

Antrag des Regierungsrates vom 5. März 2025

5977 a

Polizeigesetz (PolG)

(Änderung vom: Datenbearbeitung)

Der Kantonsrat,

nach Einsichtnahme in die Anträge des Regierungsrates vom 28. August 2024 und vom 5. März 2025,

beschliesst:

I. Das Polizeigesetz vom 23. April 2007 wird wie folgt geändert:

§ 2. Abs. 1 unverändert.

Geltungsbereich

² Für die polizeiliche Tätigkeit im Rahmen der Strafverfolgung gelten nur § 32 i sowie die Bestimmungen des 3., 5. und 8. Abschnitts. Im Übrigen richtet sich diese polizeiliche Tätigkeit namentlich nach den Bestimmungen der Strafprozessordnung und des GOG.

Abs. 3 unverändert.

§ 32. Abs. 1 und 2 unverändert.

Polizeiliche
Observation

³ Bestehen ernsthafte Anzeichen für eine Straftat im Sinne von Art. 269 Abs. 2 StPO, kann die Polizei zu deren Verhinderung oder Erkennung technische Überwachungsgeräte zur Feststellung des Standortes von Personen oder Sachen einsetzen. Die Aufnahmen können zu Beweis Zwecken gespeichert werden. Der Einsatz bedarf der Genehmigung des Zwangsmassnahmengerichts. Für den Einsatz und das Genehmigungsverfahren gelten Art. 269–279 und 281 StPO sinngemäss. An die Stelle der Staatsanwaltschaft tritt das Polizeikommando.

Abs. 3 und 4 werden zu Abs. 4 und 5.

⁶ Für die Mitteilung einer Massnahme gemäss Abs. 3 gilt Art. 279 StPO sinngemäss.

§ 32 d. ¹ Für folgende Zwecke erfolgt die Überwachung des Strassenverkehrs mit Videogeräten in einer Weise, dass Personen, Fahrzeuge und Kontrollschilder nicht identifiziert werden können:

d. Überwachung
des Strassen-
verkehrs mit
Videogeräten

- a. Verkehrsmanagement,
- b. Ereignisbewältigung bei Verkehrsunfällen,
- c. Verbesserung der Strasseninfrastruktur und der Verkehrssicherheit.

² Für folgende Zwecke kann die Polizei die Videoaufzeichnungen des Strassenverkehrs vom betroffenen Abschnitt für die notwendige Zeitspanne in hochauflösender Weise so auswerten, dass auch Personen, Fahrzeuge und Kontrollschilder identifiziert werden können:

- a. bei ernsthaften Anzeichen für eine Gefahr für Personen oder Sachen, um die Gefahr zu lokalisieren und zu beseitigen,
- b. um den Einsatz für die Bewältigung grösserer Ereignisse zu führen,
- c. um die Verkehrsführung des betreffenden Abschnitts zu ändern.

³ Zu den Zwecken gemäss Abs. 1 und 2 kann die Polizei Daten beziehen von Verkehrsmanagement- und -überwachungssystemen

- a. des Bundesamtes für Strassen,
- b. des kantonalen Tiefbauamtes.

⁴ Die Polizei regelt die Zugriffsberechtigungen und die technische Umsetzung der Datenauswertung. Sie führt ein Verzeichnis der stationären Videoüberwachungsanlagen.

§§ 32 d und 32 e werden zu §§ 32 e und 32 f.

Informations-
beschaffung im
virtuellen Raum

a. Öffentlich
zugängliche
Informationen

§ 32 g. ¹ Die Polizei kann zur Erfüllung ihrer Aufgaben im Internet oder in anderen Netzwerken öffentlich zugängliche Informationen beschaffen und bearbeiten.

² Für die Verwendung von Analysesystemen zur Beschaffung und Bearbeitung gilt § 52 a.

b. Nicht öffent-
lich zugängliche
Informationen

§ 32 h. ¹ Um Gefahren für das Leben einer Person sowie Straftaten gemäss Art. 269 Abs. 2 StPO zu erkennen und zu verhindern, kann das Polizeikommando mit Genehmigung des Zwangsmassnahmengerichts den Einsatz von Software anordnen, um im Internet oder in anderen Netzwerken nicht öffentlich zugängliche Informationen zu beschaffen und zu bearbeiten sowie einen allfälligen Zugriffsschutz zu umgehen.

² Der Einsatz darf nur angeordnet werden, wenn

- a. ernsthafte Anzeichen für solche Gefahren oder Straftaten bestehen,
- b. die Schwere dieser Gefahren oder Straftaten die Massnahme rechtfertigt und
- c. andere Massnahmen erfolglos geblieben sind oder die Vorermittlung sonst aussichtslos wäre oder unverhältnismässig erschwert würde.

³ Für die Verwendung von Analysesystemen zur Beschaffung und Bearbeitung gilt zudem § 52 a.

⁴ Nicht zulässig ist die Überwachung des Fernmeldeverkehrs im Sinne von Art. 269 ff. StPO, insbesondere der Einsatz besonderer Informatikprogramme gemäss Art. 269^{ter} StPO.

⁵ Für die Durchführung und Mitteilung des Einsatzes sowie die Beschwerdemöglichkeiten sind Art. 274–279 StPO sinngemäss anwendbar. An die Stelle der Staatsanwaltschaft tritt das Polizeikommando.

⁶ Die erhobenen Daten werden zwei Monate nach Mitteilung des durchgeführten Einsatzes gelöscht, soweit sie nicht für ein Straf-, Zivil- oder Verwaltungsverfahren benötigt werden.

§ 32 i. Die Ausschreibung von Personen und Sachen zwecks verdeckter Registrierung, gezielter Kontrolle und Ermittlungsanfrage gemäss der Verordnung vom 8. März 2013 über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro ist zulässig.

Verdeckte Registrierung, gezielte Kontrolle, Ermittlungsanfrage

§ 32 j. ¹ Die Polizei kann mit Personen zusammenarbeiten, die gegen Zusicherung von Vertraulichkeit aus eigenem Antrieb oder im Auftrag der Polizei Informationen liefern (vertrauliche Quellen)

Quellenführung

- a. zur Erkennung, Verhinderung und Aufklärung von Verbrechen oder Vergehen,
- b. zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung.

² Vertrauliche Quellen verfügen über keine hoheitlichen Befugnisse.

³ Sie dürfen nicht

- a. Straftaten begehen,
- b. Beihilfe zu Straftaten leisten,
- c. Personen zur Begehung von Straftaten anstiften.

⁴ Die Polizei kann vertrauliche Quellen entschädigen und belohnen.

§ 43. ¹ Auf Gesuch der zuständigen zivilen und militärischen Stellen kann die Polizei eine Person auf Sicherheitsrisiken überprüfen, einen Bericht über sie erstellen und eine Einschätzung abgeben, wenn

- a. das Gesetz dies ausdrücklich vorsieht,
- b. die ersuchende Stelle zur Erfüllung ihrer gesetzlichen Aufgaben auf die Informationen angewiesen ist und sie diese weder von der betroffenen Person noch durch andere eigene Erhebungen erhalten kann,

Polizeiliche Berichte zur Person und Personensicherheitsprüfungen

- c. die Person eine sicherheitsrelevante Funktion für die öffentliche Verwaltung oder für mit öffentlichen Aufgaben betraute Private ausübt oder ausüben soll und die Überprüfung zur Gewährleistung der Sicherheit im jeweiligen Bereich erforderlich ist oder
- d. die Person Zugang zu nicht öffentlichen Räumlichkeiten oder Zugriff auf Informationen der öffentlichen Verwaltung hat und die Überprüfung zur Gewährleistung der Sicherheit im jeweiligen Bereich erforderlich ist.

² Das Gesuch nennt den Zweck, die gesetzliche Grundlage und die benötigten Informationen. Die ersuchende Stelle gewährleistet, dass der betroffenen Person vor einem Entscheid zu ihren Ungunsten die Möglichkeit zur Stellungnahme eingeräumt wird.

³ Die Polizei tätigt Erhebungen bei Amtsstellen, aus öffentlich zugänglichen Quellen und bei der betroffenen Person. Dritte werden nur ausnahmsweise und mit ausdrücklichem Auftrag der ersuchenden Stelle befragt.

⁴ Die Polizei kann der ersuchenden Stelle Gebühren auferlegen.

Vor Gliederungstitel «5. Abschnitt: Angehörige der Polizei»

Präventive
Ausschreibung
schutzbedürfti-
ger Personen

§ 44 a. Die Polizei ist zuständig für den Entscheid im Sinne von Art. 32 Abs. 4 der Verordnung (EU) 2018/1862¹, wenn Personen nach Art. 32 Abs. 1 Bst. d und e jener Verordnung zu ihrem eigenen Schutz ausgeschrieben werden müssen.

Daten-
bearbeitung

§ 52.* ¹ Die Polizei und das Forensische Institut Zürich sind befugt, zur Erfüllung ihrer Aufgaben und zur Führung ihrer Geschäftskontrolle Daten zu bearbeiten und dazu geeignete Informationssysteme zu betreiben.

Abs. 2 unverändert.

**Koordinationsbedarf mit Vorlage 5923 (Gesetz über die Information und den Datenschutz [IDG], Totalrevision)*

¹ Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission, Fassung gemäss ABl. L 312 vom 7. Dezember 2018, S. 56.

³ Die Kantonspolizei, die kommunalen Polizeien und das Forensische Institut Zürich gewähren einander Zugriff auf ihre Informationssysteme, soweit dies zur Erfüllung der polizeilichen Aufgaben notwendig ist.

Abs. 4 und 5 unverändert.

§ 52 a. ¹ Die Polizei kann zur Erfüllung ihrer gesetzlichen Aufgaben Analysesysteme einsetzen, welche die Erschliessung, Darstellung und Analyse von Zusammenhängen oder grossen Datenbeständen einschliesslich besonderer Personendaten erlauben.

Einsatz von
Analyse-
systemen
a. Im
Allgemeinen

² Zu den Analysesystemen zählen

- a. einfache Analysesysteme, die von natürlichen Personen festgelegte Regeln für die automatisierte Ausführung von Operationen befolgen,
- b. intelligente Analysesysteme, die auf der Grundlage einer algorithmischen Entscheidungsfindung aus den Eingaben eigenständig Ergebnisse ableiten.

³ Die Polizei darf besondere Personendaten mit intelligenten Analysesystemen bearbeiten, wenn

- a. ernsthafte Anzeichen für Verbrechen, schwere Vergehen oder eine Gefahr für das Leben einer Person bestehen und die Bearbeitung zu ihrer Erkennung oder Verhinderung dient,
- b. die Bearbeitung zum gleichen Zweck wie die Erhebung der Daten erfolgt oder sich auf eine besondere Rechtsgrundlage stützt,
- c. der Zugriff auf solche Systeme durch besonders für das jeweilige System geschulte Mitarbeitende der Polizei erfolgt,
- d. die vom System gemeldeten Ergebnisse durch diese Mitarbeitenden auf ihre Richtigkeit überprüft werden und
- e. der Einsatz solcher Systeme protokolliert wird.

⁴ Unter den Voraussetzungen von Abs. 3 darf die Polizei erhobene Bilder im Einzelfall und unter Verwendung intelligenter Analysesysteme mit anderen polizeilichen Datenbanken abgleichen, um eine Person oder einen Gegenstand zu identifizieren. Die Echtzeit-Gesichtserkennung ist nicht erlaubt. Der Regierungsrat regelt die Einzelheiten.

⁵ Für die Löschung ist § 53 Abs. 2 sinngemäss anwendbar.

b. Im Bereich
der seriellen
Kriminalität

§ 52 b. ¹ Die Polizei kann zur Erkennung und Verhinderung von Verbrechen und Vergehen, die wiederholt und häufig durch gleiche Täterschaften verübt werden, einfache Analysesysteme betreiben, sich an solchen Systemen beteiligen und die dafür notwendigen Daten, einschliesslich besonderer Personendaten, automatisiert auswerten. Zugriff auf die Analysesysteme haben die Mitarbeitenden der Kriminalanalyse.

² Die Polizei kann die dafür notwendigen Daten mit Polizeibehörden des Bundes, der Kantone und der Gemeinden sowie mit dem Bundesamt für Zoll und Grenzsicherheit (BAZG) im Abrufverfahren austauschen. Der Datenaustausch wird protokolliert.

³ Die Polizei bearbeitet in ihren Analysesystemen neben den von ihr erhobenen Daten ausschliesslich solche, die von Polizeibehörden des Bundes, der Kantone und Gemeinden sowie vom BAZG zur Verfügung gestellt wurden.

⁴ Die Löschung der in den Analysesystemen erfassten und darin erzeugten Daten erfolgt

- a. umgehend, sobald sie für die Bearbeitung nicht mehr benötigt werden,
- b. spätestens nach fünf Jahren, wobei anonymisierte Erzeugnisse der Analysesysteme auch länger verwendet werden dürfen.

⁵ Der Regierungsrat regelt die Einzelheiten, insbesondere die eingesetzten Systeme, die Zugriffsberechtigung und die Kategorien von Personendaten, die in den Analysesystemen bearbeitet werden dürfen.

§ 52 a wird zu § 52 c.

Gemeinsames
Informations-
system

§ 54.* ¹ Die Kantonspolizei und die Stadtpolizeien Zürich und Winterthur betreiben gemeinsam ein modulares polizeiliches Informationssystem. Das Forensische Institut Zürich nutzt dieses zur Erfüllung seiner Aufgaben.

