsvorfalls in der Regel keine zusätzlichen Massnahmen ergriffen. In Einzelfällen wurde eine erneute Überprüfung der bestehenden Prozesse vorgenommen, die jedoch keinen unmittelbaren Handlungsbedarf ergab. Lediglich die UZH reagierte mit einer strukturellen Anpassung: Sie setzte nach Bekanntwerden des Datensicherheitsvorfalls einen Chief Information Security Officer (CISO) ein und erstellte auf Basis eines Risikokonzepts ein entsprechendes Risikoprofil.

16.3 Würdigung durch die PUK

Zusammenfassend stellt die PUK Datensicherheit fest, dass seitens der zuständigen Direktionen nur wenige verbindliche Vorgaben – etwa in Bezug auf einzuhaltende Standards – gegenüber den selbständigen öffentlich-rechtlichen Anstalten bestehen. Die Thematik der Informationssicherheit wird innerhalb der Anstalten entsprechend unterschiedlich gehandhabt, selbst wenn diese vergleichbare Aufgaben erfüllen oder derselben Direktion zugeordnet sind. Die PUK Datensicherheit erwartet, dass diese Thematik durch die zuständigen Direktionen und den Regierungsrat aufgenommen wird. Verbindliche Vorgaben für die selbständigen öffentlich-rechtlichen Anstalten sind im Rahmen der Eigentümerstrategien zwingend zu adressieren und zu überprüfen.

Zudem hat sich gezeigt, dass die meisten selbständigen öffentlich-rechtlichen Anstalten ihre Regelwerke und Vorgaben zur Informationssicherheit erst in den letzten Jahren eingeführt haben. Nur ein Teil der Anstalten hat eine eigene CISO-Stelle etabliert. Die Zuständigkeiten und Befugnisse der verantwortlichen Stellen – unabhängig davon, ob es sich um dezidierte Positionen handelt oder ob die Aufgabe anderweitig angesiedelt ist – variieren erheblich. Sie reichen von reinen Prüfrechten bis hin zu Weisungs- und Anordnungsbefugnissen. Auch hinsichtlich Schulungen und Weiterbildungen bestehen erhebliche Unterschiede sowohl in der Häufigkeit als auch – deutlich ausgeprägter – im Grad der Verbindlichkeit für die Mitarbeitenden.

17. State of the Art und diesbezügliche Entwicklungen

17.1 Einleitung

Das Gesetz über die Information und den Datenschutz des Kantons Zürich (IDG)[1002] schreibt vor, dass Informationen, welche die öffentlichen Organe nicht mehr benötigen, aufzubewahren und nach Ablauf der Aufbewahrungsfrist dem zuständigen Archiv anzubieten oder, sofern das Archiv die Informationen nicht als archivwürdig erachtet, zu vernichten sind[1003] und dass Personendaten zu löschen, anonymisieren oder pseudonymisieren sind, sobald und soweit dies möglich ist[1004].

Im Allgemeinen versteht man unter dem Begriff «Vernichtung» entweder die physische Zerstörung oder das dauerhafte Löschen von Informationen. Bei der physischen Vernichtung wird das Speichermedium selbst – etwa ein Datenträger oder ein Blatt Papier – zerstört. Im Gegensatz dazu bezeichnet «Löschung» das Unkenntlichmachen der gespeicherten Daten, wobei das Speichermedium intakt bleibt.[1005]

Sowohl die Arten der Datenvernichtung und -löschung als auch die diesbezüglichen Praktiken (State of the Art) haben, wie die IKT, grosse Entwicklungen durchgemacht. Neue technische Möglichkeiten und die zunehmenden Mengen an (zu entsorgenden) Datenträgern fordern neue Massnahmen. Die nachfolgenden Informationen zur Entwicklung der Datenvernichtung und -löschung basieren auf der Auswertung von beigezogenen Unterlagen sowie auf Aussagen von Fachpersonen, die im Rahmen der Informationsbeschaffungsphase befragt worden sind. In Kapitel 17.6 wird die Praxis im Bankensektor auf Basis der Entwicklung bei der Zürcher Kantonalbank beleuchtet.[1006] Die Erkenntnisse geben einen Überblick über den Wandel der Datenlöschpraktiken in den letzten Jahrzehnten und zeigen, wie sich technologische, rechtliche und sicherheitsrelevante Anforderungen auf die Unternehmensprozesse ausgewirkt haben.

17.2 Standards und Zertifizierungen

Zertifizierungen wie ISO, NIST oder DIN sind anerkannte Standards, die festlegen, wie Prozesse, Produkte oder Sicherheitsmassnahmen in der Informatik und IT gestaltet sein sollten, damit sie sicher, zuverlässig und vergleichbar sind.

- ISO (International Organization for Standardization) ist eine weltweite Organisation, die internationale Normen für Produkte, Dienstleistungen und Systeme entwickelt. Ein bekanntes Beispiel ist ISO 27001 für Informationssicherheits-Managementsysteme (ISMS), das beschreibt, wie ein Unternehmen seine Informationssicherheit systematisch aufbauen und nachweisen kann.
- NIST (National Institute of Standards and Technology) ist eine US-amerikanische Behörde, die vor allem technische und sicherheitsrelevante Leitlinien erstellt, z. B. Empfehlungen für sichere Passwörter, Verschlüsselung oder den Umgang mit Cyberangriffen. So beschreibt die bekannte Richtlinie NIST-800-88 Methoden, um Daten auf Speichermedien sicher zu löschen.

[1002] Gesetz über die Information und den Datenschutz (IDG; LS 170.4).

[1003] § 5 Abs. 2 und 3 IDG.

[1004] § 11 Abs. 2 IDG.

[1005] Merkblatt «Vernichten elektronischer Daten» der Datenschutzbeauftragten des Kantons Zürich (V 2.5 / Oktober 2024), Ziffer 1.1.

[1006] Protokoll der Befragung von David Bänziger und Michael Wydler vom 22. März 2024.

