Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 4. Juni 2025

572. Kantonspolizei, Weiterführung und Betrieb eines Security Information and Event Management Systems sowie eines Security Operations Centers (gebundene Ausgabe und Vergabe)

A. Ausgangslage

Mit RRB Nr. 277/2021 wurde der Ausbau und der vierjährige Betrieb des zentralen Log-Management-Systems bei der Kantonspolizei (Kapo) (ZLMK) mit Gesamtausgaben von 1,59 Mio. Franken für eine vierjährige Mindestvertragslaufzeit bis Mitte 2025 bewilligt. Das ZLMK sammelt von Servern, Netzwerkelementen und Applikationen Protokolldateien über Zugriffe und Änderungen in IT-Systemen, speichert diese und ermöglicht u. a. eine Analyse durch ein Security Operations Center (SOC). Mit RRB Nr. 139/2021 wurde dazu der Aufbau und Betrieb eines Security Information and Event Management Systems (SIEM) sowie des SOC bei der Kapo mit Gesamtausgaben von 3,46 Mio. Franken für eine vierjährige Vertragslaufzeit bis Mitte 2025 bewilligt, das sicherheitsrelevante Daten aus verschiedenen Systemen sammelt, auswertet und bei Sicherheitsvorfällen automatisiert alarmiert sowie sicherheitsrelevante Vorgänge der IT-Landschaft bei der Kapo rund um die Uhr während 365 Tagen überwacht, auswertet und nötigenfalls Schutzmassnahmen ergreift.

Der Betrieb des SIEM, das im ZLMK integriert ist, sowie die Dienstleistungen des SOC sollen weitergeführt und weiterentwickelt werden.

B. Beschaffung und Vergabe

Die Kapo führte im September 2024 eine öffentliche Ausschreibung für den weiteren Betrieb und die Weiterentwicklung des SIEM und des SOC mit vier Losen durch und integrierte darin das ZLMK (Los 1: First- und Second-Level-Analyse sowie Automatisierung; Los 2: Krisenmanagement und Krisenvorbereitung; Los 3: Betrieb der SOC-Infrastruktur; Los 4: Bereitstellung von Lizenzen im Bereich Security, u. a. für ZLMK). Für die Lose 1–4 soll für Dienstleistungen und Lizenzen ein Rahmenvertrag mit Einzelverträgen für vorerst eine fünfjährige Mindestvertragslaufzeit (Mitte 2025 bis Mitte 2030) ohne Bezugspflicht durch die Kapo mit den Unternehmen abgeschlossen werden, die sich ohne Kündigung automatisch um jeweils ein weiteres Jahr, bis auf eine Vertragslaufzeit von längstens acht Jahren (bis Mitte 2033), verlängern können.

Für Los 1 wurden vier sowie für die Lose 2, 3 und 4 je fünf gültige Angebote eingereicht. Die Angebote der Anomal GmbH, Dübendorf, vom 21. Oktober 2024 (Lose 1 und 3), der Oneconsult AG, Zürich, vom 26. November 2024 (Los 2) sowie der terreActive Swiss Post Cybersecurity AG, Aarau, vom 12. Mai 2025 (Los 4) erfüllten sämtliche Eignungskriterien und sind die vorteilhaftesten, weshalb ihnen, gestützt auf Art. 41 der Interkantonalen Vereinbarung über das öffentliche Beschaffungswesen (LS 720.1) der Zuschlag zu erteilen ist.

Die Vergabesummen für die Weiterführung des SIEM- und SOC-Betriebs (Lose 1–4) für vorerst eine fünfjährige Mindestvertragslaufzeit bis Mitte 2030 bzw. bei einer Verlängerung um drei Jahre bis längstens Mitte 2033 setzen sich wie folgt zusammen:

Vergabeübersicht (in Franken, gerundet; einschliesslich MWSt)	**Erfolgsrechnung** (jährliche Aufwendungen)	**Total 5 Jahre** (Mindestvertragslaufzeit)	**Total 8 Jahre** (maximale Vertragslaufzeit)
First- und Second-Level-Analyse sowie Automatisierung (Los 1) (Anomal GmbH, Dübendorf; Angebot vom 21. Oktober 2024)	287 872	1 439 360	2 302 976
Unvorhergesehenes/Teuerung/Rundungen	12 128	60 640	97 024
Vergabesumme Los 1, Anomal GmbH	***300 000***	***1 500 000***	***2 400 000***
Krisenmanagement und Krisenvorbereitung (Los 2) (Oneconsult AG, Zürich; Angebot vom 26. November 2024, betraglich reduziert)	116 760	583 800	934 080
Unvorhergesehenes/Teuerung/Rundungen	3 240	16 200	25 920
Vergabesumme Los 2, Oneconsult AG	***120 000***	***600 000***	***960 000***
Betrieb der SOC-Infrastruktur (Los 3) (Anomal GmbH, Dübendorf; Angebot vom 21. Oktober 2024)	71 951	359 755	575 608
Unvorhergesehenes/Teuerung/Rundungen	8 049	40 245	64 392
Vergabesumme Los 3, Anomal GmbH	***80 000***	***400 000***	***640 000***
Bereitstellung von Lizenzen im Bereich Security, u. a. für ZLMK (Los 4; Wegfall des laufzeitbedingten Preisvorteils sowie zusätzliche Lizenzen für 6. bis 8. Betriebsjahr) (terreActive Swiss Post Cybersecurity AG, Aarau; Angebot vom 12. Mai 2025)	781 780	3 908 900	8 139 540
Unvorhergesehenes/Teuerung/Rundungen sowie Währungsrisiko	38 220	191 100	660 460
Vergabesumme Los 4, terreActive Swiss Post Cybersecurity AG	***820 000***	***4 100 000***	***8 800 000***
Vergaberelevantes Zwischentotal (Lose 1–4)	***1 258 363***	***6 291 815***	***11 952 204***
Unvorhergesehenes/Teuerung/Rundungen sowie für Los 4 ein Währungsrisiko	61 637	308 185	847 796
Gesamte Vergabesumme (Lose 1–4)	**1 320 000**	**6 600 000**	**12 800 000**