Abs. 2–7 unverändert.

**Koordinationsbedarf mit Vorlage 5923 (Gesetz über die Information und den Datenschutz [IDG], Totalrevision)*

Elektronische
Zusammen-
arbeit
a. Im
Allgemeinen

§ 54 a. ¹ Die Polizei kann zur Erfüllung ihrer Aufgaben gemäss §§ 3 ff. dieses Gesetzes und §§ 7 ff. POG sowie für andere, ihr gesetzlich zugewiesene Aufgaben mit Behörden des Bundes, der Kantone und der Gemeinden sowie des Fürstentums Liechtenstein auf elektronischem Weg zusammenarbeiten.

² Sie kann dazu Schnittstellen zwischen eigenen Informationssystemen und jenen des Bundes, der Kantone und der Gemeinden einrichten.

§ 54 b. ¹ Die Polizei darf Daten ihrer polizeilichen Datenbearbeitungs- und Informationssysteme, einschliesslich besonderer Personendaten, im Abrufverfahren anderen Behörden bekannt geben, sich zu diesem Zweck an der gemeinsamen Abfrageplattform beteiligen und ihre Datenbearbeitungs- und Informationssysteme daran anschliessen. Die Bekanntgabe ist nur zulässig:

b. Bekanntgabe von Daten im Abrufverfahren

- a. an Behörden gemäss Abs. 2,
- b. für Aufgaben gemäss Abs. 3,
- c. zu Zwecken gemäss Abs. 4 und
- d. von Datentypen gemäss Abs. 5.

² Folgenden anderen Behörden darf die Polizei im Abrufverfahren Daten bekannt geben:

- a. dem Bundesamt für Polizei für seine Aufgaben gemäss Abs. 3 lit. a–d,
- b. dem BAZG für seine Aufgaben gemäss Abs. 3 lit. a–c,
- c. der Militärpolizei für ihre Aufgaben gemäss Abs. 3 lit. e,
- d. der Transportpolizei für ihre Aufgaben gemäss Abs. 3 lit. f,
- e. den Polizeibehörden der anderen Kantone und ihrer Gemeinden für ihre Aufgaben gemäss Abs. 3 lit. a–d.

³ Folgende Aufgaben berechtigen Personen, die mit deren Erfüllung in den Behörden gemäss Abs. 2 betraut sind, zum Abruf von Daten:

- a. gerichts- und sicherheitspolizeiliche Aufgaben zu den Zwecken gemäss Abs. 4 lit. a–i,
- b. verwaltungspolizeiliche Aufgaben zu den Zwecken gemäss Abs. 4 lit. a–i,
- c. unterstützende und koordinative Aufgaben zu den Zwecken gemäss Abs. 4 lit. a–g,
- d. assistenzpolizeiliche Aufgaben zu den Zwecken gemäss Abs. 4 lit. a–d,
- e. militärpolizeiliche Aufgaben zu den Zwecken gemäss Abs. 4 lit. d und j,
- f. transportpolizeiliche Aufgaben zu den Zwecken gemäss Abs. 4 lit. k.

⁴ Zu folgenden Zwecken darf die Polizei anderen Behörden für die Erfüllung der ihnen gesetzlich zugewiesenen Aufgaben im Abrufverfahren Daten bekannt geben:

- a. Grenzkontrolle an der Schengen-Aussengrenze: Daten gemäss Abs. 5 lit. a,
- b. Personenkontrolle im Inland: Daten gemäss Abs. 5 lit. a–c,
- c. Ermittlung (polizeiliche Vorermittlungen und strafprozessuale Ermittlungen): Daten gemäss Abs. 5 lit. a–c,
- d. Verkehrskontrolle: Daten gemäss Abs. 5 lit. a und b,
- e. Gewaltschutz: Daten gemäss Abs. 5 lit. a,
- f. Bearbeitung von Ausweisverlustmeldungen: Daten gemäss Abs. 5 lit. a,
- g. Personensicherheitsprüfung: Daten gemäss Abs. 5 lit. a,
- h. waffenrechtliche Bewilligung: Daten gemäss Abs. 5 lit. a,
- i. Bewilligung, namentlich für Sicherheitsunternehmen: Daten gemäss Abs. 5 lit. a,
- j. militärpolizeiliche Überprüfung: Daten gemäss Abs. 5 lit. a,
- k. transportpolizeiliche Kontrolle im Rahmen von Art. 7 des Bundesgesetzes vom 18. Juni 2010 über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr: Daten gemäss Abs. 5 lit. a.

⁵ Folgende Datentypen darf die Polizei im Abrufverfahren bekannt geben:

- a. Daten, einschliesslich besonderer Personendaten, über Personen, die als Beschuldigte, Geschädigte oder Opfer in Bezug auf Ereignisse gemäss lit. d oder unabhängig von ihrer Rolle gemäss lit. e registriert sind: Angaben aus der Personendatenbank einschliesslich biometrischer und erkennungsdienstlicher Daten, bevorzugter Vorgehensweisen sowie Haftdaten zu vorläufigen Festnahmen oder polizeilichem Gewahrsam,
- b. Daten über Fahrzeuge, die als gestohlen ausgeschrieben oder im Zusammenhang mit Ereignissen gemäss lit. d oder e registriert sind,
- c. Daten über Sachen, die als gestohlen ausgeschrieben oder im Zusammenhang mit Ereignissen gemäss lit. d oder e registriert sind,

- d. Daten über Straftaten, ausgenommen Daten über Fälle gemäss § 54 f Abs. 1; bei Übertretungen darf aber im Abrufverfahren nur deren Vorhandensein und nicht deren Inhalt bekannt gegeben werden,
- e. Daten über Fälle zu aussergewöhnlichen Todesfällen, Vermissten, Ausweisverlusten, fürsorglichen Unterbringungen, Gewaltschutzverfahren, Suizidversuchen, Aufenthaltsnachforschungen, Entweichungen und Entlaufen, Fundsachen sowie Verdachtsmeldungen zu Verbrechen und Vergehen.

⁶ Werden Daten eines Datentyps gemäss Abs. 5 bekannt gegeben, dürfen auch die mit ihnen verknüpften Daten der anderen Datentypen bekannt gegeben werden. Journaldaten und andere im System abgelegte Dokumente wie Rapporte und Einvernahmen werden im Abrufverfahren nicht bekannt gegeben.

⁷ Die Zugriffe werden protokolliert und stichprobenweise kontrolliert. Die Ergebnisse der Kontrollen werden jährlich der oder dem Beauftragten für den Datenschutz vorgelegt. Die Zugriffsprotokolle können auf Anfrage den zuständigen eidgenössischen oder kantonalen Aufsichtsbehörden herausgegeben werden.

§ 54 c. Die Polizei darf die Daten aus Systemen von ausserkantonalen Behörden abfragen und bearbeiten, soweit dies die massgeblichen rechtlichen Grundlagen zulassen.

c. Bearbeitung von Daten aus Systemen anderer Behörden

- § 54 d. Der Regierungsrat regelt durch Verordnung,
- a. bei welchen eigenen Informationssystemen die Polizei gemäss §§ 54 a und 54 b Schnittstellen einrichten kann,
 - b. welche Attribute aus den in § 54 b Abs. 5 genannten Datentypen anderen Behörden bekannt gegeben werden.

d. Regelungsbefugnisse

§ 54 e. Für den direkten Informationsaustausch mit Polizei- und Strafverfolgungsbehörden anderer Staaten, die mit der Schweiz über eines der Schengen-Assoziierungsabkommen verbunden sind (Schengen-Staaten), finden die bundesrechtlichen Bestimmungen über den Informationsaustausch zwischen den Strafverfolgungsbehörden des Bundes und denjenigen der anderen Schengen-Staaten sinngemäss und Art. 355c StGB Anwendung.

e. Schengen-Informationsaustausch

§§ 54 a–54 c werden zu §§ 54 f–54 h.*

**Koordinationsbedarf mit Vorlage 5923 (Gesetz über die Information und den Datenschutz [IDG], Totalrevision)*

II. Das Polizeiorganisationsgesetz vom 29. November 2004 wird wie folgt geändert:

Kantons-
übergreifende
Zusammen-
arbeit

§ 29. ¹ Die Kantonspolizei und das Forensische Institut Zürich arbeiten mit Polizeistellen und Behörden anderer Kantone, des Bundes und des Auslands zusammen.

Abs. 2 unverändert.

³ Die Kantonspolizei und das Forensische Institut Zürich können zugunsten von Polizeistellen und Behörden des Bundes, anderer Kantone, der Gemeinden und des Auslands Dienstleistungen erbringen, die mit ihrer eigenen Tätigkeit in einem sachlichen Zusammenhang stehen.

III. Diese Gesetzesänderungen unterstehen dem fakultativen Referendum.

Bericht

1. Ausgangslage

Die Datenbearbeitung und insbesondere der Datenaustausch unter den Polizeikörps und mit Partnerorganisationen gewinnen in der Polizeiarbeit immer mehr an Bedeutung. Auf europäischer, nationaler und kantonaler Ebene sind daher verschiedene Bestrebungen und Projekte zur Weiterentwicklung der Kooperation und Interoperabilität zwischen Sicherheitsbehörden im Gang. Die Teilnahme des Kantons Zürich an diesen Vorhaben ist Voraussetzung für eine wirksame Kriminalitätsbekämpfung im Kanton selbst, aber auch über die Kantons- und Landesgrenzen hinweg. Die Zürcher Polizeikörps sind auf einen unkomplizierten Datenaustausch angewiesen, um verschiedene Deliktsarten, insbesondere im Bereich der seriellen Kriminalität (z. B. bei Einbruchserien, Bestellbetrug und Online-Anlagebetrug), effektiv und effizient zu bekämpfen. Von besonderer Bedeutung ist der Datenaustausch bei der Deliktprävention, namentlich bei der Abwehr von Straftaten mit extremistischem Hintergrund und bei der Verhinderung von Terroranschlägen. Die heutigen Hindernisse beim Datenaustausch stehen einer wirksamen Kriminalitätsbekämpfung immer häufiger im Wege.

Um den notwendigen Datenaustausch zu ermöglichen, braucht es im Kanton Zürich entsprechende Rechtsgrundlagen, weshalb das Polizeigesetz vom 23. April 2007 (PolG, LS 550.1) revidiert werden soll. Die erforderlich gewordene Teilrevision wurde zugleich zum Anlass genommen, das PolG auf weiteren Anpassungsbedarf zu überprüfen, zum Beispiel im Bereich des Strassenverkehrs oder der Informationsbeschaffung im virtuellen Raum. Die Gesetzgebungsarbeiten erfolgten unter der Leitung der Sicherheitsdirektion. Die Datenschutzbeauftragte wurde schon früh in die Erarbeitung des Entwurfs miteinbezogen.

Mit RRB Nr. 507/2023 wurden die zu revidierenden Themenbereiche zusammengefasst und die Sicherheitsdirektion ermächtigt, das Vernehmlassungsverfahren zur Teilrevision des Polizeigesetzes durchzuführen. In der Folge wurde das Vernehmlassungsverfahren am 4. Mai 2023 eröffnet.

2. Ergebnis der Vernehmlassung

Der Vorentwurf zur Teilrevision des PolG wurde den im Kantonsrat vertretenen politischen Parteien, dem Verband der Gemeindepräsidenten des Kantons Zürich, den politischen Gemeinden, dem Obergericht, dem Verwaltungsgericht, der Statthalter-Konferenz, den Ombudsstellen,

dem Forensischen Institut Zürich, den Demokratischen Juristinnen und Juristen Zürich (DJZ), dem Zürcher Anwaltsverband (ZAV), dem Touring Club Schweiz (TCS), dem Automobil Club der Schweiz (ACS) sowie den Direktionen des Regierungsrates und der Staatskanzlei zur Vernehmlassung zugestellt. Auch die Datenschutzbeauftragte des Kantons Zürich wurde zur Vernehmlassung eingeladen.

Die Mitte, die EVP und die SVP waren mit der vorgeschlagenen Teilrevision einverstanden. Auch die FDP unterstützte das Vorhaben, hatte jedoch Vorbehalte in Bezug auf Dienstleistungen der Polizei zugunsten anderer Behörden und wünschte, dass die Observation mit GPS-Geräten und die Informationsbeschaffung im virtuellen Raum nur zur Abwehr schwerer Rechtsgutverletzungen möglich ist. AL und SP begrüßten zwar eine effizientere Zusammenarbeit der Polizeibehörden, erachteten jedoch insbesondere den automatisierten Informationsaustausch und das Abrufverfahren als problematisch und forderten detaillierte Regelungen für die Datenbearbeitung auf Gesetzesstufe. Die Grünen und die DJZ lehnten die beabsichtigte Teilrevision grundsätzlich ab und hielten die Änderungen insgesamt für zu wenig bestimmt und nicht verhältnismässig. Gleichermassen äusserte sich auch die Piratenpartei.

Die Gemeinden begrüßten die vorgeschlagenen Änderungen.

Die Statthalter-Konferenz unterstützte die geplanten Änderungen, machte jedoch u. a. einen Vorbehalt betreffend den Einsatz vertraulicher Quellen. Die Ombudsstelle des Kantons Zürich stimmte den geplanten Änderungen zu.

Das Forensische Institut Zürich begrüßte die geplanten Änderungen.