– DIN (Deutsches Institut für Normung) erstellt in Deutschland Normen, die oft in Zusammenarbeit mit der ISO entstehen. Sie sorgen dafür, dass technische Produkte und Verfahren in Deutschland einheitlich und kompatibel sind. Die DIN-Norm 66399 zeigt beispielsweise je nach Schutzstufe der Informationen, welche Partikelgrösse für eine sichere physische Vernichtung von Datenträgern angezeigt ist.

Solche Zertifizierungen dienen Unternehmen als Nachweis gegenüber Kunden, Partnern und Behörden, dass sie bewährte Verfahren einhalten. Ausserdem schaffen sie klare Anforderungen, an denen sich Prozesse messen lassen, und helfen, rechtliche Vorgaben zu erfüllen.

17.3 Arten der Datenvernichtung und -löschung

17.3.1 Physische Vernichtung

Bei der physischen Vernichtung wird das Speichermedium – etwa durch mechanisches Zerkleinern (z. B. Schreddern) oder Einschmelzen resp. Verbrennen – vollständig zerstört, sodass sämtliche gespeicherten Daten vollumfänglich vernichtet werden.[1007]

17.3.2 Magnetische Löschung

Durch spezielle Löschgeräte können ganze Festplatten durch spezifische Magnetisierung gelöscht werden. Diese Methode verunmöglicht resp. erschwert weitgehend die Datenwiederherstellung und kann auch bei defekten Festplatten noch wirksam angewendet werden.[1008]

17.3.3 Technisches Überschreiben (Wipen)

Wiederbeschreibbare Speichermedien oder einzelne Dateien können dauerhaft gelöscht werden, indem sie mehrfach mit zufälligen Zeichenfolgen überschrieben werden. Diese Methode, bekannt als «Wipen», verhindert eine Wiederherstellung der Daten. Die Überschreibung ist mehrfach vorzunehmen, da bei einmaligem Überschreiben eventuell noch magnetische Restladungen auf dem Datenträger gemessen werden können, die zur Rekonstruktion ausreichen könnten.[1009]

17.3.4 Löschen nichtflüchtiger elektronischer Speichermedien (NVM)

Moderne Geräte enthalten häufig nichtflüchtige Speichermedien (NVM) wie Solid State Disks (SSD) oder NVM Express (NVMe). Aufgrund ihrer Architektur lassen sich die auf diesen Medien gespeicherten Daten nicht durch Wipen oder Magnetisierung löschen. Stattdessen müssen sie über spezielle Löschbefehle gelöscht werden. Falls ein Speichermedium solche Befehle nicht unterstützt, ist es vor der Aussonderung zu verschlüsseln und anschliessend physisch zu vernichten (Schreddern).[1010]

[1007] Merkblatt «Vernichten elektronischer Daten» der Datenschutzbeauftragten des Kantons Zürich (V 2.5 / Oktober 2024), Ziffer 3.1.

[1008] Merkblatt «Vernichten elektronischer Daten» der Datenschutzbeauftragten des Kantons Zürich (V 2.5 / Oktober 2024), Ziffer 3.2.

[1009] Merkblatt «Vernichten elektronischer Daten» der Datenschutzbeauftragten des Kantons Zürich (V 2.5 / Oktober 2024), Ziffer 3.3.

[1010] Merkblatt «Vernichten elektronischer Daten» der Datenschutzbeauftragten des Kantons Zürich (V 2.5 / Oktober 2024), Ziffer 3.4.

17.3.5 Logische Löschung

Bei der logischen Löschung wird lediglich der Zugriffsschlüssel (Index) auf eine Datei entfernt – etwa durch Betätigen der Delete-Taste oder Verschieben in den Papierkorb. Hierbei wird nur die Indexdatei gelöscht. Die Datei selbst bleibt erhalten und kann durch Wiederherstellung des Indexes erneut zugänglich gemacht werden.[1011]

17.4 Risikoreduzierende Massnahmen

Personenbezogene Daten sollten unmittelbar nach Wegfall des Verwendungszwecks und der Aufbewahrungsdauer gelöscht oder vernichtet werden. Wenn eine sofortige Datenvernichtung ausnahmsweise nicht möglich ist, müssen alternative Massnahmen getroffen werden, um den Schutz der betroffenen Daten bis zur endgültigen Löschung sicherzustellen.[1012]

Mögliche risikoreduzierende Massnahmen sind:[1013]

- Anonymisierung: Entfernen des Personenbezugs, sodass keine oder nur eine mit unverhältnismässig hohem Aufwand verbundene Zuordnung zu einer Person möglich ist.
- Schlüsselvernichtung: Löschen aller Entschlüsselungsschlüssel, um den Zugriff auf verschlüsselte Daten zu verhindern.
- Zugriffsbeschränkung: Begrenzung und Protokollierung des Datenzugriffs auf autorisierte Personen.
- Pseudonymisierung: Ersetzen personenbezogener Daten durch Identifikatoren; Rückführung nur mit Pseudonymisierungsschlüssel möglich.
- Löschen von Referenzen: Entfernen von Referenzen, sodass Daten nicht mehr auffindbar sind, sie bleiben jedoch im System vorhanden.

17.5 Praxis der Datenvernichtung und -löschung

Für die folgenden Ausführungen stützt sich die PUK Datensicherheit auf die Erfahrungen eines etablierten Unternehmens im Bereich der Datenlöschung, wie sie ihr im Rahmen der Befragung geschildert wurden:[1014]

1990er-Jahre: Fokus auf Wiedervermarktung

In den 1990er-Jahren lag der Fokus eher auf der Wiedervermarktung gebrauchter Hardware als beim konkreten Umgang mit den Daten des Kunden. Der Datenschutz und die konkrete Datenlöschung fanden noch wenig Beachtung. Dies deutet auf ein damals geringes Bewusstsein für Datenschutzrisiken hin.[1015]

[1011] Merkblatt «Vernichten elektronischer Daten» der Datenschutzbeauftragten des Kantons Zürich (V 2.5 / Oktober 2024), Ziffer 3.5.

