Antrag des Regierungsrates vom 28. August 2024

5977

Polizeigesetz (PolG)

(Änderung vom . . . . . .; Datenbearbeitung)

Der Kantonsrat,

nach Einsichtnahme in den Antrag des Regierungsrates vom 28. August 2024,

beschliesst:

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

Geltungsbereich

§ 2. Abs. 1 unverändert.

[2] Für die polizeiliche Tätigkeit im Rahmen der Strafverfolgung gelten nur §§ 32 d–32 h, 32 k, 32 m, 32 n und 54 a–54 d 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.

Polizeiliche Observation

§ 32. Abs. 1 und 2 unverändert.

[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 Beweiszwecken 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.

d. Überwachung des Strassenverkehrs mit Videogeräten

§ 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:

a. Verkehrsmanagement,

b. Ereignisbewältigung bei Verkehrsunfällen,

c. Verbesserung der Strasseninfrastruktur und der Verkehrssicherheit.

[2] Für folgende Zwecke kann die Polizei die Videoaufzeichnungen des Strassenverkehrs in einer Weise auswerten, dass Personen, Fahrzeuge und Kontrollschilder identifiziert werden können:

a. Fahndung nach vermissten oder im Zusammenhang mit Verbrechen oder Vergehen gesuchten Personen oder Sachen,
b. Erkennung, Verhinderung und Verfolgung von Verbrechen oder Vergehen,
c. Beweissicherung bei Verkehrsunfällen.

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

a. der Polizeibehörden des Bundes, der Kantone und der Gemeinden,
b. der Landespolizei des Fürstentums Liechtenstein,
c. des für das Zollwesen und die Grenzsicherheit zuständigen Bundesamtes,
d. des Bundesamtes für Strassen (ASTRA),
e. des kantonalen Tiefbauamtes.

[4] In den Fällen gemäss Abs. 2 und 3 muss die Identifikation erforderlich sein und es dürfen keine weniger eingreifenden Mittel zur Verfügung stehen.

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

Automatisierte Fahrzeugfahndung im Strassenverkehr

a. Optische Erfassung, Auslesung und Abgleich

§ 32 e. [1] Die Polizei kann automatisiert Fahrzeuge, deren Insassinnen und Insassen sowie Kontrollschilder optisch erfassen, auslesen und mit polizeilichen Fahndungsaufträgen im Zusammenhang mit Delikten gemäss Art. 269 StPO sowie mit Ausschreibungen im nationalen automatisierten Polizeifahndungssystem, im Schengener Informationssystem und in der Fahndungsdatenbank für gestohlene Fahrzeuge von Interpol abgleichen

a. zur Fahndung nach vermissten oder im Zusammenhang mit Verbrechen oder Vergehen gesuchten Personen oder Sachen,
b. zur Erkennung, Verhinderung und Verfolgung von Verbrechen oder Vergehen.

[2] Erzielt der Abgleich gemäss Abs. 1 keinen Treffer, werden keine Bilder gespeichert.

[3] Geräte zur automatisierten Fahrzeugfahndung dürfen nur auf Anordnung einer Polizeioffizierin oder eines Polizeioffiziers auf- oder eingebaut werden.

[4] Mobile Geräte dürfen längstens einen Monat am gleichen Standort eingesetzt werden.

[5] Bei stationären und bei dauerhaft in Polizeifahrzeugen eingesetzten Geräten überprüft die Polizei jährlich die Zweckmässigkeit des Einsatzes.

[6] Der Einsatz der automatischen Fahrzeugfahndungssysteme wird protokolliert.

b. Bezug und Austausch von Daten

§ 32 f. [1] Die Polizei kann zu den Zwecken gemäss § 32 e Abs. 1 Daten beziehen von automatisierten Fahrzeugfahndungssystemen sowie von Verkehrsmanagement- und -überwachungssystemen

a. der Polizeibehörden des Bundes, der Kantone und der Gemeinden,
b. der Landespolizei des Fürstentums Liechtenstein,
c. des für das Zollwesen und die Grenzsicherheit zuständigen Bundesamtes,
d. des ASTRA,
e. des kantonalen Tiefbauamtes.

[2] Unter den Voraussetzungen von Abs. 3 kann sie mit den Behörden gemäss Abs. 1 lit. a–c erfasste Daten der automatisierten Fahrzeugfahndungssysteme automatisiert austauschen.