Die Datenschutzbeauftragte des Kantons Zürich reichte eine Stellungnahme mit verschiedenen Kritikpunkten ein. Die Datenschutzbeauftragte wurde laufend in die Überarbeitung der Vorlage miteinbezogen, wobei ihre Einwendungen weitgehend berücksichtigt wurden.

Weiter reichte die Flughafen Zürich AG (FZAG) eine Stellungnahme zur beabsichtigten Teilrevision ein und wünschte, dass ausserbehördliche Institutionen, die punktuell behördliche Aufgaben wahrnehmen und in dieser Funktion Daten mit der Polizei austauschen, beim elektronischen Datenaustausch miteinbezogen werden.

CSP, EDU, GLP, das Obergericht, das Verwaltungsgericht, die Ombudsstellen der Städte Zürich und Winterthur, der ZAV sowie TCS und ACS reichten keine Stellungnahme ein oder verzichteten auf eine solche.

Nach Auswertung der Vernehmlassungsantworten wurden insbesondere die nachstehenden Anpassungen vorgenommen:

- Der Einsatz technischer Überwachungsgeräte zur Feststellung des Standortes von Personen oder Sachen mit Speicherung der Aufnahmen zu Beweis Zwecken im Rahmen von polizeilichen Observationen wurde eingeschränkt auf Fälle, in denen ernsthafte Anzeichen für eine Straftat im Sinne von Art. 269 Abs. 2 der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (StPO, SR 312.0) bestehen.
- Der Einsatz automatisierter Fahrzeugfahndungssysteme im Strassenverkehr wurde überprüft.
- In Bezug auf die Informationsbeschaffung im virtuellen Raum wurde klargestellt, dass der Einsatz besonderer Informatikprogramme (GovWare) im Sinne von Art. 269^{ter} StPO ausgeschlossen ist.
- Der Einsatz vertraulicher Quellen wurde ausdrücklich beschränkt auf Fälle, die der Erkennung, Verhinderung und Aufklärung von Verbrechen und Vergehen oder der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung dienen.

3. Überarbeitung nach Bundesgerichtsentscheid

Am 28. August 2024 unterbreitete der Regierungsrat dem Kantonsrat den Antrag für eine Änderung des Polizeigesetzes betreffend Datenbearbeitung (RRB Nr. 893/2024, Vorlage 5977, vgl. ABl 2024-09-13).

Mit Urteil vom 17. Oktober 2024 entschied das Bundesgericht über die Zulässigkeit von Änderungen des Gesetzes über die Luzerner Polizei vom 27. Januar 1998, die der Luzerner Kantonsrat am 24. Oktober 2022 beschlossen hatte (BGE 1C_63/2023), insbesondere in den Bereichen automatische Fahrzeugfahndung und Verkehrsüberwachung, Betrieb von Analysesystemen im Bereich der seriellen Kriminalität und polizeilicher Informationssystem-Verbund des Bundes und der Kantone. Dabei äusserte es sich u. a. zur Abgrenzung der Rechtsetzungskompetenz zwischen dem Bund und den Kantonen und legte gegenüber früheren Entscheiden genauer fest, welche Regelung es in den genannten Bereichen auf Gesetzesstufe braucht.

Aufgrund dieser höchstgerichtlichen Rechtsprechung überprüfte die Sicherheitsdirektion den Antrag des Regierungsrates und kam zum Schluss, dass dieser in verschiedener Hinsicht anzupassen ist. In der Folge wurde die Vorlage 5977 überarbeitet. Der Regierungsrat und die zuständige Kommission des Kantonsrates hatten sich mit diesem Vorgehen einverstanden erklärt.

Die Auswertung von BGE 1C_63/2023 ergab, dass die Vorlage 5977 in den Bereichen Überwachung des Strassenverkehrs mit Videogeräten (§§ 32d ff.), Informationsbeschaffung im virtuellen Raum (§§ 32k f.), Datenbearbeitung mit Analysesystemen (neu §§ 52a f.) und elektronische Zusammenarbeit (§§ 54a ff.) und folglich auch § 2 Abs. 2 betreffend Geltungsbereich der polizeilichen Tätigkeit im Rahmen der Strafverfolgung anzupassen ist.

Die automatisierte Fahrzeugfahndung, wie es das revidierte Luzerner Polizeigesetz vorsah, diene gemäss den Erläuterungen in erster Linie der Strafverfolgung. Das Bundesgericht hob die Bestimmung auf, da den Kantonen in diesem Bereich keine Gesetzgebungskompetenz zukomme und die Regelung mit Blick auf den verbleibenden Anwendungsbereich eine unverhältnismässig weitreichende Datenerfassung, -auswertung und -aufbewahrung zulasse (vgl. BGE 1C_63/2023 E. 3 ff.).

Die Vorlage 5977 zur Änderung des Zürcher Polizeigesetzes verbot zwar im Gegensatz zum revidierten Polizeigesetz des Kantons Luzern die Speicherung von Bildern, sofern kein Treffer erfolgt, sah aber gleichermassen die Erfassung der Kontrollschilder und Speicherung für 100 Tage und u. a. den Einsatz für die Strafverfolgung vor. Der zürcherische Entwurf hält somit mindestens teilweise der bundesgerichtlichen Rechtsprechung nicht stand, weshalb im heutigen Zeitpunkt auf eine kantonale Regelung zur automatisierten Fahrzeugfahndung zu verzichten ist. Die Überwachung des Strassenverkehrs wird auf rein polizeiliche Zwecke, insbesondere zur Gefahrenabwehr, eingeschränkt.

Bei der Informationsbeschaffung im virtuellen Raum werden die Voraussetzungen zur Beschaffung von nicht öffentlich zugänglichen Informationen präzisiert. Dem Entscheid des Bundesgerichts lässt sich entnehmen, dass die Anforderungen an die Bestimmtheit einer Norm bei schweren Eingriffen in die informationelle Selbstbestimmung hoch sind. Auch hier wird die Bestimmung auf rein polizeiliche Zwecke eingeschränkt. Die Verwendung von Analysesystemen wird in einem separaten Paragraphen geregelt, weil das Bundesgericht differenzierte Bestimmungen in diesem Bereich verlangt.

In Bezug auf die elektronische Zusammenarbeit mit ausserkantonalen Behörden und dem Bund wird das Abrufverfahren separat und detailliert geregelt, da das Bundesgericht in diesem Bereich sehr hohe Anforderungen an den Regulierungsgrad stellt. Dies tut es auch in Bezug auf die Regelung des Betriebs gemeinsamer Informationssysteme. Die elektronische Zusammenarbeit wird daher spezifisch auf die projektierte polizeiliche Abfrageplattform «POLAP» ausgerichtet. So werden detaillierte Regelungen zu den Zwecken des Datenaustauschs und den Datenkategorien eingefügt. Die Daten, die im Abrufverfahren bekannt gegeben werden sollen, werden stark eingeschränkt.

Insgesamt werden gegenüber der Vorlage 5977 Einschränkungen vorgenommen und detaillierte Regelungen eingefügt, um so der bundesgerichtlichen Rechtsprechung Genüge zu tun.

4. Erläuterungen zu den einzelnen Bestimmungen

I. Änderungen des PolG

§ 2 Abs. 2 Geltungsbereich

Das Polizeirecht regelt das präventive Handeln der Polizei, solange noch kein Anfangsverdacht vorliegt. Auch die Vorermittlung, d. h. die ersten Abklärungen aufgrund von Anzeichen oder Hinweisen für das Erkennen einer strafbaren Handlung, sind im Polizeirecht zu regeln. Demgegenüber legt die StPO als Bundesrecht die Strafverfolgung abschliessend fest, also das Handeln der Behörden zur Aufklärung von Delikten, wenn ein Anfangsverdacht vorliegt. Der Übergang ist fließend. Nach der Literatur muss der bisherige § 2 Abs. 2 PolG (mit Ausnahme des bisherigen § 32g) so ausgelegt werden, dass er sich lediglich auf die Vorermittlung, die Organisation der Polizei oder die Staatshaftung des Kantons bezieht.

In BGE 1C_63/2023 E. 3.5.2 erklärt nun das Bundesgericht, entscheidend für die Abgrenzung der Rechtsetzungskompetenz sei die Zielsetzung einer Regelung im Polizeirecht bzw. der Schwerpunkt des verfolgten Zweckes. Bei den im Folgenden auszuführenden Gesetzesänderungen liegt dieser klar auf der präventiven Gefahren- bzw. Deliktsbekämpfung und Erkennung, nicht auf der Aufklärung. Aus dem genannten Bundesgerichtsentscheid ist zu folgern, dass Bestimmungen, die Vorermittlungshandlungen regeln, die unter Umständen auch in einer späteren Strafuntersuchung münden, nicht ausdrücklich in § 2 Abs. 2 PolG aufzuzählen sind. Die Verweisung auf den bisherigen § 32g (neu: § 32i) PolG ist jedoch in § 2 Abs. 2 PolG zu belassen, da sich die kantonale Kompetenz zur Regelung der verdeckten Registrierung direkt aus Art. 33 Abs. 2 der Verordnung vom 8. März 2013 über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro (N-SIS-Verordnung, SR 362.0) ergibt.

§ 32 Abs. 3 Polizeiliche Observation

Unter technische Überwachungsgeräte im Sinne von § 32 Abs. 2 fallen nicht nur Ton- und Bildaufnahmegeräte, sondern auch Ortungsgeräte wie GPS- und Peilsender. Da das Bundesgericht in seiner jüngsten Recht-

sprechung (BGE 1C_181/2019 E. 17.5.2) für den Einsatz von GPS-Ortungsgeräten im Rahmen polizeilicher Observationen mindestens dieselben verfahrensrechtlichen Garantien verlangt wie bei der GPS-Überwachung gemäss StPO, braucht es eine entsprechende gesetzliche Grundlage, die mit Abs. 3 geschaffen wird.

Der sich zurzeit in Revision befindende Art. 282 Abs. 3 E-StPO, der das bewilligungsfreie taktische Setzen von Ortungsgeräten ohne Speicherung und ohne Beweiszweck an Fahrzeugen ermöglicht, ist vom bestehenden Abs. 2 erfasst.

Mit der Verweisung in § 32 Abs. 3 auf Art. 269 Abs. 2 StPO ist klar gestellt, dass solche Geräte nur eingesetzt werden dürfen, wenn dies zur Entdeckung oder Verhinderung einer Katalogtat (z. B. Menschenhandel, Freiheitsberaubung und Entführung, Beteiligung an kriminellen und terroristischen Organisationen) erforderlich ist, deren Schwere eine solche Überwachung rechtfertigt. Mit der Verweisung auf Art. 269–279 und 281 StPO wird verdeutlicht, dass sich der Einsatz sinngemäss nach den Art. 269 ff. StPO richtet. Damit ist auch klargestellt, dass die zeitlichen Bedingungen bezüglich Genehmigung durch das Zwangsmassnahmengericht genauso streng sind wie im Verfahren nach der StPO und diese bis spätestens 24 Stunden nach dem Einsatz eingeholt werden muss (Art. 281 Abs. 4 in Verbindung mit Art. 274 Abs. 1 StPO). Es werden ernsthafte Anzeichen für eine der Katalogtaten vorausgesetzt, um solche Überwachungsgeräte einzusetzen. Es bedarf aber keines konkreten, geschweige denn eines dringenden Verdachts im Sinne der StPO, dass eine Straftat begangen worden ist, sondern es genügen «ernsthafte Anzeichen» dafür, dass eine Katalogtat vor der Ausführung steht oder bereits ausgeführt wird (vgl. BGE 1C_181/2019 E. 17.5.2). Eine anlassfreie Überwachung zum Zweck der Verhinderung solcher Taten ist in jedem Fall nicht möglich.

Betreffend die Mitteilung einer Observation mittels technischer Überwachungsgeräte zur Feststellung des Standortes gemäss Abs. 3 soll Art. 279 StPO sinngemäss zur Anwendung kommen (§ 32 Abs. 6). Im polizeirechtlichen Bereich erfolgt die Mitteilung damit nach Abschluss der Vorermittlungen, sobald es unter Berücksichtigung des Ermittlungszwecks (d. h. insbesondere, ohne Verdächtige zu warnen) möglich ist. Konkretisiert sich aufgrund der Vorermittlungen ein Deliktsverdacht, kommt die StPO direkt und nicht mehr analog zur Anwendung.

Die Aufbewahrungsdauer der Überwachungsdaten richtet sich nach § 53 Abs. 2 PolG. Sie müssen daher spätestens nach 100 Tagen gelöscht werden, soweit sie nicht weiterhin für ein Straf-, Zivil- oder Verwaltungsverfahren benötigt werden.

§ 32d Überwachung des Strassenverkehrs mit Videogeräten

Das Bundesamt für Strassen (ASTRA) ist gemäss Art. 83 der Bundesverfassung vom 18. April 1999 (BV, SR 101) und Art. 57c des Strassenverkehrsgesetzes vom 19. Dezember 1958 (SR 741.01) für den Bau, den Betrieb und den Unterhalt des Nationalstrassennetzes verantwortlich, hat ein Verkehrsmanagement zu betreiben und kann zu diesem Zweck die Nationalstrasseninfrastruktur bildlich erfassen. Es kann die Aufgabe u. a. den Kantonen übertragen. Für die Nationalstrassen auf dem Gebiet des Kantons Zürich sowie Teilen der Kantone Schwyz, Thurgau, St. Gallen und Zug hat es den Kanton Zürich mit dieser Aufgabe betraut (Leistungsvereinbarung vom 4. Juni 2014 über das Verkehrsmanagement auf Nationalstrassen). Die Kantonspolizei nimmt diese als regionale Verkehrsleitzentrale des Bundes wahr.