Die Vergaben an die Oneconsult AG, Zürich, für das Krisenmanagement und die Krisenvorbereitung (Los 2) sowie an die Anomal GmbH, Dübendorf, für den Betrieb der SOC-Infrastruktur (Los 3) fallen gestützt auf § 34 in Verbindung mit § 39 lit. a der Finanzcontrollingverordnung

(LS 611.2) in die Kompetenz der Sicherheitsdirektion. Die Mehrkosten im Vergleich zu RRB Nrn. 139/2021 und 227/2021 begründen sich vor allem durch zusätzliche Lizenzen sowie ab dem 6. bis 8. Betriebsjahr durch den Wegfall des laufzeitbedingten Preisvorteils (vgl. Los 4), verbunden mit der Einbindung von weiteren rund 800 Applikationen und Systemen.

Für die fachliche Unterstützung und zur Aktualisierung der SOC-Prozesse an die heutigen Anforderungen sowie für die Durchführung der Submission hat die Kapo mit Verfügung vom 19. April 2024 gebundene Ausgaben von Fr. 68 492 bewilligt. Diese Ausgabenbewilligung ist Teil der zu bewilligenden Gesamtausgabe und ist somit aufzuheben.

C. Gebundene Ausgabe und Finanzierung

Die Aufwendungen für die Weiterführung und den Betrieb von SIEM (einschliesslich ZLMK) sowie des SOC für vorerst eine fünfjährige Mindestvertragslaufzeit bis Mitte 2030 bzw. bei einer Verlängerung um drei Jahre bis längstens Mitte 2033 setzen sich wie folgt zusammen:

Kostenübersicht (in Franken, gerundet; einschliesslich MWSt)	**Erfolgsrechnung** (einmalig)	**Erfolgsrechnung** (jährliche Aufwendungen)	**Total 5 Jahre** (Mindestvertragslaufzeit)	**Total 8 Jahre** (maximale Vertragslaufzeit)
Unterstützung zur Aktualisierung der SOC-Prozesse aus fachlicher Sicht an die heutigen Anforderungen sowie für die Durchführung der Submission (Verfügung der Kapo vom 19. April 2024)	68 492		68 492	68 492
First- und Second-Level-Analyse sowie Automatisierung (Los 1) (Anomal GmbH, Dübendorf; Angebot vom 21. Oktober 2024)		287 872	1 439 360	2 302 976
Krisenmanagement und Krisenvorbereitung (Los 2) (Oneconsult AG, Zürich; Angebot vom 26. November 2024, betragsmässig reduziert)		116 760	583 800	934 080
Betrieb der SOC-Infrastruktur (Los 3) (Anomal GmbH, Dübendorf; Angebot vom 21. Oktober 2024)		71 951	359 755	575 608
Bereitstellung von Lizenzen im Bereich Security, u. a. für ZLMK (Los 4; Wegfall des laufzeitbedingten Preisvorteils sowie zusätzliche Lizenzen für 6. bis 8. Betriebsjahr) (terreActive Swiss Post Cybersecurity AG, Aarau; Angebot vom 12. Mai 2025)		781 780	3 908 900	8 139 540
Zwischentotal (Lose 1–4)	***68 492***	***1 258 363***	***6 360 307***	***12 020 696***
Unvorhergesehenes/Teuerung/Rundungen sowie für Los 4 ein Währungsrisiko	11 508	61 637	319 693	859 304
Total Aufwendungen (Lose 1–4)	**80 000**	**1 320 000**	**6 680 000**	**12 880 000**

Sämtliche Ausgaben sind zur Erfüllung von gesetzlich vorgeschriebenen Aufgaben (u. a. aus Polizeiorganisationsgesetz [LS 551.1]) zwingend erforderlich und dienen namentlich der Beschaffung und Erneuerung der für die Verwaltungstätigkeit erforderlichen sachlichen Mittel. Sie gelten deshalb als gebundene Ausgabe im Sinne von § 37 Abs. 2 lit. a des Gesetzes über Controlling und Rechnungslegung (LS 611).