[3] Der automatisierte Austausch ist zulässig, soweit

a. diesen Behörden der Datenaustausch gesetzlich erlaubt ist,
b. der Datenschutz hinreichend gewährleistet ist,
c. das Datenschutzniveau mindestens demjenigen des Kantons entspricht.

[4] Die Polizei kann mit den automatisierten Fahrzeugfahndungssystemen der Behörden gemäss Abs. 2 Schnittstellen einrichten und nutzen.

c. Analyse von Daten

§ 32 g. [1] Die Polizei kann auf Anordnung einer Polizeioffizierin oder eines Polizeioffiziers die Daten gemäss § 32 f zur Erstellung von Bewegungsprofilen analysieren,

a. wenn eine konkrete schwere Gefahr für die öffentliche Sicherheit droht,
b. zur Verhinderung, Aufklärung oder Verfolgung eines Verbrechens oder eines schweren Vergehens.

[2] Sie kann die Daten automatisiert abgleichen mit Daten des Strassenverkehrsamtes und weiterer Verkehrszulassungsstellen zu Kontrollschildern von Fahrzeugen, deren Halterinnen oder Haltern der Führerausweis entzogen oder verweigert worden ist.

[3] Die für den Kanton Zürich zuständige Verkehrszulassungsstelle stellt der Polizei die dafür notwendigen Daten automatisiert zur Verfügung.

d. Überprüfung

§ 32 h. [1] Die oder der Datenschutzbeauftragte überprüft periodisch den Einsatz der automatisierten Fahrzeugfahndung auf die Einhaltung der gesetzlichen Bestimmungen.

[2] Sie oder er informiert die Öffentlichkeit über die Kontrollen.

§§ 32 d und 32 e werden zu §§ 32 i und 32 j.

Informationsbeschaffung im virtuellen Raum

a. Nicht zugriffsgeschützter Bereich

§ 32 k. [1] Die Polizei kann mit Software in Bereichen des Internets und in anderen Netzwerken, die nicht zugriffsgeschützt sind, Informationen beschaffen und diese bearbeiten

a. zur Erkennung und Abwehr von Gefahren für die öffentliche Sicherheit,
b. zur Durchführung von Personensicherheitsüberprüfungen gemäss § 43,
c. zur Erkennung, Verhinderung und Verfolgung von Verbrechen oder Vergehen.

[2] Nicht zulässig ist der Einsatz von Kommunikationsüberwachung im Sinne des Bundesgesetzes vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), insbesondere der Einsatz besonderer Informatikprogramme gemäss Art. 269ter StPO.

b. Zugriffsgeschützter Bereich

§ 32 l. [1] Bestehen ernsthafte Anzeichen, dass Gefahren gemäss Abs. 2 entstehen oder Straftaten gemäss Abs. 2 vorbereitet oder verübt werden, kann das Polizeikommando mit Genehmigung des Zwangsmassnahmengerichts anordnen, dass zu deren Erkennung und Abwehr Software in virtuellen Bereichen eingesetzt wird, die gegen Zugriff geschützt und einem beschränkten Benutzerkreis zugänglich sind. Nicht zulässig ist der Einsatz von Kommunikationsüberwachung im Sinne des BÜPF, insbesondere der Einsatz besonderer Informatikprogramme gemäss Art. 269ter StPO.

[2] Zulässig ist der Einsatz bei ernsthaften Anzeichen für

a. Amokläufe und Anschläge,
b. schwere Ausschreitungen und Hooliganismus gemäss Art. 2 des Konkordats vom 15. November 2007 über Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen,
c. Gewaltdelikte, schwere Sachbeschädigungen oder andere schwere Rechtsgutverletzungen einschliesslich des Aufrufs zu diesen,
d. schwere Sexualdelikte,
e. schwere Betäubungsmitteldelikte,
f. Cyberangriffe,
g Verbrechen oder Vergehen an Einrichtungen von öffentlichem Interesse.

[3] Für die Durchführung und Mitteilung der Massnahme sind Art. 274 und 279 StPO sinngemäss anwendbar. An die Stelle der Staatsanwaltschaft tritt das Polizeikommando.

Verdeckte Registrierung, gezielte Kontrolle, Ermittlungsanfrage

§ 32 m. 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.

Quellenführung

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

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.

Polizeiliche Berichte zur Person und Personensicherheitsprüfungen

§ 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,
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 Berichte müssen sachlich sein.

[5] Die Polizei kann der ersuchenden Stelle Gebühren auferlegen.