§ 32d Abs. 1 schafft die Rechtsgrundlage, um auch auf kantonalen Autobahnen und Autostrassen ein Verkehrsmanagement zu betreiben, zu diesem Zweck den Verkehr bildlich zu erfassen und die Verwendung der daraus gewonnenen Bilder zu erlauben. Die verkehrspolizeiliche Aufgabe der Verkehrslenkung stützt sich dabei auf §§ 10 und 15 des Polizeiorganisationsgesetzes vom 29. November 2004 (POG, LS 551.1). Für die in Abs. 1 aufgeführten polizeilichen Zwecke genügen grundsätzlich Bilder, mit denen die Identifikation von Personen, Fahrzeugen und Kontrollschildern nicht möglich ist.

In bestimmten Bereichen braucht die Polizei jedoch hochauflösende Bilder zur Gefahrenabwehr, z. B. wenn sie nach einer Meldung, dass sich Ölsuren oder herabgefallene Ladungsteile auf der Fahrbahn befinden, Sofortmassnahmen zum Schutz der Verkehrsteilnehmenden ergreifen muss. Ebenso braucht sie solche Bilder bei Ereignissen wie Verkehrsunfällen oder Sturmschäden, die Gefahren für die übrigen Verkehrsteilnehmenden schaffen. Schliesslich erfordert auch der Wechsel der Verkehrsführung, wie die Freigabe des Pannestreifens als zusätzliche Fahrspur, dass dieser präventiv mittels Überwachungskameras auf herumliegende Fahrzeug- oder Ladungsteile abgesucht wird. Die üblicherweise zur Verkehrsüberwachung übermittelten Bilder zeigen keine scharfen Konturen, weshalb für die Einsatzleitung in der Verkehrsleitzentrale Flüssigkeiten oder kleinere Gegenstände auf der Fahrbahn nicht erkannt oder nicht identifiziert werden können oder bei einem Einsatz nicht erkennbar ist, welche Funktionärinnen und Funktionäre welcher Blaulichtorganisation was erledigen. Abs. 2 zählt abschliessend auf, in welchen Fällen die vertiefte Einsicht in die Aufnahmen ausnahmsweise notwendig und daher zulässig sein soll.

Hochauflösende Bilder können auch für die Strafverfolgung wichtig sein, z. B. zur Rekonstruktion eines Unfallherganges, zur Identifikation eines flüchtenden Unfallbeteiligten oder auch zur Bestimmung der Fluchtrichtung der Täterschaft nach einem Verbrechen in der Nähe wie z. B.

einem Raubüberfall. Das Bundesgericht interpretiert aber die Kompetenzen der Kantone zum Erlass von Regelungen im Bereich der Strafverfolgung sehr einschränkend. Der Bund habe von seiner Gesetzgebungskompetenz auf dem Gebiet des Strafprozessrechts mit dem Erlass der StPO grundsätzlich erschöpfend Gebrauch gemacht und den Kantonen verbleibe damit die Rechtsetzungskompetenz im Bereich der umfassenden Gefahrenabwehr, insbesondere zur Verhinderung von Straftaten (vgl. BGE 1C_63/2023 E. 3.5.1). Folglich soll das PolG lediglich die Erhebung und Auswertung von Videoaufzeichnungen des Strassenverkehrs zu polizeilichen Zwecken regeln. Das Strafprozessrecht erlaubt jedoch grundsätzlich die Verwendung der Bilder aus Verkehrsüberwachungssystemen zur Strafverfolgung (vgl. BGE 6B_346/2024 E. 2.3.2 und 2.4).

Das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation ist bereit, den Polizeikorps zu diesen Zwecken den Zugriff auf die Aufzeichnungen des Video- und Bildspeichersystems des ASTRA gestützt auf kantonales Recht zu gewähren, da eine Regelung im Bundesrecht nicht vorgesehen ist. Abs. 3 schafft die nötige gesetzliche Grundlage, wie es die Weisungen «Videoüberwachungen» des ASTRA, Ziff.4.2, ausdrücklich vorsehen. Das kantonale Tiefbauamt ist Betreiber der Überwachungssysteme auf Kantonsstrassen, weshalb auch der Beizug von Daten aus diesen Systemen geregelt wird.

Abs. 4 trägt dem datenschutzrechtlichen Anliegen der Sicherstellung des korrekten Umgangs mit den Daten der Verkehrsmanagement- und -überwachungssysteme Rechnung. Analog zu § 15 Abs. 3 der Verordnung über das Polizei-Informationssystem POLIS vom 13. Juli 2005 (POLIS-Verordnung, LS 551.103) ist eine Regelung auf der Stufe einer internen Weisung vorzusehen. Die Polizei führt ein Verzeichnis über die stationären Videoüberwachungsanlagen, in das gestützt auf § 20 Abs. 1 des Gesetzes über die Information und den Datenschutz (IDG, LS 170.4) Einsicht verlangt werden kann.

Die Löschung der Aufzeichnungen richtet sich nach § 53 Abs. 2 PolG.

§§ 32g und h Informationsbeschaffung im virtuellen Raum

Im früheren § 32f PolG war die Informationsbeschaffung im Internet geregelt. Diese Bestimmung hob das Bundesgericht auf (BGE 1C_653/2012), weshalb eine neue Formulierung unter Berücksichtigung der Vorgaben des Bundesgerichts (Vorbehalt einer richterlichen Genehmigung beim Einsatz von technischen Mitteln in Bereichen mit einem beschränkten Benutzerkreis und nachträgliche Information Betroffener) nötig wurde. Zudem soll aufgrund der Rückmeldungen aus der Vernehmlassung der Zweck der Informationsbeschaffung bei nicht öffentlich zugänglichen Informationen klar eingegrenzt und vom in der StPO ver-

wendeten Begriff der «besonderen Informatikprogramme» Abstand genommen werden.

Aus dem neueren Entscheid des Bundesgerichts lässt sich zudem herleiten, dass die Anforderungen an die Bestimmtheit einer Norm bei schweren Eingriffen in die informationelle Selbstbestimmung hoch sind (vgl. BGE 1C_63/2023 E. 3.3.1 f.). Da das Beschaffen von Personendaten im Internet dieses Grundrecht berührt, wurde die Informationsbeschaffung im Internet entsprechend detailliert geregelt. Die Strafverfolgung wurde aufgrund der bundesgerichtlichen Rechtsprechung nicht aufgenommen (vgl. BGE 1C_63/2023 E. 3.5.1).

In Bezug auf die Informationsbeschaffung im virtuellen Raum wird nun technologieunabhängig unterschieden, ob die Informationen öffentlich zugänglich sind oder nicht. Der Begriff der «öffentlich zugänglichen Informationen» beschreibt den rechtlichen und sozialen Kontext der Zugänglichkeit und berücksichtigt die informationelle Selbstbestimmung aus Sicht der betroffenen Person und im Sinne des Bundesgerichts. Informationen sind öffentlich zugänglich, wenn sie für eine grosse Menge von Personen abrufbar sind. Nicht öffentlich sind sie, wenn sie nur einem begrenzten Kreis von Nutzerinnen und Nutzern vorbehalten sind. Letzteres ist z. B. bei einer sozialen Plattform der Fall, wenn es einer Freundschaftsanfrage bedarf.

§ 32g a. Öffentlich zugängliche Informationen

Abs.1 regelt allgemein Abfragen in öffentlichen Netzwerken. Diese Art der Informationsbeschaffung ist heute aus dem polizeilichen Alltag nicht mehr wegzudenken. Sie ist nicht nur für verschiedene verwaltungspolizeiliche Tätigkeiten (wie für die Prüfungen von Veranstaltungsbewilligungen), sondern auch für die Verhinderung verschiedener Deliktsformen unentbehrlich. So spielt sie insbesondere bei der frühzeitigen Erkennung von Radikalisierungen und Gewaltandrohungen, aber auch bei anderen Deliktsformen wie beispielsweise bei Online-Anlagebetrügen eine wichtige Rolle. Das Verbot der Fernmeldeüberwachung muss an dieser Stelle nicht aufgenommen werden, da dem Fernmeldegeheimnis unterliegende Informationen gar nicht öffentlich zugänglich sind. In Abs.2 wird festgelegt, dass bei der Beschaffung und Bearbeitung von öffentlich zugänglichen Informationen Analysensysteme eingesetzt werden dürfen, dies jedoch nur unter den Voraussetzungen von § 52a.

§ 32h b. Nicht öffentlich zugängliche Informationen

Erfahrungsgemäss werden polizeilich bedeutsame Informationen im Internet aber nicht nur im allgemein zugänglichen Bereich, sondern oft in geschlossenen Foren bzw. sogenannten Closed User Groups ausge-

tauscht. Mit § 32h wird die Grundlage für einen Einsatz von Software in nicht öffentlich zugänglichen Bereichen geschaffen. Diese Bestimmung soll der Polizei die Möglichkeit einräumen, zur Erkennung und Verhinderung von Gefahren für das Leben einer Person sowie Straftaten gemäss Art. 269 Abs. 2 StPO die Verwendung von Software mit Genehmigung des Zwangsmassnahmengerichts anzuordnen und allfällige Zugriffsbeschränkungen (z. B. Passwortschutz) umgehen zu können. Dabei geht es vor allem darum, im Rahmen der polizeilichen Präventionstätigkeit gegen die Gefahr sexueller Handlungen mit Kindern und der Kinderpornografie vorzugehen sowie frühzeitig Informationen über die Vorbereitung von folgenschweren Ausschreitungen und Gewalttaten wie z. B. Amokläufen, gewalttätiges Verhalten anlässlich von Grossveranstaltungen, Angriffe auf Infrastrukturen wie die Trinkwasser- oder die Stromversorgung sowie allgemein Informationen über bevorstehende schwere Rechtsgutverletzungen zu gewinnen, um rechtzeitig die erforderlichen Gegenmassnahmen einleiten zu können.

Die Anwendung wird einerseits auf die Erkennung und Verhinderung von Gefahren für das Leben einer Person beschränkt. Gemeint sind Situationen, in denen ein Mensch ohne strafbare Dritteinwirkung einer Lebensgefahr ausgesetzt ist, z. B. wenn ein Kind oder eine demente Person vermisst wird. Andererseits wird auf den Anforderungskatalog in Art. 269 Abs. 2 StPO verwiesen und dadurch die Nutzung von unbestimmten Rechtsbegriffen vermieden. Zudem darf der Einsatz gemäss Abs. 2 nur angeordnet werden, wenn ernsthafte Anzeichen für solche Gefahren oder Straftaten bestehen. Ein anlassfreies Durchsuchen solcher geschlossenen Foren ist damit ausgeschlossen. Ferner muss die Massnahme in Bezug auf die Schwere der jeweiligen Gefahr verhältnismässig sein und es darf keine mildere Massnahme möglich sein. Gestützt auf diese Kriterien entscheidet das Zwangsmassnahmengericht, ob und wie ein allfälliger Zugriffsschutz (z. B. ein Passwort oder eine andere technische Barriere) mit spezialisierter Software im Sinne von Art. 280 StPO umgangen werden darf. Für die Verwendung von Analysesystemen gelten die Einschränkungen gemäss § 52a. Wie in Abs. 4 dargelegt, ist der Einsatz von Fernmeldeüberwachung in jedem Fall verboten. Mit Abs. 5 und 6 wird geregelt, dass die betroffene Person nach Beendigung der Massnahme grundsätzlich informiert wird und gegen die vom Zwangsmassnahmengericht bewilligte Massnahme Beschwerde erheben kann. Um den Rechtsschutz zu gewähren, muss sichergestellt sein, dass die erhobenen Daten auch bei Nichtverwendung erst gelöscht werden, nachdem die betroffene Person davon Kenntnis erhalten hat und dass die Rechtsmittelinstanz die Daten bei Bedarf bei der Polizei einfordern kann. Mit der vorgesehenen Löschfrist von zwei Monaten verbleibt für Letzteres genügend Zeit.

§ 32i Verdeckte Registrierung, gezielte Kontrolle, Ermittlungsanfrage

Die Europäische Union (EU) baut das Fahndungssystem SIS aus. Die bestehenden Massnahmen der verdeckten Registrierung («heimliche» Erfassung von Informationen wie Reiseweg, Reiseziel, Begleitpersonen usw. anlässlich von polizeilichen Überprüfungen und deren Übermittlung an den ausschreibenden Schengen-Staat) und der gezielten Kontrolle (Durchsuchung der befragten Person und mitgeführten Sachen) werden erweitert. Das neue Instrument der sogenannten Ermittlungsanfrage (vgl. Art. 33 Abs. 1 N-SIS-Verordnung) erlaubt die Befragung der gesuchten Person gemäss einem spezifischen Fragenkatalog, den die Behörde des ausschreibenden Staates im SIS hinterlegt hat. Sie soll vor allem der Bekämpfung von Terrorismus und anderen schweren Straftaten dienen. Aufgrund der Polizeihochheit der Kantone bedarf die Umsetzung dieser Fahndungsmassnahme im polizeirechtlichen Anwendungsbereich einer kantonalrechtlichen Grundlage, die mit § 32i geschaffen wird.