[1012] Merkblatt «Vernichten elektronischer Daten» der Datenschutzbeauftragten des Kantons Zürich (V 2.5 / Oktober 2024), Ziffer 4.

[1013] Merkblatt «Vernichten elektronischer Daten» der Datenschutzbeauftragten des Kantons Zürich (V 2.5 / Oktober 2024), Ziffern 4.1– 4.5.

[1014] Protokoll der Einvernahme von Predrag Nenadovic (CBA Computer Broker AG) vom 22. März 2024; Schreiben der CBA Computer Broker AG mit dem Titel «Überblick über die Entwicklungen der Datenlöschungspraktiken, Handlungsbedarf» vom 17. April 2024.

[1015] CBA Computer Broker AG, Schreiben vom 16. Dezember 2002.

2000er-Jahre: Wendepunkt – Einführung strukturierter Datenvernichtung

Ab den 2000er-Jahren wurden Datenlöschsoftwares systematisch im Kundenumfeld eingesetzt. Die Datenlöschung etablierte sich als eigenständiger, fester Schritt der Rollout-Prozesse, der noch vor der eigentlichen Geräteprüfung stattfand. Dies verdeutlicht das wachsende Bewusstsein für Datenschutz sowie eine zunehmende Sensibilisierung für den sicheren Umgang mit heiklen Informationen und für die Einhaltung gesetzlicher Vorgaben.

Frühe 2010er-Jahre: Datenvernichtung als Nebenleistung

In den frühen 2010er-Jahren blieb die Wahrnehmung der Datenlöschung noch stark von pragmatischen und betriebswirtschaftlichen Überlegungen geprägt. Man verstand sie als notwendige Vorbedingung für die Wiederverwertung gebrauchter Hardware. Der Fokus lag auf wirtschaftlichen Aspekten, wie dem Rückkauf und Weiterverkauf von Geräten, während Datenschutzmassnahmen häufig eher als notwendige Nebenleistung ergriffen wurden, um gesetzliche Vorgaben umzusetzen und dadurch den Wiederverkauf zu ermöglichen. Zwar kamen bereits verschiedene Löschstufen und optionale Löschprotokolle zum Einsatz, doch standen nachhaltige Datenvernichtung und tiefergehende Datensicherheitsrisiken noch nicht im Mittelpunkt. Die Datenlöschung war meist Teil eines umfassenden Hardware-Management-Prozesses und wurde eher als unterstützende Massnahme denn als eigenständiger Sicherheitsfaktor betrachtet. Ein grundlegendes Datenschutzbewusstsein war zwar vorhanden, entsprach jedoch noch nicht den heutigen Standards.

Späte 2010er-Jahre: Professionalisierung der Datenvernichtung

Ab Mitte der 2010er-Jahre entwickelte sich die Datenlöschung zu einem zentralen, standardisierten Bestandteil im IT-Lifecycle-Management. Während zuvor meist nur allgemein von Löschleistungen die Rede war, wurden nun konkrete Löschmethoden und Sicherheitsstandards – wie etwa die einfache oder dreifache Überschreibung gemäss anerkannten Normen – fest in die Prozesse integriert.[1016] Die Abläufe wurden systematisch gestaltet, von der sicheren Zwischenlagerung der Geräte über die Datenlöschung bis zur Endverarbeitung der Geräte. Damit rückten Sicherheit, Compliance und transparente Dokumentation stärker in den Fokus. Diese Entwicklung zeigt ein deutlich gestiegenes Bewusstsein für Datenschutzrisiken und regulatorische sowie sicherheitstechnische Anforderungen im Umgang mit sensitiven Daten sowie die Notwendigkeit verlässlicher und nachvollziehbarer Datenvernichtungsprozesse.

Aktuelle Standards

Die Datenlöschung hat sich in den 2020er-Jahren weiter professionalisiert und ist heute auch in der Schweiz stark an internationale Datenschutzstandards angepasst. Es werden verschiedene Methoden angewendet wie bspw. moderne Löschsoftwarelösungen, die auf höchste Sicherheitsstandards ausgerichtet, durch anerkannte Prüfstellen zertifiziert und mit globalen Datenschutzvorgaben wie der Datenschutz-Grundverordnung der EU (DSGVO) konform sind.

Das der PUK Datensicherheit vorliegende Vertragsmuster aus dem Jahr 2024 zeigt, dass die Transparenz und Nachvollziehbarkeit durch detaillierte Dokumentationen und auditierbare Berichte gegenüber der Situation Mitte der 2010er-Jahren nochmals verbessert wurde.[1017] Manipulationssichere Protokolle sorgen dafür, dass jeder Schritt im

[1016] CBA Computer Broker AG, Offerte vom 28. Juli 2016.

[1017] CBA Computer Broker AG, Muster Zusammenarbeitsvertrag IT Asset Disposition Agreement vom 17. April 2024.

Löschprozess rechtlich abgesichert und dokumentiert ist. Ergänzt wird dies durch eine verstärkte physische und technische Sicherheitsinfrastruktur, wie gesicherte Standorte, Zugangskontrollen und regelmässige externe Audits. Die Datenlöschung ist heute nicht mehr nur eine Nebenleistung, sondern ein zentraler Bestandteil eines umfassenden Sicherheits- und Compliance-Prozesses.

Mit dem wachsenden Bedarf an Dienstleistungen im Bereich der Datenträgervernichtung und Datenlöschung ist auch das diesbezügliche Angebot gewachsen. Nicht alle Anbieter genügen den sicherheitsrelevanten Anforderungen, ihre Dienstleistungen erfüllen nicht die erforderlichen Standards. Vor diesem Hintergrund ist vonseiten der Auftraggeber in einem professionellen Submissionsprozess sicherzustellen, dass nur zuverlässige Anbieter den Zuschlag bekommen.