Vor Gliederungstitel «5. Abschnitt: Angehörige der Polizei»

Präventive Ausschreibung schutzbedürftiger Personen

§ 44 a. Die Polizei ist zuständig für den Entscheid im Sinne von Art. 32 Abs. 4 der Verordnung (EU) 2018/1862[1], wenn Personen nach Art. 32 Abs. 1 Bst. d und e jener Verordnung zu ihrem eigenen Schutz ausgeschrieben werden müssen.

[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.

Datenbearbeitung

§ 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.

[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.

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

Gemeinsames Informationssystem

§ 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 Zusammenarbeit

a. Schweizerische und liechtensteinische Behörden

§ 54 a. [1] Die Polizei kann zur Erfüllung ihrer Aufgaben gemäss §§ 3 ff. PolG 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

a. Schnittstellen zwischen eigenen Informationssystemen und jenen des Bundes, der Kantone und der Gemeinden einrichten,

b. mit Behörden des Bundes, der Kantone und der Gemeinden gemeinsame Informationssysteme betreiben.

[3] Die Polizei kann zur Erfüllung ihrer Aufgaben gemäss Abs. 1 Informationen, einschliesslich Personendaten und besonderer Personendaten, bei den Behörden des Bundes, der Kantone und der Gemeinden sowie des Fürstentums Liechtenstein im Abrufverfahren einholen.

[4] Die Polizei kann ihre Daten den Behörden des Bundes, der Kantone und der Gemeinden sowie des Fürstentums Liechtenstein zur Erfüllung von deren gesetzlichen Aufgaben im Abrufverfahren zur Verfügung stellen.

b. Protokollierung

§ 54 b. Die Zugriffe werden protokolliert.

c. Regelungsbefugnisse

§ 54 c. [1] Der Regierungsrat regelt durch Verordnung,

a. bei welchen eigenen Informationssystemen die Polizei gemäss § 54 a Schnittstellen einrichten kann,
b. welche gemeinsamen Informationssysteme mit anderen Behörden gemäss § 54 a betrieben werden können.

[2] Beteiligt sich die Polizei an gemeinsamen Informationssystemen mit anderen Behörden, regelt sie die Einzelheiten der Zusammenarbeit in einer Vereinbarung, insbesondere:

a. Organisation,
b. Verantwortung für den Betrieb und die Datenbearbeitung,
c. Löschfristen,
d. Massnahmen zur Gewährleistung der Informationssicherheit,
e. Modalitäten der Gewährung von Auskunft und Einsicht,
f. Kostentragung.

[3] Die Polizei bestimmt die zugriffsberechtigten Polizeistellen und Funktionen für die gemeinsam betriebenen Informationssysteme.

d. Schengen-Informationsaustausch-Gesetz

§ 54 d. Für den direkten Informationsaustausch mit Polizei- und Strafverfolgungsbehörden anderer Staaten, die mit der Schweiz über eines der Schengen-Assoziierungsabkommen verbunden sind (Schengen-Staaten), finden das Bundesgesetz vom 12. Juni 2009 über den Informationsaustausch zwischen den Strafverfolgungsbehörden des Bundes und denjenigen der anderen Schengen-Staaten (Schengen-Informationsaustausch-Gesetz) sinngemäss und Art. 355 c StGB Anwendung.

§§ 54 a–54 c werden zu §§ 54 e–54 g.*

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

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

Kantonsübergreifende Zusammenarbeit

§ 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.

IV. Mitteilung an den Regierungsrat.

Bericht

1. Ausgangslage

Die Datenbearbeitung und insbesondere der Datenaustausch unter den Polizeikorps 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 Polizeikorps 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 Deliktsprävention, namentlich bei der Abwehr von Straftaten mit extremistischem Hintergrund und bei der Verhinderung von Terroranschlägen. Die heutigen Hindernisse beim Datenaustausch stehen jedoch 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 PolG 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 Gemeindepräsidien des Kantons Zürich, den Politischen Gemeinden, dem Obergericht, dem Verwaltungsgericht, der Statthalter-Konferenz, den Ombudsstellen, dem Forensischen Institut Zürich, den Demokratischen Juristinnen und Ju-

risten 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 sind mit der vorgeschlagenen Teilrevision einverstanden. Auch die FDP unterstützt das Vorhaben, hat jedoch Vorbehalte in Bezug auf Dienstleistungen der Polizei zugunsten anderer Behörden und wünscht, dass die Observation mit GPS-Geräten und die Informationsbeschaffung im virtuellen Raum nur zur Abwehr schwerer Rechtsgutverletzungen möglich ist. AL und SP begrüssen zwar eine effizientere Zusammenarbeit der Polizeibehörden, erachten jedoch insbesondere den automatisierten Informationsaustausch und das Abrufverfahren als problematisch und fordern detaillierte Regelungen für die Datenbearbeitung auf Gesetzesstufe. Die Grünen und die DJZ lehnen die beabsichtigte Teilrevision grundsätzlich ab und halten die Änderungen insgesamt für zu wenig bestimmt und nicht verhältnismässig. Gleichermassen äusserte sich auch die Piratenpartei.