§ 32j Quellenführung

In Deliktsfeldern, in denen es üblicherweise keine Anzeigerstattungen gibt, werden Ermittlungen der Polizei oft durch Informationen von vertraulichen Quellen ausgelöst. Die eingesetzten Personen verfügen über besondere Kontakte zu kriminellen Milieus (z. B. in den Bereichen Terrorismus, internationale Geldwäscherei, Menschen- oder Betäubungsmittelhandel) und können den Strafverfolgungsbehörden Insiderinformationen weitergeben. Im Kanton Zürich besteht bereits heute mit § 4 PolG eine Rechtsgrundlage zum Umgang mit vertraulichen Informantinnen und Informanten. Im Gegensatz zu mehreren anderen Kantonen (u. a. Bern, Zug, Graubünden und Schwyz) enthält das PolG aber bisher keine ausdrückliche Regelung für die Quellenführung. Angesichts der Bedeutung dieses Instituts wird die Quellenführung ausdrücklich in das Gesetz aufgenommen.

Vertraulichkeit muss zugesichert werden können, um die Quellen vor Repressalien und/oder Racheakten zu schützen. Die Zusicherung der Vertraulichkeit ist die Grundvoraussetzung für die Zusammenarbeit mit vertraulichen Quellen. Ohne eine solche Zusicherung ist kaum jemand bereit, der Polizei Informationen aus dem kriminellen Milieu zu liefern, wenn die Informationsgeberin oder der Informationsgeber von Anfang an davon ausgehen muss, dass das kriminelle Milieu ihren bzw. seinen Namen erfahren wird. Die Dokumentation erfolgt daher für rein polizeiinterne Zwecke. Das Recht einer Person auf Informationszugang gemäss §§ 20 ff. IDG kann hier infolge der Interessenabwägung im Sinne von § 23 IDG zum Schutz der vertraulichen Quellen grundsätzlich nicht gewährt werden.

Hat die Polizei nicht die Möglichkeit, im Vorfeld eines Ermittlungsverfahrens Informationen (nicht Beweismittel) von vertraulichen Quellen anzunehmen, verliert es wesentlich an Wirksamkeit und Glaubwürdigkeit. Die Vertraulichkeitszusage und die daraus resultierende Offenheit der informationsgebenden Person gegenüber der Polizei ermöglicht es erst, die informationsgebende Person einer angemessenen Prüfung durch die Polizei zu unterziehen, was danach dazu führt, dass die Glaubwürdigkeit der Person und somit auch die Glaubhaftigkeit ihrer Aussagen eingeschätzt werden kann.

Vertrauliche Quellen werden grundsätzlich nicht aktiv rekrutiert. Als Quellen infrage kommende Personen werden in angemessener Weise überprüft, insbesondere wird abgeklärt, ob sie polizeilich gesucht werden oder in einem Zusammenhang mit einem Ermittlungsverfahren stehen.

Die Handhabung der Entschädigung und Belohnung von Quellen erfolgt restriktiv.

§ 43 Polizeiliche Berichte zur Person und Personensicherheitsprüfungen

Die Polizei hat Zugang zu einer Vielzahl sensibler Informationen. Wo notwendig, lassen sich diese bei einer Person zu einem Gesamtbild zusammenfassen, um Aussagen über ihre Vertrauenswürdigkeit tätigen zu können. Die Kantonspolizei Zürich bekommt schon heute verschiedene Anfragen. Aufgrund des sensiblen Bereichs und damit dem Persönlichkeitsschutz genügend Rechnung getragen werden kann, ist der Umgang mit diesen Anfragen genauer zu regeln. Einerseits ist eine genügende rechtliche Grundlage zu schaffen. Andererseits ist auch das öffentliche Interesse an solchen möglichen Eingriffen zu konkretisieren.

§ 43 Abs. 1 lit. a verweist auf spezialgesetzliche Rechtsgrundlagen. Solche sind teilweise vorhanden (z. B. Art. 14 Bundesgesetz vom 3. Februar 1995 über die Armee und die Militärverwaltung [SR 510.10]), fehlen aber auch in gewissen Bereichen, in denen ein starkes Bedürfnis nach einer fundierten und unter Umständen regelmässigen Überprüfung auf Sicherheitsrisiken besteht. Insbesondere in der kantonalen Gesetzgebung sind kaum gesetzliche Grundlagen vorhanden, die eine Überprüfung erlauben. Als Beispiele lassen sich Mitarbeitende externer Dienstleister (z. B. im IT-Bereich sowie im Bereich von Sicherheitsdienstleistungen, namentlich im Strafvollzug), Personal mit Aufgaben im Zusammenhang mit dem Betrieb kantonalen Infrastruktur (Polizei- und Justizzentrum) oder Angestellte der kantonalen und kommunalen Verwaltungen (z. B. Mitarbeitende der Polizeikorps im Kanton Zürich) anführen. Die Bestimmungen von § 43 Abs. 1 lit. b–d sollen diese Lücke schliessen. Mit lit. b wird die Grundlage zur Unterstützung von Stellen, die gesetzliche

Aufgaben erfüllen, geschaffen. In Betracht kommen beispielsweise Konzessionsnehmerinnen wie die FZAG. Diese hat für den Betrieb des Landesflughafens erhöhte Sicherheitsanforderungen an Personen mit Zutritt zum Sicherheitsbereich des Flughafens (vgl. Art. 108b Bundesgesetz vom 21. Dezember 1948 über die Luftfahrt [LFG, SR 748.0]). Mit lit. c und d soll eine solide Grundlage zur Überprüfung von Mitarbeitenden anderer Verwaltungsstellen und externer Dienstleistenden geschaffen werden.

Vorausgesetzt wird gemäss § 43 Abs. 2 ein entsprechendes Gesuch der zuständigen Stelle, das sich zum Zweck des Gesuchs äussert, damit ersichtlich ist, ob die gesetzlichen Voraussetzungen für die Überprüfung erfüllt sind. Des Weiteren hat die ersuchende Stelle sicherzustellen, dass die betroffene Person vor einer Entscheidung zu ihren Ungunsten zum Resultat der Überprüfung Stellung nehmen kann. Die Überprüfung gemäss dem neuen Abs. 1 lit. c und d muss zur Gewährleistung der Sicherheit erforderlich sein. Somit dürfen Sicherheitsüberprüfungen nicht flächendeckend durchgeführt werden, sondern nur dort, wo es aufgrund besonderer Umstände verhältnismässig erscheint.

In Bewerbungsverfahren ist zusätzlich § 11a Abs. 2 der Vollzugsverordnung zum Personalgesetz vom 19. Mai 1999 (LS 177.111) zu berücksichtigen, der die Einholung von Referenzen, Leumundsberichten, Sicherheitsüberprüfungen und anderen Eignungsabklärungen nur mit Einwilligung der Bewerbenden erlaubt.

§ 43 Abs. 3 erlaubt das Einholen von Informationen bei anderen öffentlichen Organen. In dieser Hinsicht ist auf § 12 IDG hinzuweisen, der öffentliche Organe verpflichtet, Betroffene über die Beschaffung von Personendaten zu informieren. Die Polizei kann bei ihren Abklärungen Informationen aus öffentlich zugänglichen Quellen (namentlich aus dem Internet) berücksichtigen.

Benötigt die ersuchende Stelle nicht nur einen Bericht, der sich auf Wahrnehmungen und Feststellungen beschränkt, sondern eine auf polizeilicher Expertise beruhende Beurteilung, soll eine entsprechende Einschätzung vorgenommen werden können. Dies ist beispielsweise der Fall bei der Überprüfung von Personen mit Zutritt zum Sicherheitsbereich des Flughafens (vgl. Art. 108d LFG). Die Möglichkeit der betroffenen Person zur Einsicht- und Stellungnahme richtet sich nach §§ 20 ff. IDG. Da polizeiliche Berichte immer sachlich sein müssen, ist der ganze bisherige Abs. 4 aufzuheben.

Mit dem neuen Abs. 4 wird eine solide Grundlage für die Verrechnung des Aufwands geschaffen. Die Bemessung richtet sich nach § 4 der Gebührenordnung für die Verwaltungsbehörden vom 30. Juni 1966 (LS 682).

§ 44a Präventive Ausschreibung schutzbedürftiger Personen

Das bisherige EU-Recht sah vor, dass schutzbedürftige Personen erst dann im SIS II ausgeschrieben werden können, wenn sie vermisst werden. Mit Art. 32 der Verordnung (EU) 2018/1862 «SIS Polizei» wurde die Möglichkeit eingeführt, Personen, die zu ihrem eigenen Schutz oder zum Zweck der Gefahrenabwehr von einer Auslandsreise abgehalten werden müssen, präventiv im SIS auszuschreiben. Die Bestimmung kann beispielsweise relevant sein, wenn eine Kindesentführung durch einen Elternteil unmittelbar bevorsteht oder wenn eine konkrete Gefahr besteht, dass Opfer von Zwangsheirat oder Menschenhandel unfreiwillig ins Ausland gebracht werden. Es liegt nahe, die Zuständigkeit zum Erlass des erforderlichen Entscheids der Polizei zu übertragen.

Die Ziele und Bedingungen der Ausschreibung sind in Art. 32 und 33 der Verordnung (EU) 2018/1862 näher definiert. Voraussetzung für eine Ausschreibung ist überdies deren Eignung und Erforderlichkeit zur Erreichung des Zwecks (Schutz der Betroffenen bzw. Gefahrenabwehr) sowie die Zumutbarkeit, die eine Abwägung der Interessen der von der Massnahme betroffenen Person gegenüber dem öffentlichen Interesse erfordert.

Gemäss Art. 16 Abs. 1 der N-SIS-Verordnung können SIS-Ausschreibungen nur über die Bundessysteme RIPOL (automatisiertes Polizeifahndungssystem) oder ZEMIS (Zentrales Migrationsinformationssystem) erfasst werden; relevante Zusatzinformationen sind über das SIRENE-Büro zu übermitteln.

§ 52 Datenbearbeitung

In Abs. 1 und 3 werden die veralteten Bezeichnungen «Datenbearbeitungssysteme» bzw. «Datenbestände» durch «Informationssysteme» ersetzt.

§§ 52a und 52b Einsatz von Analysesystemen

Das Bundesgericht äussert sich im Entscheid zum Luzerner Polizeigesetz auch zu den gesetzlichen Anforderungen an den Betrieb von Analysesystemen und verlangt differenziertere Normen in diesem Bereich (BGE 1C_63/2023 u.a. E. 4.5.3). Es sind daher spezifische Vorschriften für deren Einsatz einzufügen.

§ 52a a. Im Allgemeinen

§ 52a regelt den Einsatz von einfachen und von intelligenten Analysesystemen. Einfache Analysesysteme sind Programme, welche die Polizei bei der systematischen Zusammentragung und Darstellung bestehender polizeilich relevanter Daten unterstützen. Hierbei handelt es sich beispiels-

weise um Programme, die den Verlauf von Geldtransaktionen visualisieren, oder auch um moderne Datenbanken wie PICAR oder PICSEL (siehe nachfolgend). Davon zu unterscheiden sind die intelligenten Analysensysteme, die erhobene Daten eigenständig mit künstlicher Intelligenz bearbeiten können. Während bei den einfachen Analysesystemen das angezeigte Resultat schrittweise nachvollziehbar ist, gilt dies bei den intelligenten Systemen nicht unbedingt. Künstliche Intelligenz ist in der Lage, gestützt auf vorhandene Daten oder Anweisungen teilweise selbstständig Antworten oder Resultate zu entwickeln. In Anlehnung an den Bundesgerichtsentscheid (BGE 1C_63/2023 u.a. E. 4.5.3) werden die gesetzlichen Anforderungen an den Einsatz solcher intelligenten Analysensysteme in Abs. 3 geregelt: Es muss damit sichergestellt werden, dass die Bearbeitung von besonderen Personendaten der Erkennung oder Verhinderung von Verbrechen, schweren Vergehen oder von einer Gefahr für das Leben einer Person dient, dass eine rechtliche Grundlage für eine solche Datenbearbeitung besteht (vgl. BGE 1C_63/2023 E. 6.6.3), dass in jedem Einzelfall die von einer Software gemeldeten Resultate durch einen Menschen überprüft werden, der über die Risiken und Gefahren von künstlicher Intelligenz instruiert ist, und dass der Softwareeinsatz protokolliert wird. Dadurch wird sichergestellt, dass die Polizei zeitgemässe Software einsetzen kann, um den neuen technischen Herausforderungen und Datenmengen begegnen zu können, und dass gleichzeitig die Schlusseinschätzung eines Sachverhaltes durch einen Menschen vorgenommen wird. Im Übrigen wird auf die laufende Revision des IDG verwiesen, die detailliert Stellung zum Einsatz von künstlicher Intelligenz nimmt (Vorlage 5923).