17.6 Datenträgerentsorgung und Datenvernichtung im Bankensektor

Da Banken aufgrund der Menge sensitiver Daten früh ein starkes Bewusstsein für Datenschutz entwickelten und ihnen ein besonders hoher Standard bei der Datenvernichtung zugeschrieben wird, hat die PUK Datensicherheit die Zürcher Kantonalbank (ZKB) zu ihren Prozessen im Bereich der Datenträgerentsorgung und Datenvernichtung befragt. Nachfolgend sind die wichtigsten Erkenntnisse zusammengefasst.[1018]

Bis Anfang der 2010er-Jahre nutzte die ZKB intern entwickelte Löschprogramme. Aufgrund des rasanten technologischen Fortschritts und des stetig wachsenden Datenträgervolumens erwiesen sich diese Methoden jedoch zunehmend als ineffizient. In der Folge zerstörte man die Datenträger, in dem man sie physisch durchbohrte.

Um das Jahr 2014 beschloss man, die Datenträger nach einem standardisierten Verfahren schreddern zu lassen respektive zu löschen. Mit diesem Übergang zu standardisierten Verfahren richtet sich die Vernichtung nach der DIN 66399 für physische Zerstörung sowie dem NIST-Standard für softwarebasierte Datenlöschung (Wipen). Dabei wird keine Unterscheidung zwischen Datenträgertypen vorgenommen, sondern grundsätzlich davon ausgegangen, dass alle Datenträger vertrauliche Informationen enthalten. Entsprechend erfolgt die Vernichtung einheitlich nach höchsten Sicherheitsstandards.

Im Unterschied zu den in Kapitel 17.5 dargelegten Entwicklungen im Bereich der Datenvernichtung, die insbesondere einen Fokus auf Löschsoftware legt, vernichtet die ZKB ihre Datenträger vorwiegend physisch (Schreddern oder Verbrennen). Sollen Datenträger ausnahmsweise nicht zerstört und stattdessen weiterverkauft werden, überschreibt die ZKB die Geräte technisch (Wipen).

Ein zentraler Sicherheitsaspekt besteht darin, dass Datenträger die Geschäftsräumlichkeiten – auch in Zusammenhang mit der Datenvernichtung – nie unbeaufsichtigt verlassen. Ein spezialisierter Mitarbeitender der ZKB ist dabei stets anwesend. Zudem wird ein vollständiges Inventar über alle Datenträger geführt, unabhängig davon, ob diese zur Vernichtung vorgesehen sind oder nicht.

Schreddern

Der Prozess der Datenträgervernichtung durch Schreddern folgt einem klar strukturierten und auditierbaren Prozess. Die Datenträger werden von zertifizierten Mitarbeitern ausgebaut oder von Mitarbeitenden der ZKB zu den zuständigen Stellen gebracht. Die Datenträger werden dann an einer zentralen, gesicherten Eingangsstelle in der ZKB in geschützten Behältnissen bzw. geschlossenen Containern gesammelt. An-

[1018] Protokoll der Einvernahme von Michael Wydler und David Bänziger (Zürcher Kantonalbank) vom 22. März 2024.

schliessend erfolgt die Inventarisierung in einer Entsorgungsdatenbank, in der alle Datenträger erfasst werden. Sobald eine definierte Menge erreicht ist, wird ein Entsorgungsprotokoll der inventarisierten Datenträger erstellt. Die zur Vernichtung bereitgestellten Datenträger werden anschliessend an ein spezialisiertes Unternehmen übergeben und dort unter Begleitung von mindestens zwei Mitarbeitenden der ZKB vernichtet. Abschliessend wird der gesamte Vorgang mit Vernichtungszertifikaten und entsprechender Dokumentation belegt, um eine lückenlose Nachvollziehbarkeit sicherzustellen.

Verbrennen

Magnetische Datenträger wie bspw. Tapes eignen sich nicht zum Schreddern, da das Material schwer zerstückelbar ist. Stattdessen werden sie durch Verbrennung vernichtet. Die Entsorgung erfolgt unter Augenzeugenkontrolle durch Mitarbeitende der ZKB, wobei sichergestellt wird, dass die vollständige Zerstörung der Datenträger erfolgt.

Wipen

Wenn Datenträger der ZKB weiterverwendet oder weiterverkauft werden sollen, kommt in Zusammenarbeit mit spezialisierten Dienstleistern ein sicheres Löschverfahren zum Einsatz. Diese Dienstleister stützen sich auf anerkannte Richtlinien wie NIST 800-88. Die Richtlinie empfiehlt Verfahren, die eine vollständige und unwiderrufliche Datenlöschung gewährleisten, so z. B. das mehrfache Überschreiben etwa bei SSD. Die ordnungsgemässe Durchführung wird zwischen der ZKB und den spezialisierten externen Dienstleistern vertraglich geregelt und dokumentiert.

Zur Sicherstellung der Datensicherheit behält sich die ZKB gegenüber Anbietern von Vernichtungsdienstleistungen vertraglich das Recht vor, deren Prozesse einzusehen oder Vor-Ort-Kontrollen durchzuführen. Zudem sind die Anbieter verpflichtet, der ZKB den Verlust von Zertifizierungen unverzüglich zu melden.

Darüber hinaus führt die ZKB regelmässig interne Stichproben und Audits durch, um die Einhaltung der festgelegten Sicherheitsvorgaben zu überprüfen. Zusätzlich wird die Organisation durch externe Stellen – unter anderem die FINMA oder die Revision – geprüft, insbesondere auch im Hinblick auf den Umgang mit Datenträgern.