Die Gemeinden begrüssen die vorgeschlagenen Änderungen.

Die Statthalter-Konferenz unterstützt 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 begrüsst 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 Beweiszwecken im Rahmen von polizeilichen Observationen wurde eingeschränkt auf Fälle, in denen ernsthafte Anzeichen für eine Straftat im Sinne von Art. 269 der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (StPO; SR 312.0) bestehen.

– Der Einsatz automatisierter Fahrzeugfahndungssysteme im Strassenverkehr wurde in verschiedener Hinsicht stärker eingeschränkt. Die Erstellung von Bewegungsprofilen soll nur in Fällen möglich sein, in denen eine konkrete schwere Gefahr für die öffentliche Sicherheit droht oder dies der Verhinderung, Aufklärung oder Verfolgung eines Verbrechens oder schweren Vergehens dient.
– In Bezug auf die Informationsbeschaffung im virtuellen Raum wurde klargestellt, dass der Einsatz von Kommunikationsüberwachung im Sinne des Bundesgesetzes vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1), insbesondere der Einsatz besonderer Informatikprogramme im Sinne von Art. 269ter StPO, nicht zulässig ist. Der Bereich, in dem die Polizei im Internet Software einsetzen kann, wurde gegenüber der Vernehmlassungsvorlage stärker eingeschränkt.
– 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. Erläuterungen zu den einzelnen Bestimmungen

I. Änderungen des PolG

§ 2 Abs. 2 Geltungsbereich

In § 2 Abs. 2 werden die Vorgaben der StPO aufgenommen, wonach sich die Tätigkeit der Polizei im Rahmen der Strafverfolgung nach der StPO richtet. Für das Strafverfahren gelten nur die Abschnitte 3, 5 und 8 sowie §§ 32d–32h, 32k, 32m, 32n und 54a–54d. Die §§ 54a–54d betreffen den Datenaustausch im gesamten polizeilichen Tätigkeitsbereich, d. h. auch bei der Erfüllung gerichtspolizeilicher Aufgaben, weshalb diese Bestimmungen ebenfalls aufzunehmen sind.

§ 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 Rechtsprechung (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 klargestellt, 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. 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).

Abs. 2 erlaubt es der Polizei unter einschränkenden Voraussetzungen, die Aufzeichnungen gemäss Abs. 1 zu bestimmten, genau abgegrenzten Zwecken in einer höheren Qualität, welche die Identifizierung von Personen, Fahrzeugen und Kontrollschildern ermöglicht, zu verarbeiten.

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. Darüber hinaus soll die Grundlage geschaffen werden, um von weiteren Behörden solche Daten zu beziehen. In Abs. 4 wird an das Verhältnismässigkeitsprinzip erinnert.

Abs. 5 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 (LS 551.103) ist eine Regelung auf der Stufe einer internen Weisung vorzusehen. Die Polizei führt über die stationären Videoüberwachungsanlagen ein Verzeichnis, 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.

§ 32e Automatisierte Fahrzeugfahndung im Strassenverkehr, a. Optische Erfassung, Auslesung und Abgleich

Mithilfe von Systemen für die automatische Erkennung von Kontrollschildern (License Plate Recognition oder kurz LPR-Systeme) wie das vom Bund und einzelnen Kantonen bereits eingesetzte automatisierte Fahrzeugfahndungs- und Verkehrsüberwachungssystem (AFV) lassen sich in polizeilichen Fahndungsaufträgen, im nationalen automatisierten Polizeifahndungssystem (RIPOL), im Schengener Informationssystem (SIS) oder in der Fahndungsdatenbank für gestohlene Fahrzeuge von Interpol (Automated Search Facility von Interpol [ASF]) erfasste Fahrzeugkontrollschilder automatisch erkennen. Wann Fahrzeugkontrollschilder in diesen Datenbanken erfasst werden dürfen, regeln deren rechtliche Grundlagen (vgl. Art. 15 f. Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes [SR 361]). Im Falle einer Übereinstimmung vermeldet das System einen Treffer («Hit»), sodass weitere Massnahmen eingeleitet werden können (Fahrzeug- und Identitätskon-

trolle der Insassinnen und Insassen oder Standortmeldung an die Einsatzzentrale).