Die Nutzung von Bildern von Personen, z. B. von Überwachungskameras oder Mobiltelefonen, wird immer wichtiger, da die Bilder nicht nur einen bestimmten Tatablauf aufzeigen können, sondern auch weil Gesichtsbilder zur Identifikation von Personen beitragen können. Zurzeit werden Fahndungsbilder von unbekannten Täterschaften polizeintern verbreitet, die Polizistinnen und Polizisten der jeweiligen Korps sichten diese Fotos und melden sich bei Hinweisen bei den Verantwortlichen der sogenannten Bildfahndung. Dieses Vorgehen ist ressourcentechnisch höchst aufwendig. Entsprechend soll es im neuen Abs. 4 modernisiert werden, um zukünftig wie bei einem Fingerabdruckabgleich vorgehen zu können, wie folgendes Beispiel aufzeigt: Das Gesichtsbild einer unbekannten Person wird in der polizeilichen Datenbank mit gespeicherten Gesichtsbildern von bereits erkennungsdienstlich behandelten Personen abgeglichen. Liefert das System eine mögliche Übereinstimmung, so wird der angezeigte Treffer durch einen Menschen überprüft und protokolliert. Um diesen Abgleich durchführen zu können, müssen alle obgenannten Voraussetzungen für die Nutzung von intelligenten Analysensysteme eingehalten werden. Einschränkend ist im Ge-

setzestext formuliert, dass der Abgleich nur im begründeten Einzelfall erfolgen darf. Ein massenhaftes, anlassloses Abgleichen ist nicht erlaubt. Ebenso unzulässig ist die Echtzeit-Gesichtserkennung. Auch ist eine Anwendung bei Bagatelldelikten ausgeschlossen, da gemäss Abs. 3 ernsthafte Anzeichen auf Verbrechen oder schwere Vergehen bzw. auf eine Gefahr für das Leben einer Person vorliegen müssen. Schwere Vergehen sind Tatbestände, die mit Freiheitsstrafe sanktioniert werden können (BGE 1B_489/2018 E. 4.3). Der Bund sieht ebenfalls vor, diese inzwischen erprobte Technologie 2027 einzuführen (<https://www.fedpol.admin.ch/fedpol/de/home/sicherheit/personenidentifikation-neu/gesichtsbildabgleich.html>). Diese Technik gilt es, auch präventiv anwenden zu können, da dadurch insbesondere serielle Kriminalität (z. B. bei bandenmässigen Ladendiebstählen, Missbräuchen von Bankkarten) besser erkannt und präventiv verhindert werden kann. Der Regierungsrat hat im Folgenden die Einzelheiten auf Verordnungsstufe zu regeln und u. a. festzulegen, mit welchen polizeilichen Datenbanken abgeglichen werden darf.

§ 52b b. Im Bereich der seriellen Kriminalität

Die Bekämpfung der seriellen Kriminalität – hauptsächlich im Bereich von Vermögensstraftaten wie Einbrüchen, Diebstählen, gewerbsmässigen Versicherungsbetrügen – bezweckt neben der Aufklärung von bereits begangenen Delikten insbesondere die Verhinderung von weiteren Straftaten durch dieselben Täterschaften. Aufgrund der Datenmengen und der Komplexität der Fälle braucht die Polizei für die Zukunft Analysesysteme, um die polizeilich erhobenen Daten wie z. B. die Örtlichkeiten, Tathergänge, Tatwerkzeuge, betroffene Personen oder Kommunikationsmittel (insbesondere bei Cyberdelikten) zu strukturieren und durch polizeiliche Kriminalanalytistinnen und -analysten zu analysieren, um Zusammenhänge bzw. verbundene Täterschaften erkennen zu können. In der schweizerischen Polizeilandschaft haben sich hierfür u. a. die Systeme PICAR und PICSEL etabliert. PICAR ist eine Datenbank für die Kriminalanalyse, das dem Monitoring der seriellen und mobilen Kriminalität in Form von Einbruchdiebstählen, Trickdiebstählen, Sexualdelikten usw. dient. Die Datenbank PICSEL ermöglicht spezifisch die Analyse von Erkenntnissen bei Cyberdelikten wie Online-Betrüge, Online-Erpressungen usw. Beide Systeme verfolgen das Ziel, über die Kantonsgrenzen hinaus Zusammenhänge zu erkennen.

Die vorliegend beschriebenen Analysesysteme für serielle Kriminalität grenzen sich vom interkantonalen Datenaustausch im Abrufverfahren nach dem Projekt POLAP (vgl. Erläuterungen zu §§ 54b und 54c) dahingehend ab, dass nur die Mitarbeitenden der Kriminalanalyse Zugang zu den eigentlichen Quelldaten haben. Die übrigen Polizeianghörigen werden von der Kriminalanalyse nur mit den Erkenntnissen bedient und haben keine direkte Abfragemöglichkeit.

Da das Bundesgericht die Rechtmässigkeit des Luzerner Polizeigesetzes beim Einsatz von einfachen Analysesystem bejaht hat (BGE 1C_63/2023 E. 4), stützt sich der vorliegende Gesetzesentwurf auf den Luzerner Gesetzestext. Im Nachgang zur vorliegenden Gesetzesrevision müssen die Ausführungsvorschriften noch auf Verordnungsstufe konkretisiert werden (vgl. BGE 1C_63/2023 E. 4.7).

§ 54 Gemeinsames Informationssystem

Bei § 54 handelt es sich um die bisherige formell-gesetzliche Grundlage für das Polizeiinformationssystem POLIS, das von der Kantonspolizei und den Stadtpolizeien Zürich und Winterthur gemeinsam betrieben wird. Die Bestimmung ist mit dem Zusatz «modulares» polizeiliches Informationssystem zu ergänzen, um eine zweckgemässe Gliederung des Systems zu gewährleisten. Zudem ist das Forensische Institut Zürich hier analog zu § 52 aufzuführen.

§§ 54a–54e Elektronische Zusammenarbeit

§ 54a a. Im Allgemeinen

Die Revision soll nichts an der bisherigen Kompetenzaufteilung zwischen den Polizeikörpern gemäss POG ändern. Indem § 54a Abs. 1 festhält, dass die Zusammenarbeit im Rahmen der Aufgabenerfüllung zu erfolgen hat, wird die sachliche Zuständigkeit vorausgesetzt. Als «Polizei» ist auch das Forensische Institut Zürich zu verstehen, das gemäss § 2a POG als Polizeibehörde gilt. Die polizeilichen Aufgaben sind in §§ 3ff. PolG sowie in §§ 7ff. POG klar definiert. In anderen Gesetzen können ihr weitere Aufgaben zugewiesen sein, wie z. B. im Gewaltschutzgesetz vom 19. Juni 2006 (LS 351) oder im Bevölkerungsschutzgesetz vom 4. Februar 2008 (LS 520).

Das Bundesgericht hat sich in seinem Entscheid 1C_63/2023 über den Datenaustausch im Rahmen eines polizeilichen Informationssystem-Verbands des Bundes und der Kantone geäussert und stellt für Bestimmungen über den Austausch von Informationen im Abrufverfahren sehr hohe Anforderungen an den Regulierungsgrad. Dies wiederum gilt auch für den Betrieb von gemeinsamen Informationssystemen.

§ 54a regelt zunächst nur die Grundlage für die elektronische Zusammenarbeit. Für den tatsächlichen Datenaustausch sind bestehende gesetzliche Grundlagen vorausgesetzt wie beispielsweise im Amts- oder Rechtshilfeverfahren oder mit dem neu geschaffenen § 54b. Andere als die Zürcher Polizeibehörden sollen auf die Daten in den zürcherischen polizeilichen Informationssystemen grundsätzlich keinen umfassenden direkten Zugriff haben. Vielmehr werden ihnen diese nur auf konkrete Anfrage im Einzelfall auf elektronischem Weg zugänglich gemacht. Dafür soll gemäss Abs. 2 auch die Schaffung von Schnittstellen zulässig sein.

Soweit diese nicht nur konkrete Anfragen im Einzelfall, sondern direkt im Abrufverfahren ermöglichen, gelten die im neuen § 54b statuierten strengen Einschränkungen. Auf den Betrieb gemeinsamer Informationssysteme mit Behörden des Bundes oder anderer Kantone und Gemeinden wird verzichtet.

§ 54b b. Bekanntgabe von Daten im Abrufverfahren

Für die Erkennung und Abwehr von Gefahren ist es wichtig, dass die Polizei bei der Überprüfung einer Person nicht nur die im eigenen System registrierten Vorgänge sieht, sondern auch auf Vorkommnisse in anderen Kantonen aufmerksam wird. Vermutet die Polizei, dass eine Person in anderen Kantonen bekannt ist, hat sie heute per E-Mail oder Telefon bei der zuständigen ausserkantonalen Behörde anzufragen, die dann auf einem dieser Wege die benötigten Informationen im Rahmen der Amtshilfe übermittelt. Oftmals erreichen diese Informationen die Zürcher Polizei aber zu spät, weshalb z. B. ein verdächtigtes Verhalten im Nachbarkanton erst dann entdeckt wird, wenn die Person bereits wieder aus der Kontrolle entlassen worden ist. Die Informationsdefizite nutzen z. B. Einbrecherinnen und Einbrecher aus, die häufig national oder sogar international aktiv sind. Wenn die Polizei eines Kantons mutmassliche Einbrecherinnen und Einbrecher überprüft, ist es entscheidend, zu wissen, ob diese Personen in einem anderen Kanton im Zusammenhang mit Einbrüchen bekannt sind. Auch wenn jemand in einem Kanton mit Drohungen auffällt, kann für die Einschätzung der Gefahrenlage relevant sein, ob die Person in anderen Kantonen bereits polizeibekannt ist. Kriminelle Gruppierungen agieren oft interkantonal und international, besonders in den Bereichen Cyberkriminalität, Menschenhandel, Terrorismus und bandenmässigen Vermögensdelikten. Der rasche Erhalt von Informationen anderer Kantone ist daher entscheidend, um Serien und Zusammenhänge zu erkennen.

Zur Verbesserung der polizeilichen Informationsvorgänge des Bundes und der Kantone ist deshalb eine polizeiliche Abfrageplattform «POLAP» projektiert. POLAP dient als zentralisiertes Online-System, das es ermöglicht, Informationen aus kantonalen, nationalen und internationalen Datenbanken effizient und standardisiert abzurufen. POLAP agiert als eine Art Transportkanal, der den Nutzenden über standardisierte Ansichten vordefinierte Informationen aus den angeschlossenen Datenbanken bekannt gibt. Diese Datenbanken werden als «Quellsysteme» bezeichnet. POLAP speichert keine Daten, sondern ermöglicht die Anzeige von spezifischen Informationen aus den angeschlossenen Quellsystemen wie Personen-, Fahrzeug- oder Waffendaten. Der oder die Nutzende greift aber nicht direkt auf das Quellsystem zu und kann darin deshalb auch nichts verändern.

Bereits heute besteht ein Verbund der verschiedenen polizeilichen Informationssysteme, gestützt auf verschiedene Rechtsgrundlagen, insbesondere dem Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes (BPI, SR 361). Das von der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren genehmigte Programm POLAP bringt für die Kantone zwei wesentliche Verbesserungen; erstens ermöglicht es die Abfrage auf alle zulässigen Informationssysteme über eine einheitliche Oberfläche mittels einer Abfrage und zweitens modernisiert es den nationalen Polizeiindex. In diesem sind bereits heute die gemäss Art. 17 BPI bezeichneten Daten aus den Informationssystemen der kantonalen Polizeibehörden enthalten. Dieses System soll sukzessive durch POLAP abgelöst werden, damit die Daten nicht zuerst in einer eigenen Datenbank des Polizeiindexes zusammengeführt und verwaltet werden müssen, sondern direkt im Abrufverfahren zugänglich gemacht werden. Damit wird das heute bestehende Problem der zeitverzögerten Übermittlung der Daten in die Datenbank des Polizeiindexes sowie deren Aktualität und Vollständigkeit behoben. Der Umfang der über POLAP im Abrufverfahren bereitgestellten Daten ist gegenüber dem Polizeiindex damit detaillierter, umfasst aber wie bisher auch nur den Grund des Eintrags und keinen vollständigen Zugriff auf alle Daten im kantonalen System.

Weitergehende Informationen über einen Vorgang werden nicht mit POLAP verfügbar, sondern sind wie bisher über das Amtshilfeverfahren einzuholen. POLAP erlaubt aber in vielen Fällen eine genügende Übersicht, um die Amtshilfe auf die relevanten Fälle zu reduzieren. Es erfolgt eine Protokollierung jeder Abfrage im Quellsystem, was eine transparente und nachvollziehbare Datenweitergabe zwischen den Polizeibehörden sicherstellt.

Aufgrund der erwähnten höchstrichterlichen Rechtsprechung ist ein spezifisch auf das Abfragesystem POLAP ausgerichteter § 54b zu schaffen.

Der neue § 54b regelt nur den Zugriff ausserkantonomer Behörden auf die Zürcher Polizeidaten über das Abfragesystem POLAP. Das Projekt knüpft diesen Zugang an die Voraussetzung, dass Daten aus den eigenen Datenbearbeitungs- und Informationssystemen zur Verfügung gestellt werden. Für die Frage, inwieweit Zürcher Polizeiangehörige darauf zugreifen und diese bearbeiten dürfen, wird in § 54c auf die entsprechenden Regelungen ausserkantonomer Behörden verwiesen.

Das Bundesgericht kritisierte in seinem Entscheid 1C_63/2023 in Bezug auf die Regelung des Kantons Luzern, sie sei zu weit gefasst, da sie weder den Zweck des Datenaustauschs, die betroffenen Datenkategorien, den Kreis der beteiligten Behörden noch die Zugriffsberechtigten genügend begrenze. Auch sei nicht ersichtlich, warum für Bagatelldfälle ein Zugriff im Abrufverfahren erforderlich sei (vgl. BGE 1C_63/2023).