17.7 Würdigung durch die PUK

Allgemein stellt die PUK Datensicherheit fest, dass sich auch innerhalb der befragten Unternehmen beobachten lässt, dass der bewusste Umgang mit den Daten sich erst über die Zeit entwickelt hat und die Prozesse im Hinblick auf die Informationssicherheit stetig verbessert wurden. Es zeigt sich, dass ab den 2010er-Jahren die Prozesse diesbezüglich professionalisiert worden sind. Für die PUK Datensicherheit ist nachvollziehbar, dass in den 2000er-Jahren das Bewusstsein in der Verwaltung noch schwach ausgeprägt war. Allerdings liegen ihr Löschprotokolle gewisser Direktionen aus den Jahren 2008 und 2010 vor, was zeigt, dass man sich auf Ebene der zuständigen IT-Leiter schon damals der Thematik bewusst war und auch entsprechend handelte.

Basierend auf den Aussagen der befragten Fachpersonen sowie den eingesehenen Unterlagen konnte die PUK Datensicherheit mehrere kritische Themen im Bereich der Datenlöschung identifizieren. Diese werden im Folgenden zusammengefasst:[1019]

[1019] Protokoll der Einvernahme von Predrag Nenadovic (CBA Computer Broker AG) vom 22. März 2024; Schreiben der CBA Computer Broker AG mit dem Titel «Überblick über die Entwicklungen der Datenlöschungspraktiken, Handlungsbedarf» vom 17. April 2024.

Lückenlose Nachverfolgbarkeit von Datenträgern

Eigentümer bzw. Besitzer von Datenträgern haben bei der systematischen Inventarisierung noch erheblichen Nachholbedarf. Um eine vollständige und nachvollziehbare Datenlöschung zu gewährleisten, sind alle Datenträger in Anlagelisten mit Seriennummern zu erfassen. Nur durch eine lückenlose Dokumentation und die Zuordnung entsprechender Löschzertifikate pro Gerät kann die normgerechte Vernichtung sensitiver Daten nachgewiesen werden.

Regulierung der Datenlöschungsbranche

Die wachsende Zahl von Anbietern im Bereich der Datenlöschung führt vermehrt zu Fällen unsachgemässer Entsorgung, unvollständiger Löschung oder gar Missbrauch sensitiver Informationen. Aus Sicht der PUK Datensicherheit tragen gesetzliche Vorgaben und die Berücksichtigung internationaler Normen und Standards dazu bei, die Qualität und Sicherheit der Datenvernichtung zu gewährleisten.

Standort der Durchführung der Datenlöschung

Die PUK Datensicherheit ist der Ansicht, dass die Datenlöschung bei öffentlichen Organen im Inland gemäss den hier geltenden Normen und anerkannten Standards zu erfolgen hat. Auf diese Weise lassen sich Sicherheitsrisiken, wie eine unzureichende Verschlüsselung, Diebstahl während des Transports oder mangelhafte Einhaltung der Sicherheitsstandards, vermeiden.

18. Empfehlungen der PUK Datensicherheit

18.1 Koordination und Zusammenarbeit innerhalb des Regierungsrates

1.	Die PUK Datensicherheit stellt im Regierungsrat als einer Kollegialbehörde einen starken Fokus der einzelnen Regierungsmitglieder auf die eigene Direktion fest. Die PUK Datensicherheit fordert mit Nachdruck eine intensivere Zusammenarbeit und gemeinsame Verantwortung.	Kapitel 12 und 13
2.	Das Silodenken mit Fokus auf die eigene Direktion muss gerade im Bereich der Informationssicherheit überwunden werden. Dazu sind nötigenfalls auch die rechtlichen Grundlagen zu überarbeiten.	
3.	Konkret fordert die PUK Datensicherheit eine Anpassung der Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung, welche mit § 60 Abs. 1 lit. e die Zuständigkeit für die Regeln zur Umsetzung des IDG aktuell auf der Direktionsebene statt auf der kantonalen Ebene verortet.	
4.	Die PUK Datensicherheit erwartet, dass insbesondere die Compliance im Bereich der Informationssicherheit und des Datenschutzes im gesamten Kanton auf der Regierungsebene gemeinsam angegangen wird. Die PUK Datensicherheit sieht ganz klar den Regierungsrat als Kollegialbehörde in der Pflicht, die Umsetzung der Empfehlungen aus dem Bericht der Administrativuntersuchung und des KPMG-Berichtes, beispielsweise im Bereich der vertraglichen Vorgaben, der Personensicherheitsprüfung oder des Risikomanagements, auf der gesamtkantonalen Ebene und einheitlich anzugehen.	
5.	Aus Sicht der PUK Datensicherheit ist es beim wichtigen Thema der Informations- und Cybersicherheit nicht angebracht, auf dem eigenen Machtbereich zu beharren und eigenständige Lösungen zu forcieren. Vor diesem Hintergrund kann es sich die PUK Datensicherheit vorstellen, dass künftig auch eine gemeinsame Zuständigkeit für das Amt für Informatik (AFI) oder eine andere Verortung des AFI geprüft werden.	Kapitel 14

18.2 Strategische Grundlagen, strategische Steuerung und Begleitung durch den Regierungsrat

6.	Die PUK Datensicherheit attestiert dem Regierungsrat, dass er mit der Verabschiedung der IKT-Strategie, der Strategie Digitale Verwaltung sowie der Strategie Digitaler Wandel an den Schulen der Sekundarstufe II die Basis der heutigen IKT-Governance gelegt hat. Bisher ist die Informationssicherheit in diesen Digitalisierungsstrategien aber nicht zufriedenstellend berücksichtigt. Angesichts der vielfältigen und komplexen Dynamik in der digitalen Transformation ist für die PUK Datensicherheit die Informationssicherheit auch auf der Ebene der strategischen Überlegungen zu behandeln. Es reicht nicht aus, diese Fragen nur im Kontext der Organisation oder der konkreten Projekte zu berücksichtigen.	Kapitel 10
7.	Die PUK Datensicherheit fordert dazu auf, die strategischen Herausforderungen der Digitalisierung gesamtheitlich zu betrachten und angesichts der Vielzahl strategischer Grundlagen[1020] in diesem Bereich eine Klärung herbeizuführen, die Grundlagen zu vereinheitlichen und unter Berücksichtigung des Aspekts der Informationssicherheit zusammenzuführen.	Kapitel 14
8.	Die PUK Datensicherheit sieht im Bereich der strategischen Steuerung das SDI in der Pflicht, dafür zu sorgen, dass auf Grundlage der in den Direktionen und der Staatskanzlei erhobenen Informationen eine gesamtkantonale Steuerung möglich ist. Mit einer gesamtkantonalen Sicht ist für einen effizienten Ressourceneinsatz zu sorgen.	