Da mit der Verwendung eines AFV-Systems ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung (vgl. Art. 13 Abs. 2 BV) verbunden ist, muss dessen Verwendungszweck hinreichend bestimmt sein. § 32e erlaubt den Einsatz von AFV-Systemen nicht anlassfrei, sondern nur zu den in Abs. 1 genannten Zwecken. Demnach dürfen die erfassten Kontrollschilder nur mit polizeilichen Fahndungsaufträgen zur Verfolgung von Delikten gemäss dem Deliktskatalog von Art. 269 StPO sowie mit den genannten polizeilichen Fahndungsregistern abgeglichen werden. Die heutigen AFV-Systeme protokollieren das Kontrollschild jedes vorbeifahrenden Fahrzeugs (Durchfahrtsdaten). Sie gleichen die erfassten Schilder mit den polizeilichen Datenbanken ab. Nur ein Treffer löst das Erstellen einer Bildaufnahme aus. Das ist in Abs. 2 ausdrücklich so vorzusehen, um klarzustellen, dass es bei Nichttreffern keine Bilder gibt, deren Löschung geregelt werden müsste.

Die Daten aus der AFV (einschliesslich Durchfahrtenspeicher) müssen gemäss § 53 Abs. 2 PolG gelöscht werden, sobald sie nicht mehr benötigt werden, spätestens aber nach 100 Tagen. Die Polizei hat so die Möglichkeit, z. B. nach einem Tötungsdelikt oder einem Raubüberfall in der Umgebung des Geräts zu prüfen, ob das Täterfahrzeug vor oder nach der Tat am Gerät vorbeigefahren ist. Dasselbe gilt, wenn z. B. eine in der Umgebung wohnende Person wegen Suizidgefahr dringend gesucht wird. So können Daten für solche wichtigen Fälle während einer begrenzten Zeit noch zur Verfügung stehen. Aufgrund der Rückmeldungen aus der Vernehmlassung wird der Auf- oder Einbau von AFV-Geräten weiter eingeschränkt, indem er nur von höherem Polizeikader angeordnet werden kann. Der Einsatz mobiler Geräte an einem bestimmten Standort wird auf einen Monat befristet, analog einer angeordneten Observation mittels technischer Überwachungsgeräte gemäss § 32 Abs. 2 PolG. Der Einsatz von in Polizeifahrzeugen für die Patrouillentätigkeit eingebauten AFV-Geräten unterscheidet sich vom Einsatz mobiler Geräte, die während einer bestimmten Zeit an einem Standort aufgestellt werden. Beim Einsatz in Polizeifahrzeugen prüfen die Polizeifunktionärinnen und -funktionäre zudem unmittelbar die Verwertbarkeit des Treffers.

Durch die Protokollierung des Einsatzes soll die Polizei jederzeit Rechenschaft über ihre Aktivitäten ablegen können.

§ 32f b. Bezug und Austausch von Daten

Diese Bestimmung ermöglicht es der Polizei, die erwähnten Daten zu den Zwecken gemäss § 32e Abs. 1 zu beziehen, um sie analog den Daten des eigenen AFV-Systems zu nutzen.

In §§ 54a–54d wird der Datenaustausch der Polizei im Allgemeinen geregelt. Da es im Bereich der automatisierten Fahrzeugfahndungssysteme besondere Regelungen braucht, werden in Abs. 2 und 3 die spezi-

fischen Vorschriften für den Datenaustausch mit den Polizeibehörden des Bundes, der Kantone und der Gemeinden, der Landespolizei des Fürstentums Liechtenstein, dem für das Zollwesen und die Grenzsicherheit zuständigen Bundesamt, dem ASTRA und dem kantonalen Tiefbauamt festgelegt. Ein Datenaustausch darf ausdrücklich nur für die in Abs. 1 bzw. § 32e Abs. 1 genannten Zwecke erfolgen. Für anderweitige Zwecke dürfen die erfassten Daten nicht ausgetauscht werden.

Mit Behörden gemäss Abs. 2 soll die Polizei mit deren AFV-Systemen Schnittstellen einrichten und nutzen können. Damit kann die Beschaffung bzw. Bekanntgabe der Daten beispielsweise über eine zentrale elektronische Infrastruktur (Datenplattform) erfolgen.