E. 6). Dieser Kritik wird in erster Linie begegnet, indem die Daten massiv eingeschränkt werden, die im Abrufverfahren überhaupt bekannt gegeben werden sollen (Einzelheiten siehe Erläuterungen zu Abs. 5 und 6). Zusätzlich wird dem Anspruch an den Datenschutz und die Verhältnismässigkeit Rechnung getragen, indem die Abfragerechte differenziert nach Rollen und dem Kontext, in dem die Abfrage erfolgt, abgestuft und sämtliche Abfragen auf die Datensysteme protokolliert werden (Einzelheiten siehe Erläuterungen zu Abs. 7).

Abs. 1 stellt klar, dass der vorliegende Paragraph spezifisch die Bekanntgabe von Daten aus den polizeilichen Datenbearbeitungs- und Informationssystemen des Kantons Zürich (bislang POLIS) im Abrufverfahren regelt. Der Kanton Zürich soll sich zu diesem Zweck an der Abfrageplattform POLAP beteiligen und seine Systeme daran anschliessen dürfen. Um die in POLAP sehr differenzierten Zugriffsrechte abzubilden, ist es unumgänglich, dass jede Stufe auf die weiterführenden Einschränkungen der nächsten verweist, um deren Vernetzung zu verdeutlichen. Zum besseren Verständnis, wie der vorliegende Paragraph zu lesen ist, wird dessen Aufbau in Abs. 1 lit. a–d erläutert.

Abs. 2 trägt dem erwähnten Bundesgerichtsentscheid Rechnung, indem er die Behörden genau bezeichnet, die beschränkt auf ihre eigene Zweckerfüllung via POLAP Abfragen auf den Zürcher Datenbearbeitungs- und Informationssystemen vornehmen können, also an welche die Zürcher Polizei Daten bekannt gibt. Es handelt sich dabei allesamt um Behörden, die polizeiliche Aufgaben wahrnehmen. Die Polizeibehörden der Zürcher Gemeinden sind nicht aufgeführt, da diese entweder selbst am Zürcher System beteiligt sind oder ihnen darauf direkter Zugriff gewährt werden kann (§ 54 Abs. 1 und 4). Gleichzeitig wird in Abs. 2 normiert, für welche Aufgaben die konkrete Behörde via POLAP Daten abrufen kann.

Abs. 3 beschränkt den Zugriff auf definierte, polizeiliche Aufgaben, zu deren Erfüllung die in Abs. 2 genannten Behörden Daten über POLAP abfragen können. Den Angehörigen einer Polizeibehörde wird eine Rolle in POLAP vergeben, die diesen Aufgaben entsprechen. Je nach dem, für welche polizeiliche Aufgabe die Datenabfrage ausgeführt wird, stehen unterschiedliche Abfragekontexte (und damit verbunden unterschiedliche Quellsysteme, siehe Erläuterungen zu Abs. 4) zur Verfügung. Das Rollenkonzept ist ein wichtiger Teil der verhältnismässigen Ausgestaltung der Datenbekanntgaben («Need to know»-Prinzip). Die vorliegend verwendeten Begriffe der Aufgaben und Zwecke entsprechen denjenigen für die im Projekt POLAP vorgesehenen Rollen bzw. Kontexte.

Als eine erste Rolle wurde die «gerichts- und sicherheitspolizeiliche Aufgabe» definiert (Abs. 3 lit. a). Damit wird sowohl die repressive, kriminalpolizeiliche Tätigkeit (Aufklärung von Straftaten) als auch die prä-

ventive Polizeitätigkeit (Verhinderung von Straftaten) erfasst. Dieser Rolle stehen aufgrund des grossen öffentlichen Interesses an der Verhinderung und Erkennung von Straftaten die meisten Abfragekontexte zur Verfügung. «Verwaltungspolizeiliche Aufgaben» (Abs. 3 lit. b) sind einerseits polizeiliche Aufgaben, die durch Angehörige von Verwaltungsbehörden (z. B. Zollbeamtinnen und Zollbeamte) ausgeübt werden, anderseits verwaltungsrechtliche Aufgaben, die durch die Polizeibehörden wahrgenommen werden (z. B. Waffenbewilligungen oder Personensicherheitsüberprüfungen). Damit die Polizistinnen und Polizisten ihre Aufgaben wahrnehmen können, braucht es zudem Personen mit unterstützenden und koordinativen Aufgaben (vgl. Abs. 3 lit. c). Ähnlich verhält es sich mit «Polizeiassistentinnen und Polizeiassistenten (mit oder ohne Diplom)» (Abs. 3 lit. d), die z. B. Eingangskontrollen bei Behörden usw. wahrnehmen. Die eingrenzende Funktion der Rollen zeigt sich bei den «militärpolizeilichen Aufgaben» (Abs. 3 lit. e) und den «transportpolizeilichen Aufgaben» (Abs. 3 lit. f). Angehörige der Militärpolizei können POLAP gemäss ihrer gesetzlichen Ermächtigung lediglich im Rahmen von Verkehrskontrollen und militärpolizeiliche Überprüfungen verwenden. Die Transportpolizei kann nur im Kontext «transportpolizeiliche Kontrolle» POLAP abfragen.

Abs. 4 regelt die zulässigen Bearbeitungszwecke, die eine Abfrage rechtfertigen. Jeder Kontext begrenzt die Auswahl an möglichen Quellsystemen, die über POLAP abgefragt werden darf. Mit POLAP werden keine neuen Zugriffsberechtigungen eingeführt, sondern die bestehenden gesetzlichen Abfragerechte systematisch kanalisiert. Damit die Datenbekanntgabe im Abrufverfahren verhältnismässig ist, werden den Nutzenden nicht in allen Abfragekontexten Daten aus allen Quellsystemen bekannt gegeben. Die Regelung unterscheidet folgenden Kontexte:

Im Kontext «Grenzkontrolle an der Schengen-Aussengrenze» (Abs. 4 lit. a) geht es um die systematische Kontrolle aller Personen bei der Einreise in den Schengen-Raum an den Schweizer Flughäfen. Die Vornahme der systematischen Kontrolle ist in Art. 8 des Schengener Grenzkodex geregelt (Verordnung [EU] 2016/399) und besteht je nachdem, ob es sich um eine/n EU-Bürger/in bzw. eine/n Schweizerbürger/in oder eine/n Drittstaatsangehörige/n handelt, in einer Feststellung der Identität, der Staatsangehörigkeit (u. a. anhand des Reisedokuments), der Überprüfung des Reisedokuments und Abfrage der Person sowie der Dokumente in den internationalen, europäischen und nationalen Datenbanken. Zusätzlich wird überprüft, ob die Person keine Gefahr für die öffentliche Ordnung, die innere Sicherheit, die öffentliche Gesundheit oder die internationalen Beziehungen einer der Schengen-Mitgliedstaaten darstellt.

Der Kontext «Personenkontrolle im Inland» (Abs. 4 lit. b) ist gegeben, wenn eine Person angehalten, kontrolliert oder festgenommen wird, z. B. bei Verdacht auf eine Straftat. Die Voraussetzungen sind im jeweils anwendbaren Polizeigesetz (im Kanton Zürich § 21 PolG) bzw. in der StPO geregelt. Die Identität einer Person soll zuverlässig festgestellt und ihre Angaben verifiziert werden, ihre Berechtigungen, wie z. B. das Recht, ein Fahrzeug zu lenken, eine Waffe zu transportieren, legal in die Schweiz einzureisen oder sich dort aufzuhalten, sollen überprüft und es soll festgestellt werden, ob die Person oder ein von ihr mitgeführter Gegenstand zur Fahndung ausgeschrieben ist. Zusätzlich interessieren die Gründe für die Ausschreibung, die Gefährlichkeit und welche Sofortmassnahmen zu ergreifen sind. Für den Entscheid über das weitere Vorgehen ist mitunter von Bedeutung, ob sich aus den bestehenden polizeilich registrierten Daten Hinweise für deliktisches Verhalten ergeben.

Abfragen im Kontext «Ermittlungen (polizeiliche Vorermittlungen und strafprozessuale Ermittlungen)» (Abs. 4 lit. c) werden bei Ermittlungshandlungen der Polizei getätigt. Unter polizeilichen Vorermittlungen versteht man Abklärungen und Massnahmen der Polizei, die auf Verdachtsbegründung ausgerichtet sind und die auf einem bloss vagen, noch unbestimmten Anfangsverdacht oder kriminalistischen Erfahrungswerten gründen. Ermittlungen nach Art. 306 StPO werden angehoben, wenn ein hinreichender Tatverdacht auf straffbare Handlungen vorliegt. Dabei wertet die Polizei neben den ihr zugänglichen polizeilichen und amtlichen Registern allgemein zugängliche Informationen oder Beobachtungen im öffentlichen Raum aus. Die polizeilichen Abklärungen beschränken sich nicht auf die unter Verdacht stehende Person, sondern umfassen auch Personen und Sachen in deren Umfeld. Zum Kontext «Ermittlung» gehört auch die Identifikation von Opfern von Unfällen, Naturkatastrophen und Gewalttaten sowie von geschädigten oder vermissten Personen.

Der Kontext «Verkehrskontrolle» (Abs. 4 lit. d) kommt bei Strassenverkehrskontrollen zur Anwendung. Diese dienen der Kontrolle der Fahrberechtigung und Fahrfähigkeit der Fahrzeugführerinnen und Fahrzeugführer sowie der Kontrolle des technischen Zustandes von Fahrzeugen. Kontrollen des ruhenden Verkehrs haben im System POLAP einen eigenen Kontext. Für solche Kontrollen ist kein Zugriff auf die Daten der Zürcher Datenbearbeitungs- und Informationssysteme vorgesehen, weshalb dieser Kontext vorliegend nicht zu regeln ist.

Im Kontext «Gewaltschutz» (Abs. 4 lit. e) geht es um die Verhinderung und Erkennung von schweren Gewaltdelikten. Ein Schwerpunkt ist die Früherkennung von Warnsignalen (gewaltverschärfendes Verhalten) im Vorfeld zielgerichteter Gewalt im familiären Umfeld sowie im Alltag im Umgang mit Behörden und Verwaltungen. Dazu muss die Gewaltbereitschaft einer Person erkannt und strukturiert beurteilt werden.

Diese Beurteilung gibt Aufschluss über die Interventionsnotwendigkeit und -dringlichkeit. Mit den gewonnenen Erkenntnissen werden sodann die entsprechenden Massnahmen festgelegt und umgesetzt.

Bekanntgaben im Kontext «Bearbeiten von Ausweisverlustmeldungen» (Abs. 4 lit. f) sind im Rahmen der Aufnahme von Verlustmeldungen gemäss Art. 8 und 12 des Bundesgesetzes vom 22. Juni 2001 über die Ausweise für Schweizer Staatsangehörige (SR 143.1) notwendig.

Der Kontext «Personensicherheitsüberprüfungen» (Abs. 4 lit. g) dient zur Prüfung von Personen, die sicherheitsempfindliche Funktionen ausüben oder sich in sicherheitsempfindlicher Umgebung aufhalten bzw. in entsprechenden Projekten tätig sind und die somit Zugang zu sensiblen Einrichtungen und Informationen haben.

Im Kontext «waffenrechtliche Bewilligungen» (Abs. 4 lit. h) werden Abklärungen getätigt, die vor dem Erteilen einer waffenrechtlichen Bewilligung gemacht werden müssen, um allfällige Hinderungsgründe auszuschliessen, die gegen das Ausstellen der Bewilligung sprechen. Waffenrechtliche Bewilligungen sind zudem erforderlich für das Tragen von Waffen (Tragbewilligung), für das Verbringen über die Grenze (EU-Feuerwaffenpässe) und weitere Sachverhalte (wie z. B. das Schiessen mit Seriefeuerwaffen).

Der Kontext «Bewilligungen, namentlich für Sicherheitsunternehmen» (Abs. 4 lit. i) dient dazu, Abklärungen betreffend juristische Personen (z. B. Sicherheitsunternehmen) und natürliche Personen (z. B. Geschäftsführerinnen und Geschäftsführer einer Sicherheitsfirma) zu allfälligen Hinderungsgründen im Rahmen der Erteilung von Betriebsbewilligungen vorzunehmen. Je nach kantonaler Gesetzgebung betrifft dies neben den Betriebsbewilligungen für private Sicherheitsunternehmen auch verschiedene Bewilligungen für Mitarbeitende eines Sicherheitsunternehmens, spezifische Bewilligungen für spezialisierte Personen (z. B. Detektivinnen und Detektive, Hundeführerinnen und Hundeführer) sowie Bewilligungen zum Ausüben spezieller Tätigkeiten (z. B. Verkehrsdienste).

Daneben bestehen die Kontexte «militärpolizeiliche Überprüfungen» (Abs. 4 lit. j) und «transportpolizeiliche Überprüfungen» (Abs. 4 lit. k). Diese Kontexte stehen einzig der Militär- bzw. der Transportpolizei zur Erfüllung ihrer Aufgaben zur Verfügung.

Die Kontexte entscheiden auch, nach welchen Eigenschaften in POLAP eine Abfrage möglich ist. In den meisten Kontexten steht lediglich eine Abfrage nach Personen zur Verfügung. In den Kontexten «Personenkontrolle im Inland» und «Ermittlungen» können zudem Fahrzeuge oder Sachen (z. B. anhand von Seriennummern usw.) abgefragt werden. Im Kontext «Verkehrskontrolle» ist neben der Personenabfrage auch die Fahrzeugabfrage freigeschaltet.