[1020] IKT-Strategie vom 25. April 2018 auf Antrag der Finanzdirektion; Strategie Digitaler Wandel an den Schulen der Sekundarstufe II vom 20. März 2019 auf Antrag der Bildungsdirektion; Informationssicherheitsstrategie (Cybersicherheitsstrategie) vom 4. Mai 2022 auf Antrag der Finanzdirektion; Strategie Digitale Verwaltung 2025+ vom 19. Januar 2025 auf Antrag der Staatskanzlei und der Finanzdirektion.

18.3 Rechtliche Grundlagen

18.3.1 Regelungen zur Informationssicherheit

9. Die PUK Datensicherheit fordert, die Regelungen zur Informationssicherheit rechtlich stärker zu verankern.	Kapitel 10
10. Die PUK Datensicherheit ist der Ansicht, dass die wesentlichen organisatorischen Zuständigkeiten auf Verordnungsstufe zu regeln sind, da sich die Verwaltung in ihrer Arbeitsweise an den rechtlichen Grundlagen orientiert.	Kapitel 14
11. Die heutigen Governance-Strukturen sind nach dem Eindruck der PUK Datensicherheit äusserst komplex ausgestaltet und speisen sich aus unterschiedlichen Quellen und Vorgaben. Sie sind für Aussenstehende, aber auch für Mitarbeitende der kantonalen Verwaltung in dieser Art nur schwer nachvollziehbar. Aus Sicht der PUK Datensicherheit bietet die laufende Überführung der IKT-Strukturen in eine Verordnung die Gelegenheit, auch die Verantwortlichkeiten im Bereich der Informationssicherheit im Einklang mit der neuen IKT-Verordnung festzuschreiben.	
12. Für eine wirkungsvolle Umsetzung der Informationssicherheit fordert die PUK Datensicherheit eine Vereinfachung und Klärung der Strukturen.	

18.3.2 Allgemeine Informationssicherheitsrichtlinie (AISR)

13. Konkret fordert die PUK Datensicherheit, die AISR als Verordnung zu erlassen, um ihr mehr Gewicht und Geltungskraft zu verleihen.	Kapitel 14
14. Die neue AISR vom 16. April 2025 illustriert die weiterhin starken Autonomiebestrebungen in den Direktionen und der Staatskanzlei. Sie sieht vor, dass die Direktionen eigene AISR auf der Ebene der Direktion oder der Staatskanzlei erlassen sollen. Dieses Ansinnen erachtet die PUK Datensicherheit als verfehlt und nicht zielführend. Es ist im Grundsatz abzulehnen. Wesentliche organisatorische Festlegungen für die Direktionen und die Staatskanzlei sind kantonal zu definieren. Direktionsspezifische Bestimmungen sollen nur ergänzenden Charakter haben.	
15. Die PUK Datensicherheit verlangt vom Regierungsrat, die heute in der AISR festgelegten, übergeordneten Informationssicherheitsregelungen so anzupassen, dass im Grundsatz kantonale Lösungen festzulegen und umzusetzen sind. Es ist sicherzustellen, dass direktionseigene Präzisierungen und Richtlinien nur besondere, direktionsspezifische Risiken adressieren.	
16. Die PUK Datensicherheit sieht den Gesamtregierungsrat und das SDI in der Pflicht, die Umsetzung der Bestimmungen zur Informationssicherheit eng zu begleiten und grundsätzlich kantonale Vorgaben zu machen.	

18.3.3 Revision des Archivgesetzes

17. Die PUK Datensicherheit ist der Ansicht, dass bei der Revision des Archivgesetzes darauf zu achten ist, dass die Vorgaben zur Aktenführung, die Anbietepflicht, die Garantie für die korrekte Löschung der vom Staatsarchiv nicht übernommenen Unterlagen sowie die diesbezüglichen Zuständigkeiten klar aus dem Gesetz hervorgehen.	Kapitel 11
18. Überdies ist zu gewährleisten, dass in allen Direktionen und der Staatskanzlei keine Aufräumaktionen stattfinden, ohne dass die für die Amtsstelle zuständige Person des Staatsarchivs informiert und allenfalls beteiligt wird.	

18.3.4 Regelung der Amtsübergaben

19. Die PUK Datensicherheit regt an, sich auch auf der Ebene des ganzen Kantons Gedanken zu machen, wie bei Amtsübergaben die nachfolgenden Funktionsträger strukturiert und umfassend über die bestehenden Probleme und Herausforderungen informiert werden können. Diese heiklen Übergänge sind besser auszugestalten und zu regeln.	Kapitel 11