§ 32g c. Analyse von Daten

Abs. 1 schafft die Rechtsgrundlage für die Datenanalyse für die Erstellung von Bewegungsprofilen. Bei Vorermittlungen kann der Einsatz von AFV-Systemen zur Erstellung von Bewegungsprofilen namentlich in den Bereichen der grenzüberschreitenden Serien- und der organisierten Kriminalität, des Extremismus und des Terrorismus wertvolle Erkenntnisse liefern und dürfte als Ergänzung oder Alternative zu polizeirechtlichen Observationen zu einer Zunahme der Fahndungs- und Ermittlungserfolge beitragen. Weiter kann die Anwendung dieses Systems auch zur Verhinderung schwerer Gewaltdelikte führen, z. B. wenn Hinweise bestehen, dass ein Femizid bevorsteht und das Kennzeichen des Fahrzeugs des Gefährders bekannt ist. Aufgrund der Rückmeldungen aus der Vernehmlassung wird das Erstellen von Bewegungsprofilen nur erlaubt, um schwere Gefahren für die öffentliche Sicherheit abzuwenden oder zur Verhinderung, Aufklärung oder Verfolgung von Verbrechen und schweren Vergehen. Der Begriff der schweren Vergehen wird auch in der StPO (z. B. in Art. 221 oder Art. 231) verwendet. Darunter fallen zum Beispiel Drohungen oder Nötigungen mit einem gewissen Schweregrad (z. B. eine Bombendrohung mit anschliessender Evakuierung), schwerwiegende einfache Körperverletzungen oder schwerwiegende Delikte gegen das Vermögen. Für die Verfolgung von einfachen Vergehen und Übertretungen wird das Erstellen eines Bewegungsprofils nicht erlaubt.

Abs. 2 bildet die Grundlage für die Erkennung von Fahrzeuglenkenden mit verweigertem oder entzogenem Führerausweis. Mit § 32g Abs. 2 in Verbindung mit §§ 54a–54d soll eine Rechtsgrundlage geschaffen werden, die es erlaubt, die Daten der kantonalen Systeme zum Abgleich im Abrufverfahren zu nutzen. Damit sollen AFV-Anlagen künftig die Durchsetzung von Fahrberechtigungsentzügen bewirken bzw. zur Kontrolle entsprechender Verstösse und schliesslich zur Verbesserung der Verkehrssicherheit eingesetzt werden können. Innerkantonal soll die zuständige Verkehrszulassungsstelle der Polizei die dafür notwendigen Daten automatisiert zur Verfügung zu stellen.

§ 32h d. Überprüfung

Eine periodische Überprüfung des Einsatzes der AFV-Systeme durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten gewährleistet den ordnungsgemässen Gebrauch. Die Geltendmachung von Rechten im Zusammenhang mit der Datenbearbeitung ist mit der Auffangbestimmung von § 51 PolG, die auf das IDG verweist, sichergestellt.

§§ 32k und 32l Informationsbeschaffung im virtuellen Raum, a. nicht zugriffsgeschützter Bereich und b. zugriffsgeschützter Bereich

Im früheren § 32f war die Informationsbeschaffung im Internet geregelt. Diese Bestimmung hob das Bundesgericht auf (BGE 1C_653/2012). Mit der neuen Formulierung werden die Vorgaben des Bundesgerichts (Vorbehalt einer richterlichen Genehmigung beim Einsatz im zugriffsgeschützten Bereich und nachträgliche Information Betroffener) umgesetzt. Zudem wird aufgrund der Rückmeldungen aus der Vernehmlassung der Zweck der Informationsbeschaffung klar eingegrenzt und vom in der StPO verwendeten Begriff der «besonderen Informatikprogramme» Abstand genommen. Die Bezeichnung «Software» ist technologieneutral und beschreibt Tools, die der automatisierten Suche und Verarbeitung von Informationen in gezielten Bereichen im öffentlich zugänglichen Internet (z. B. Webcrawling) dienen. Viele solcher Tools setzen teilweise Künstliche Intelligenz ein, um die immer grösser werdende Menge der Daten effizient zu verarbeiten, insbesondere zu durchsuchen und zu strukturieren. Die daraus gewonnenen Informationen und Erkenntnisse unterstützen nur die menschliche Entscheidfindung und dienen nicht unmittelbar der Umsetzung von Massnahmen. Mit dem Begriff «Software» ist nicht der Einsatz von Kommunikationsüberwachung im Sinne des BÜPF gemeint. Ausgeschlossen ist insbesondere der Einsatz besonderer Informatikprogramme (GovWare), wie sie in der StPO genannt werden.