Abs. 5 benennt, welche Datentypen im Abrufverfahren aus dem Quellsystem bekannt gegeben werden. Gemäss dem Entscheid des Bundesgerichts (BGE 1C_63/2023 E. 6.6.1) muss das Gesetz die zur Bekanntgabe im Abrufverfahren vorgesehenen Datenkategorien benennen und eingrenzen. Hingegen ist es nicht erforderlich, die einzelnen Datenfelder bereits im Gesetz aufzuführen. Dabei handelt es sich im Kanton Zürich um einen Teil der in der POLIS-Verordnung aufgelisteten Inhalte der Datenbanken. Aus diesem Grund sollen die konkreten Datenfelder durch den Regierungsrat bestimmt werden (siehe unten § 54d lit. b).

Zunächst werden via POLAP gemäss Abs. 5 lit. a Personendaten, einschliesslich besonderer Personendaten im Sinne von § 3 Abs. 4 IDG, bekannt gegeben. Es handelt sich dabei z. B. um Name, Vorname, Geburtsdatum, Heimatort, AHV-Nummer, Name der Eltern, Beschreibung des Aussehens einer Person usw. Mit «bevorzugter Vorgehensweisen» sind Modi Operandi von Täterinnen und Tätern bei Delikten gemeint, also z. B. bei Einbrecherinnen und Einbrechern, auf welche Weise sie sich üblicherweise Zugang zum Einbruchsobjekt verschaffen. Ein Grossteil dieser Daten stellen die kantonalen Polizeibehörden gestützt auf Art. 17 BPI bereits heute über den sogenannten Nationalen Polizeiindex zur Verfügung. Angezeigt werden die Personendaten zum einen nur, wenn die abgefragte Person im Rahmen der Strafverfolgung als Beschuldigte oder Geschädigte bzw. Opfer im Zusammenhang mit einem Delikt im Quellsystem registriert ist. Wer also z. B. als Zeugin oder Zeuge vermerkt ist, wird über POLAP nicht angezeigt. Obschon strafprozessual beschuldigte Personen im Ermittlungsverfahren noch als Auskunftspersonen zu befragen sind, unterscheidet das Zürcher Datenbearbeitungs- und Informationssystem POLIS zwischen den Rollen als beschuldigte oder als übrige Auskunftspersonen, da verschiedene Anforderungen an den Hinweis auf ihre Verfahrensrechte bestehen. Es ist daher nur möglich Daten anzuzeigen, wenn eine Person in der erstgenannten Rolle registriert ist. Zum anderen werden Personendaten ausserhalb der Strafverfolgung unabhängig der Verfahrensrolle angezeigt, wenn die Person im Zusammenhang mit klar bestimmten Vorfällen vermerkt ist (aussergewöhnliche Todesfälle, Vermisste, Ausweisverluste, fürsorgerische Unterbringungen, Gewaltschutzverfahren, Suizidversuche, Aufenthaltsnachforschungen, Entweichungen bzw. Entlaufen, Fundsachen sowie Verdachtsmeldungen zu Verbrechen und Vergehen).

Erfolgt eine Suche zu Fahrzeugen (Abs. 5 lit. b) oder Sachen (Abs. 5 lit. c), werden damit zusammenhängende Daten (z. B. Marke, Modell, Chassis-Nummer, Gravuren, Kaliber einer Waffe usw.) angezeigt, die entweder als gestohlen ausgeschrieben sind oder die einen Zusammenhang zu Straftaten (Abs. 5 lit. d) bzw. zu den besonderen Fällen von lit. e aufweisen. Wenn die Personen-, Fahrzeug- oder Sachabfrage ein Resultat

tat liefert, dürfen via POLAP auch die jeweiligen verknüpften Daten bekannt gegeben werden (Abs. 6). Falldaten über Straftaten (Abs. 5 lit. d) oder über weitere Vorfälle (Abs. 5 lit. e) können in keinem Kontext eigenständig abgefragt werden. Sie erscheinen nur, wenn sie mit der abgefragten Person, Sache oder dem abgefragten Fahrzeug verknüpft sind.

Bei Straffällen (Abs. 5 lit. d) ist die Bekanntgabe in mehrfacher Hinsicht eingeschränkt. So werden keine Daten über Fälle bekannt gegeben, die im Zürcher Quellsystem aufgrund von § 54f Abs. 1 bei Freisprüchen, Einstellungen oder Nichtanhandnahmen von Strafverfahren nachgeführt werden mussten. Sodann werden nur Verbrechen und Vergehen mit Angabe der Straftat bekannt gegeben. Bei Übertretungen, also z. B. bei geringfügigem Ladendiebstahl, zeigt POLAP aus Verhältnismässigkeitsgründen lediglich an, dass einer oder mehrere Einträge in einem Quellsystem vorhanden sind, nicht aber weitere Daten zum Fall. Diese müsste die abfragende Behörde auf dem Amtshilfeweg und somit unter Angabe des Anfragegrundes in Erfahrung bringen. Gar nicht Teil des Abfrageverfahrens sind Vorkommnisse, die mit Ordnungsbussen erledigt worden sind. So werden z. B. Parkbussen nicht im Quellsystem gespeichert und können daher auch nicht bekannt gegeben werden.

Das Interesse an der Bekanntgabe der weiteren im Gesetz (Abs. 5 lit. e) umschriebenen Fälle ist unterschiedlich begründet: Solche Angaben können Hinweise auf eine Selbst- oder Drittgefährdung der abgefragten Person geben, was die Polizei zu besonders behutsamem Vorgehen mahnt. Aufenthaltsnachforschungen dienen der ausschreibenden Behörde zur Rechtsdurchsetzung. Die Meldung von Ausweisverlusten in mehreren Kantonen kann auf die Absicht einer missbräuchlichen Verwendung der Ersatzdokumente hinweisen. Vorbereitungshandlungen zu Verbrechen und Vergehen sind grundsätzlich nicht strafbar (Ausnahmen in Art. 260^{bis} StGB). Stellt die Polizei z. B. bei der Kontrolle eines Fahrzeuges Einbruchswerkzeug fest, kann den Insassen aber noch keinen mindestens versuchten Einbruch nachweisen, weil sie sich erst auf dem Weg zur Tat befunden haben, kann sie lediglich eine Verdachtsmeldung machen. Die Bekanntgabe solcher Verdachtsmeldungen dient als Hinweis zur genaueren Kontrolle, wenn die Personen in einem anderen Kanton erneut kontrolliert werden. Eine rasche Bekanntgabe dieser Daten auf dem Wege des Abrufverfahrens ist deshalb sehr wichtig und verschafft den Polizeifunktionärinnen und -funktionären im Einsatz ein klareres Bild der Lage.

Abs. 6 schreibt vor, dass über POLAP keine Journaldaten oder andere in den kantonalen Datenbearbeitungs- und Informationssystemen abgelegte Dokumente wie Rapporte und Einvernahmen bekannt gegeben werden. In Journalen werden alle polizeilichen Einsätze protokolliert, auch wenn sie nicht in einer Fallbearbeitung resultieren. Solche Einträge sollen nicht abgefragt werden können. Ebenso sollen die in den Daten-

bearbeitungs- und Informationssystemen abgelegten Dokumente wie Rapporte oder Einvernahmen, aus denen naturgemäss heikle Details ersichtlich sein könnten, nicht auf diese Weise einsehbar sein. Ist im konkreten Fall für die Erfüllung der polizeilichen Aufgabe eine Einsicht erforderlich, muss im Amts- bzw. Rechtshilfverfahren nach § 54a darum ersucht werden.

Abs. 7 schliesslich regelt die Kontrollmechanismen, die einen Missbrauch von POLAP verhindern sollen. Einerseits ist sicherzustellen, dass sämtliche Abfragen im Quellsystem protokolliert werden, sodass eruiert werden kann, wer die Abfrage getätigt hat. Das Protokoll kann die bzw. der Beauftragte für den Datenschutz gestützt auf § 35 IDG jederzeit einsehen und kontrollieren. Gleichzeitig ist stichprobenweise zu kontrollieren, dass sich die Zürcher Benutzenden von POLAP an die rechtlichen Vorgaben halten, wenn sie ihrerseits Abfragen in POLAP vornehmen. Die Ergebnisse der Kontrollen sind der bzw. dem Beauftragten für den kantonalen Datenschutz vorzulegen. Ausserdem ist eine koordinierte Beaufsichtigung mehrerer zuständigen Aufsichtsbehörden möglich (siehe auch § 37 IDG). Die Zugriffsprotokolle können zu diesem Zweck an die zuständigen Behörden herausgegeben werden.

§ 54c c. Bearbeitung von Daten aus Systemen anderer Behörden

Damit ein Kanton Daten aus polizeilichen Datenbearbeitungs- und Informationssystemen anderer Kantone abrufen und bearbeiten kann, wie es das Projekt POLAP vorsieht, braucht es eine zusätzliche Rechtsgrundlage beim Kanton des Quellsystems als Datenherr. Da das Projekt POLAP bei einer Anbindung verlangt, dass jeweils auch die eigenen Datenbearbeitungs- und Informationssysteme zur Verfügung gestellt werden, ist davon auszugehen, dass auch andere Kantone eine mit § 52b vergleichbare Regelung erlassen werden. Da diese auf Zürcher Polizeiangehörige jedoch nicht direkt anwendbar sind, bedarf es einer Verweisung auf diese im neuen § 54c. Die Zürcher Polizeiangehörigen sind berechtigt, so weit auf deren Daten zuzugreifen und diese zu bearbeiten, soweit dies die massgeblichen rechtlichen Grundlagen zulassen.

§ 54d d. Regelungsbefugnisse

Der Regierungsrat regelt, bei welchen eigenen Informationssystemen die Polizei Schnittstellen errichten kann. § 54b Abs. 5 bezeichnet die Datentypen, auf die im Abrufverfahren zugegriffen werden kann. Welche Datensätze zu den einzelnen Typen im Zürcher Datenbearbeitungs- und Informationssystem POLIS erfasst sind, regelt die POLIS-Verordnung. Der Regierungsrat hat den Zugriff auf denjenigen Teil davon zu beschränken, dessen Kenntnis für ausserkantonale Behörden zu den in § 54b Abs. 4 aufgeführten Zwecken erforderlich ist.

§ 54e e. Schengen-Informationsaustausch

§ 54e setzt die Richtlinie (EU) 2023/977 über den Informationsaustausch zwischen den Strafverfolgungsbehörden der Schengen-Staaten um. Zurzeit prüft der Bund, ob das Bundesgesetz vom 12. Juni 2009 über den Informationsaustausch zwischen den Strafverfolgungsbehörden des Bundes und denjenigen der anderen Schengen-Staaten (Schengen-Informationsaustausch-Gesetz) durch einen Bundesbeschluss zu ersetzen ist (vgl. BBl 2024 2360). Es ist daher generell auf die bundesrechtlichen Bestimmungen und den anzuwendenden Art. 355c StGB zu verweisen.

II. Änderungen des Polizeiorganisationsgesetzes

§ 29 Kantonsübergreifende Zusammenarbeit

Die Kantonspolizei verfügt über eine umfangreiche Palette an Informatiklösungen, die in der täglichen Polizeiarbeit Anwendung finden und auch für Partnerorganisationen relevant sein können. Mit dieser Bestimmung soll für die Erbringung solcher, aber auch weiterer Dienstleistungen durch die Kantonspolizei oder das Forensische Institut Zürich eine Grundlage geschaffen werden.

Gemäss § 30 Abs. 1 des Gesetzes über Controlling und Rechnungslegung vom 9. Januar 2006 (CRG, LS 611) erfordert die Erbringung gewerblicher Dienstleistungen, die nicht ausnahmsweise nach § 30 Abs. 2 CRG vom Regierungsrat bewilligt werden können, eine formell-gesetzliche Grundlage, die hier geschaffen wird.

5. Finanzielle Auswirkungen

Die Vorlage selbst bringt keine neuen Verpflichtungen mit sich und verursacht keine Kosten. Solche können allerdings im Zusammenhang mit der Teilnahme der Kantonspolizei an Systemen zum Datenaustausch mit anderen Behörden bzw. mit dem Betrieb entsprechender Systeme entstehen. Im Gegenzug ist mit Einnahmen der Kantonspolizei im Zusammenhang mit den Gebühren für polizeiliche Berichte zu Personen und Personensicherheitsprüfungen, sowie im Zusammenhang mit dem Zurverfügungstellen von Informatiklösungen und anderen Dienstleistungen an Partnerorganisationen zu rechnen. Zum voraussichtlichen Umfang dieser Kosten und Einnahmen lassen sich noch keine konkreten Aussagen machen.

6. Regulierungsfolgeabschätzung

Eine Regulierungsfolgeabschätzung im Sinne des Gesetzes zur administrativen Entlastung der Unternehmen vom 5. Januar 2009 (LS 930.1) ist vorliegend nicht nötig, da die Vorlage keine direkten administrativen Mehrbelastungen von Unternehmen zur Folge hat.

7. Fakultatives Referendum

Diese Gesetzesänderungen unterstehen dem fakultativen Referendum gemäss Art. 33 der Verfassung des Kantons Zürich vom 27. Februar 2005 (LS 101).

8. Antrag

Der Regierungsrat beantragt dem Kantonsrat, den Gesetzesänderungen zuzustimmen.

Im Namen des Regierungsrates

Die Präsidentin:	Die Staatsschreiberin:
Natalie Rickli	Kathrin Arioli