Die Betriebskosten für SIEM und das SOC betragen jährlich durchschnittlich Fr. 1 320 000 bzw. für vorerst eine fünfjährige Mindestvertragslaufzeit insgesamt Fr. 6 600 000 sowie einschliesslich einmaliger Aufwendungen von Fr. 80 000 insgesamt Fr. 6 680 000. Von diesem Betrag wurden die bisher angefallenen Aufwendungen von insgesamt Fr. 63 865 der Rechnung 2024 belastet und der Restbetrag von Fr. 6 616 135 kann im Budget 2025 (rund 0,8 Mio. Franken) sowie im Konsolidierten Entwicklungs- und Finanzplan (KEF) 2025–2028, Planjahre 2026–2028 (jährlich rund 1,3 Mio. Franken) kompensiert werden. Die Beträge werden der Erfolgsrechnung der Leistungsgruppe Nr. 3100, Kantonspolizei, belastet. Die Beträge für das Planjahr 2029 (rund 1,3 Mio. Franken) und 2030 (rund 1,7 Mio. Franken, infolge Wegfalls des laufzeitbedingten Preisvorteils und der zusätzlichen Lizenzen, davon 0,7 Mio. Franken bis Mitte 2030) sowie ab 2031 (jährlich rund 2,1 Mio. Franken) sind im KEF neu einzustellen. Es fallen keine weiteren Folgeaufwendungen an.

Mit Ausgabenbewilligung der Kapo vom 19. April 2024 wurde für die Unterstützung zur Aktualisierung der SOC-Prozesse aus fachlicher Sicht an die heutigen Anforderungen sowie für die Durchführung der Submission eine einmalige gebundene Ausgabe von insgesamt Fr. 68 492 bewilligt. Diese Ausgabenbewilligung ist Teil der zu bewilligenden Gesamtausgabe von Fr. 6 680 000 und ist somit aufzuheben.

Das Vorhaben wurde mit dem Amt für Informatik und dem Gremium Operative Informatiksteuerung (OIS) abgestimmt (u. a. anlässlich der AFI-Sitzung vom 1. Oktober 2024 und der OIS-Sitzung vom 13. Februar 2025). Es gab keine Einwände.

Das Projektcontrolling wird durch die Abteilung Informatik der Kapo sichergestellt.

Auf Antrag der Sicherheitsdirektion

beschliesst der Regierungsrat:

I. Für die Weiterführung des Security Information and Event Management Systems sowie des Security Operations Centers bei der Kantonspolizei für eine fünfjährige Mindestvertragslaufzeit voraussichtlich bis Mitte 2030 wird eine gebundene Ausgabe von Fr. 6 680 000 zulasten der Erfolgsrechnung der Leistungsgruppe Nr. 3100, Kantonspolizei, bewilligt.

II. Der Auftrag für die Weiterführung und den Betrieb des Security Information and Event Management Systems sowie des Security Operations Centers (Lose 1 und 4) bei der Kantonspolizei für eine fünfjährige Mindestvertragslaufzeit bis Mitte 2030 bzw. bei einer Verlängerung um drei Jahre bis längstens Mitte 2033 wird gemäss Erwägung B an folgende Zuschlagsempfängerinnen vergeben:

– Los 1 für die First- und Second-Level-Analyse sowie Automatisierung gemäss Angebot vom 21. Oktober 2024 zu jährlich Fr. 287 872 bzw. insgesamt Fr. 1 439 360 an die Anomal GmbH, Dübendorf. Die Vergabesumme kann sich für Unvorhergesehenes auf Fr. 1 500 000 bzw. bei einer Vertragsverlängerung um drei Jahren bis längstens 2033 auf Fr. 2 400 000 erhöhen.
– Los 4 für die Bereitstellung von Lizenzen im Bereich Security mit Optionen gemäss Angebot vom 12. Mai 2025 zu jährlich Fr. 781 780 bzw. insgesamt Fr. 3 908 900 an die terreActive Swiss Post Cybersecurity AG, Aarau. Die Vergabesumme kann sich für Unvorhergesehenes sowie für Währungs- und Lizenzmodell-Risiken auf Fr. 4 100 000 bzw. bei einer Vertragsverlängerung um drei Jahren bis längstens 2033 auf Fr. 8 800 000 erhöhen.

III. Die Kantonspolizei wird ermächtigt, für das Los 1 mit der Anomal GmbH, Dübendorf, und für das Los 4 mit der terreActive Swiss Post Cybersecurity AG, Aarau, einen Rahmenvertrag mit Einzelverträgen gemäss Erwägung B abzuschliessen.

IV. Die Ausgabenbewilligung der Kantonspolizei vom 19. April 2024 für die Unterstützung zur Aktualisierung der SOC-Prozesse aus fachlicher Sicht an die heutigen Anforderungen sowie für die Durchführung der Submission wird aufgehoben.

V. Dieser Beschluss ist bis zur Veröffentlichung des Zuschlags auf simap.ch nicht öffentlich.

VI. Mitteilung an die Finanzdirektion und die Sicherheitsdirektion.

Vor dem Regierungsrat
Die Staatsschreiberin:

Kathrin Arioli