Die Informationsbeschaffung in den öffentlichen Bereichen des Internets ist heute für die Verhinderung und Aufklärung verschiedener Deliktsformen nicht mehr wegzudenken. Sie spielt insbesondere bei der frühzeitigen Erkennung von Radikalisierungen und Gewaltandrohungen aber auch bei anderen Deliktsformen wie beispielsweise bei Online-Anlagebetrügen eine wichtige Rolle.

Erfahrungsgemäss werden polizeilich bedeutsame Informationen im Internet meist nicht im allgemein zugänglichen Bereich, sondern in geschlossenen Foren bzw. sogenannten «Closed User Groups» ausgetauscht. Mit § 32l wird die Grundlage für einen solchen Einsatz (wie in § 32k beschrieben) in zugriffsgeschützten Bereichen geschaffen und soll der Polizei die Möglichkeit einräumen, unter ganz bestimmten Bedingungen in den abschliessend aufgezählten Fällen die Verwendung von Software anzuordnen, die auch Zugriffsbeschränkungen (z. B. Passwortschutz) um-

gehen können. Es geht 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 über bevorstehende schwere Rechtsgutverletzungen zu gewinnen, um rechtzeitig die erforderlichen Gegenmassnahmen einleiten zu können. Vorausgesetzt werden ernsthafte Anzeichen für die Entstehung solcher Gefahren bzw. für das Verüben solcher Delikte oder für entsprechende Vorbereitungshandlungen. Ein anlassfreies Durchsuchen solcher geschlossenen Foren ist damit ausgeschlossen.

Den Massstab für die Genehmigung durch das Zwangsmassnahmengericht bildet der Grundsatz der Verhältnismässigkeit gemäss § 10 PolG.

Die Verweisung auf die StPO trägt dem Umstand Rechnung, dass in der Praxis ein fliessender Übergang von präventiver (sicherheitspolizeilicher) zu repressiver (gerichtspolizeilicher) Tätigkeit stattfindet.

§ 32m 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. nArt. 33 Abs. 1 Verordnung über den nationalen Teil des Schengener Informationssystems [N-SIS] und das SIRENE-Büro vom 8. März 2013 [N-SIS-Verordnung; SR 362.0]) 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 Polizeihoheit der Kantone bedarf die Umsetzung dieser Fahndungsmassnahme im polizeirechtlichen Anwendungsbereich einer kantonalrechtlichen Grundlage, die mit § 32m geschaffen wird.

§ 32n Quellenführung

In Deliktsfeldern, in denen es üblicherweise keine Anzeigeerstattungen 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 Insiderinfor-

mationen 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 ins 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 §§ 20ff. IDG kann hier infolge der Interessenabwägung im Sinne von § 23 IDG zum Schutz der vertraulichen Quellen grundsätzlich nicht gewährt werden.

Hat ein Strafverfolgungssystem bzw. die präventive Gefahrenabwehr 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 bekommt schon heute verschiedene Anfragen. Aufgrund des sensiblen Bereichs und damit dem Persönlichkeitsschutz genügend Rechnung getragen werden kann, sind diese An-

fragen genauer zu regeln. Einerseits ist eine genügende rechtliche Grundlage zu schaffen. Anderseits 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 Dienstleistender (z. B. im IT-Bereich sowie im Bereich von Sicherheitsdienstleistungen, namentlich im Strafvollzug), Personal mit Aufgaben im Zusammenhang mit dem Betrieb kantonaler 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 PolG 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 Dienstleistender 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 einem Entscheid zu ihren Ungunsten zum Resultat der Überprüfung Stellung nehmen kann. Die Überprüfung gemäss den 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 §§ 20ff. IDG.

Mit § 43 Abs. 5 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 Auslandreise 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 wird die veraltete Bezeichnung «Datenbearbeitungssysteme» durch «Informationssysteme» ersetzt.

§ 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–54d Elektronische Zusammenarbeit

Die Revision soll nichts an der bisherigen Kompetenzaufteilung zwischen den Polizeikorps 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 §§ 3 ff. PolG sowie in §§ 7 ff. 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).