18.4 Sicherheitsorganisation

20. Die PUK Datensicherheit unterstützt das im Rahmen der neuen IKT-Verordnung angedachte Weisungsrecht für das AFI im Bereich der Grundversorgung ausdrücklich und fordert dessen Implementierung.	Kapitel 14
21. Für die PUK Datensicherheit ist es angezeigt, auch den ISIK im Bereich der direktionsübergreifenden Informationssicherheit mit einem Weisungsrecht auszustatten.	
22. Die organisatorische Unabhängigkeit des ISIK muss aus Sicht der PUK Datensicherheit so gewährleistet sein, dass er seine Aufgabe gesamtkantonal erfüllen kann.	
23. Für die Umsetzung in den Direktionen sind die ISID zentral. Daher sind für die PUK Datensicherheit die ISID-Positionen in allen Direktionen und der Staatskanzlei nicht der IT-Leitung zu unterstellen. Werden die ISID tief in der Hierarchie angesiedelt und dem Leiter der Informatik unterstellt, können sie keine Wirkung entfalten. Konkret sind die ISID in der Nähe der Direktionsleitung oder der Generalsekretärinnen oder Generalsekretäre anzusiedeln. Die neue AISR sieht richtigerweise vor, eine Berichterstattung über die Informationssicherheitsrisiken an die Leitung einzurichten. Weiter ist die Position der ISID gegenüber den Amtsleitungen mit einem Weisungsrecht im Bereich der Informationssicherheit zu stärken.	
24. Es sind zur Verortung und zu den Aufgaben der ISID zwingend kantonale Governance-Vorgaben notwendig, damit die ISID in allen Direktionen und der Staatskanzlei Wirkung entfalten können und die Direktionsleitungen regelmässig über die Informationssicherheitsrisiken informiert werden.	

18.5 Koordinierte Weiterentwicklung der Informationssicherheit in den Direktionen und der Staatskanzlei

18.5.1 Konkretisierung der Besonderen Informationssicherheitsrichtlinien (BISR)

25. Die Konkretisierung der BISR hat aus Sicht der PUK Datensicherheit über alle Direktionen und die Staatskanzlei im Grundsatz koordiniert zu erfolgen.	Kapitel 14
26. Zur wirkungsvollen Umsetzung der BISR-Vorgaben ist es aus Sicht der PUK Datensicherheit zwingend notwendig, diese Herausforderungen innerhalb der FAGIS gemeinsam und arbeitsteilig anzugehen. Im Bereich der unterschiedlichen Instrumente ist eine Koordinierung anzustreben, damit auch eine gesamtkantonale Aggregierung der Risiken und Erkenntnisse erleichtert wird.	
27. Die PUK Datensicherheit nimmt den Aufbau der gesamtkantonalen Dienstleistungen positiv zur Kenntnis. Aus ihrer Sicht sind jedoch kantonal bereitgestellte Dienstleistungen für alle Direktionen verpflichtend auszugestalten.	Kapitel 15
28. Konkret zu regeln und koordiniert aufzubauen sind beispielsweise die Sicherheits- und Lieferantenüberprüfungen in allen Direktionen und der Staatskanzlei.	
29. Generell ist die PUK Datensicherheit der Ansicht, dass auch die Regelungen der Datenbearbeitung auf Verordnungsstufe zu regeln sind. Massnahmen zum Schutz der Daten (§ 7 IDG) sind mit der Verbindlichkeitserklärung der heutigen AGB im Bereich der Informationsbearbeitung durch Dritte nicht ausreichend konkretisiert. Die AGB sind um zusätzliche Vorgaben zu erweitern.	
30. Die PUK Datensicherheit sieht in der allenfalls notwendigen Präzisierung der rechtlichen Grundlagen zur Personensicherheitsüberprüfung eine Chance, diese kantonal einheitlich und auf einem guten Niveau festzulegen.	

18.5.2 Entsorgung und Löschung

31. Die PUK Datensicherheit erwartet, dass Entsorgungsprozesse kantonal einheitlich abgewickelt werden. Dabei sind gesetzliche Vorgaben sowie internationale Normen und Standards einzuhalten, um die Qualität und Sicherheit der Datenvernichtung zu gewährleisten.	Kapitel 15 und 18
32. Die PUK Datensicherheit ist der Ansicht, dass die Datenlöschung bei öffentlichen Organen im Inland gemäss den hier geltenden Normen und anerkannten Standards zu erfolgen hat.	Kapitel 18
33. Um eine vollständige und nachvollziehbare Datenlöschung zu gewährleisten, sind alle Datenträger in Anlagelisten mit Seriennummern zu erfassen.	
34. Schliesslich ist in Zukunft auch eine Harmonisierung der bisher separat laufenden Prozesse der Kantonspolizei sowie der verbliebenen IKT-Abteilungen der Direktionen und der Staatskanzlei mit den kantonalen Prozessen anzustreben.	Kapitel 15

18.5.3 Lieferantenprüfungen

35. Die meisten Direktionen haben keine eigenen Lieferantenüberprüfungen vorgenommen. Es sind systematische Prüfungen für alle Lieferanten und einheitliche Vorgaben und Prozesse für den gesamten Kanton zu definieren.	Kapitel 15

18.5.4 Schulungen

36. Die PUK Datensicherheit erachtet es als dringend angezeigt, die Schulungen zur Informationssicherheit in allen Direktionen und der Staatskanzlei verpflichtend auszugestalten.	Kapitel 15

18.5.5 Umgang mit Informationssicherheitsrisiken der Cloud-Lösungen

37. Die Risiken in Bezug auf die Cloud-Lösung M365 sind sehr ernst zu nehmen und es ist durch den Regierungsrat vertieft zu prüfen, ob eine Ablösung von M365 anzustreben ist. Generell ist bei Cloud-Lösungen darauf zu achten, dass sich die Daten sowohl auf Servern im Inland befinden als auch individuell verschlüsselt und zusätzlich wirkungsvoll vor fremdem Zugriff geschützt sind.	Kapitel 14
38. Vor dem Hintergrund dieser Risiken ist es unabdingbar, dass die Klassifizierung, Nutzung und Speicherung der Daten heute in allen Direktionen und der Staatskanzlei sorgfältig vorgenommen werden. Dabei ist die Allgemeine Nutzungsrichtlinie zu beachten, welche die Nutzung und Speicherung von vertraulichen und geheimen Daten sowie von besonderen Personendaten auf der M365-Cloud explizit verbietet. Die Mitarbeitenden sind diesbezüglich stärker als heute durch die Direktionen und die Staatskanzlei zu unterstützen. Dabei sind klare, verständliche Regelungen festzulegen und kantonale Hilfsmittel, auch technischer Art, zu entwickeln.	
39. Ergänzend dazu ist der Umgang mit Cloud-Lösungen stärker als bisher durch die Aufsichtskommissionen kritisch zu begleiten.	