Neben Schnittstellen zur Erleichterung der elektronischen Informationsübermittlung (§ 54a Abs. 2 lit. a) sollen auch gemeinsame Systeme mit anderen Behörden betrieben (§ 54a Abs. 2 lit. b) und Daten im Abrufverfahren ausgetauscht werden können (§ 54a Abs. 3 und 4). Solche Systeme sind vor ihrer Einführung gestützt auf § 10 IDG in Verbindung mit § 24 der Verordnung über die Information und den Datenschutz vom 28. Mai 2008 (LS 170.41) im Rahmen einer Vorabkontrolle einer detaillierten Überprüfung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu unterziehen, womit die Datenschutzkonformität in jedem Einzelfall gewährleistet wird. Die Einführung neuer Systeme setzt überdies eine Schutzbedarfsanalyse sowie ein Informationssicherheits- und Datenschutzkonzept voraus.

Jede neue elektronische Zusammenarbeit bedarf der Genehmigung des Regierungsrates durch eine Verordnung (§ 54c Abs. 1). Zudem werden in der Praxis die beteiligten Polizeikorps die relevanten Eckpfeiler für den Betrieb eines gemeinsamen Systems in einer Vereinbarung (z. B. in Form eines Betriebsreglements) regeln (vgl. § 54c Abs. 2). Diese Vereinbarung hat namentlich auch Massnahmen zur Sicherstellung des Datenschutzes festzuhalten sowie die diesbezügliche Verantwortlichkeit zu regeln.

Während die Anforderung der ausdrücklichen Rechtsgrundlage für Abrufverfahren im Rahmen der Revision des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (SR 235.1) aufgehoben wurde, setzt das kantonale Recht nach wie vor eine ausdrückliche Regelung auf Gesetzesstufe voraus, die hier geschaffen wird. Im Zuge der zunehmenden

Mobilität und Internationalität bei Täterschaften besteht ein grosses Bedürfnis, Informationen und polizeiliche Erkenntnisse zwischen den Kantonen auszutauschen, damit Kriminalität weiterhin wirksam bekämpft werden kann.

Während sich § 54 auf den innerkantonalen polizeilichen Datenaustausch bezieht und in Abs. 4 auch die kommunalen Polizeikorps den Zugriff auf das System ermöglicht, beziehen sich §§ 54a–54c auf den Datenaustausch mit weiteren Behörden. Um auf die zukünftigen Entwicklungen sowohl in der Behördenlandschaft als auch in der Datenbearbeitung im Kanton Zürich reagieren zu können, sollen die weiteren Behörden und Systeme nicht weiter eingegrenzt werden.

Die Erwähnung der Gemeinden in § 54a ermöglicht den Datenaustausch mit grossen kommunalen Polizeikorps ausserhalb des Kantons Zürich (z. B. Stadtpolizeien Lausanne und St. Gallen) und hat für den innerkantonalen Datenaustausch, der in § 54 geregelt wird, keine weitere Bedeutung.

Der Zugriff eigener Polizeikräfte auf Daten gemeinsam mit anderen Behörden betriebener Systeme muss auf diejenigen Dienststellen und Funktionen beschränkt sein, die dies zur Erfüllung ihrer Aufgaben benötigen. Dies hängt von der innerbetrieblichen Aufgabenverteilung und somit von der aktuellen Struktur des Polizeikorps ab und muss bei Reorganisationen angepasst werden können. Die Polizei soll daher selbst festlegen, welche Funktionen auf welche Daten Zugriff erlangen.

Aufgrund der raschen technischen Entwicklung ist die spezifische Regelung einzelner Systeme auf Gesetzesstufe nicht praktikabel. Bis die rechtliche Grundlage für deren Betrieb bzw. für die Gewährung von Schnittstellen geschaffen wäre, wären die zugrunde liegenden Bedürfnisse und die darin festgelegten technischen Rahmenbedingungen bereits nicht mehr aktuell. Es muss daher dem Regierungsrat obliegen, in Verordnungen festzulegen, auf welche konkreten Systeme welche Behörden zugreifen und welche Systeme mit diesen gemeinsam betrieben werden.

§ 54d setzt die Richtlinie (EU) 2023/977 über den Informationsaustausch zwischen den Strafverfolgungsbehörden der Schengen-Staaten um.

II. Änderungen des POG

§ 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.

4. 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.

5. 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.

6. Fakultatives Referendum

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

7. Antrag

Der Regierungsrat beantragt dem Kantonsrat, den Gesetzesänderungen zuzustimmen.

Im Namen des Regierungsrates

Die Präsidentin: Natalie Rickli

Die Staatsschreiberin: Kathrin Arioli