18.6 Informationssicherheit bei von der AISR nicht erfassten kantonalen Stellen

40. Die PUK Datensicherheit begrüsst es, dass die KAPO ihre IT-Projekte dem OIS freiwillig vorlegt und sich damit mit den kantonalen Entwicklungen koordiniert. Aus Sicht der PUK Datensicherheit gilt es diese Praxis nun auch verbindlich festzulegen. Die Zusammenarbeit der KAPO mit dem OIS ist zu formalisieren.	Kapitel 14
41. Die PUK Datensicherheit erwartet, dass der Regierungsrat respektive die zuständigen Direktionen gegenüber den selbständigen öffentlich-rechtlichen Anstalten im Rahmen der Eigentümerstrategien verbindliche Vorgaben zur Informationssicherheit adressiert und überprüft.	Kapitel 16

18.7 Kommunikation

18.7.1 Information des gesamten Regierungsrates

42. Eine Information des Regierungsrates und der Aufsichtskommissionen über die laufenden Administrativuntersuchungen in den Direktionen und der Staatskanzlei ist nicht etabliert. Die PUK erachtet es als dringend notwendig, dass der Gesamtregierungsrat von den Direktionen und der Staatskanzlei über laufende Administrativuntersuchungen, welche über personalrechtliche Abklärungen von geringer Tragweite hinausgehen, in geeigneter Form in Kenntnis zu setzen ist.	Kapitel 12 und 13

18.7.2 Kommunikation gegenüber den Aufsichtskommissionen

43. Die PUK Datensicherheit erwartet, dass der Regierungsrat den Aufsichtskommissionen über die laufenden Administrativuntersuchungen in den Direktionen und der Staatskanzlei, welche über personalrechtliche Abklärungen von geringer Tragweite hinausgehen, in geeigneter Form Bericht erstattet.	Kapitel 12 und 13
44. Im Umgang mit weiteren kantonalen Stellen, wie den Aufsichtskommissionen oder der Datenschutzbeauftragten, sind klar definierte Prozesse zu erarbeiten.	
45. Analog zu der von der Finanzkontrolle vorgeschlagenen Berichterstattung über alle relevanten IT-Schlüsselprojekte ist auch zu den Informationssicherheitsrisiken der Direktionen und der Staatskanzlei eine halbjährliche oder jährliche Berichterstattung einzurichten, die ebenfalls die Bedürfnisse der exekutiven Dienstaufsicht und der parlamentarischen Oberaufsicht erfüllt.	Kapitel 14
46. Weiter ist vertieft zu prüfen, ob die Auditberichte sowie die internen Berichte der Datenschutzbeauftragten, ähnlich den Semesterberichten der Finanzkontrolle, den Aufsichtskommissionen zur Kenntnis gebracht werden sollen.	

18.8 Interne und externe Aufsicht und Oberaufsicht

18.8.1 Eigene Audittätigkeit der Direktionen und der Staatskanzlei

47. Die Direktionen und die Staatskanzlei sind in der Pflicht, ihre eigenen Risiken im Bereich der Informationssicherheit mittels eigener Audits regelmässig zu eruieren. Diese sind im Sinne der Empfehlung 8 mit dem ISIK zu teilen.	Kapitel 14

18.8.2 Stärkung der externen Aufsicht

48. Die externe Aufsicht über die Informationssicherheit ist aus Sicht der PUK Datensicherheit wesentlich zu stärken. Allenfalls ist hierfür über die bestehenden Organe hinaus eine externe Aufsicht über die Informationssicherheit in der kantonalen Verwaltung einzurichten. Kapitel 14

49. Ergänzend zur Weiterführung der externen Audits zur kantonalen Informationssicherheit, wie sie heute in der AISR vorgesehen sind, sieht die PUK Datensicherheit drei Möglichkeiten, um die Aufsicht im Bereich der Informationssicherheit zu stärken:
    a. Die Verstärkung der Kontrollaktivität der Datenschutzbehörde im Bereich der Informationssicherheit und eine Neugestaltung der diesbezüglichen Berichterstattung gegenüber den Aufsichtskommissionen. Auf diese Weise wäre es auch mit dem heutigen risikobasierten Ansatz besser möglich, die Direktionen, die Staatskanzlei und die selbständigen öffentlich-rechtlichen Anstalten zu beraten und zu prüfen.
    b. Die Stärkung der Ressourcen und Möglichkeiten der Finanzkontrolle für Prüfungen im Bereich der Informationssicherheit, die aktuell nicht zum Kerngeschäft der Finanzkontrolle gehören. Dazu müsste der bestehende gesetzliche Auftrag entsprechend erweitert werden. Allenfalls ist auch eine Erweiterung des Adressatenkreises der Berichterstattung der Finanzkontrolle zu prüfen, damit jene kantonalen Stellen, die direktionsübergreifend wirken, namentlich der ISIK und das Kompetenzzentrum Informationssicherheit, diese Informationen ebenfalls erhalten.
    c Die Schaffung einer neuen, unabhängigen Instanz zur Informationssicherheitskontrolle, welche die externe Aufsicht in diesem Bereich wahrnimmt und zuhanden der Aufsichtskommissionen berichtet.

50. Die PUK Datensicherheit erinnert schliesslich auch die Aufsichtskommissionen des Kantonsrates dringend daran, die Umsetzung der Informationssicherheit im Rahmen der begleiteten Oberaufsicht engmaschig zu verfolgen. Zu diesem Zweck hat der Kantonsrat eine wirksame Oberaufsicht durch seine bisherigen Strukturen oder gegebenenfalls durch eine neu zu schaffende Aufsichtskommission für IT-Projekte und Informationssicherheit sicherzustellen.

Binär-Code für «Bericht der Parlamentarischen Untersuchungskommission Datensicherheit»