

**Polizeigesetz
(Änderung vom 30. März 2026, Datenbearbeitung;
Inkraftsetzung)**

**Verordnung
über die polizeiliche Datenbearbeitung
(Erlass)**

Waffenverordnung (Änderung)

POLIS-Verordnung (Aufhebung)

(vom 23. September 2026)

Der Regierungsrat beschliesst:

I. Es wird eine Verordnung über die polizeiliche Datenbearbeitung erlassen.

II. Die Waffenverordnung vom 16. Dezember 1998 wird geändert.

III. Die Verordnung über das Polizei-Informationssystem POLIS vom 13. Juli 2005 wird aufgehoben.

IV. Die Änderung vom 30. März 2026 des Polizeigesetzes vom 23. April 2007, die neue Verordnung und die Verordnungsänderung treten am 1. Dezember 2026 in Kraft. Die bisherige Verordnung wird auf dieses Datum aufgehoben. Wird ein Rechtsmittel ergriffen, wird über die Inkraftsetzung und die Aufhebung erneut entschieden.

V. Gegen die neue Verordnung, die Verordnungsänderung, die Aufhebung der bisherigen Verordnung und gegen Dispositiv IV Sätze 1 und 2 kann innert 30 Tagen, von der Veröffentlichung an gerechnet, beim Verwaltungsgericht des Kantons Zürich Beschwerde erhoben werden. Die Beschwerdeschrift muss einen Antrag und dessen Begründung enthalten.

VI. Veröffentlichung dieses Beschlusses, der neuen Verordnung, der Verordnungsänderung und der Begründung im Amtsblatt sowie von Dispositiv IV Satz 1 in der Gesetzessammlung.

Im Namen des Regierungsrates

Die Präsidentin:

Carmen Walker Späh

Die Staatsschreiberin:

Kathrin Arioli

- | | | |
|------|---|--|
| § 1. | Diese Verordnung regelt | Gegenstand |
| a. | die polizeiliche Datenbearbeitung, | |
| b. | den Betrieb von polizeilichen Informationssystemen. | |
| § 2. | Die polizeiliche Datenbearbeitung dient folgenden Zwecken: | Zweck der polizeilichen Datenbearbeitung |
| a. | Dokumentation des polizeilichen Handelns, | |
| b. | Festhalten von ungesicherten Sachverhalten und Untersuchungen, | |
| c. | Erstellen von Berichten und Lagebeurteilungen, | |
| d. | Recherche und Analyse, | |
| e. | gemeinsame Datenhaltung, | |
| f. | Informations- und Datenaustausch, | |
| g. | statistische Auswertungen, | |
| h. | Planen und Führen von Einsätzen, | |
| i. | Sicherstellen der Verfügbarkeit von Daten, die für polizeiliche Ermittlungen benötigt werden, | |
| j. | Erstellen von Täterschaftsprofilen, | |
| k. | Führen von Geschäftskontrollen. | |

B. Bearbeitete Daten

Datentypen	§ 3. ¹ Die Polizei kann folgende Datentypen bearbeiten: - Personalien, - Fall- und Ereignisdaten, - Journaldaten, - Haftdaten, - Gästekontrolldaten, - Grenzkontrolldaten. ² Die Datentypen gemäss lit. d–f werden in separaten Systemen geführt.
Personalien	§ 4. ¹ Personalien sind Angaben zu natürlichen und juristischen Personen sowie zu Einzelunternehmen, Personengesamtheiten oder anderen Zusammenschlüssen. ² Als Personalien können bearbeitet werden: - Name, Vornamen, Ledigname, Rufnamen, Genanntnamen, Genanntvornamen, Aliasnamen, - Firma, Institution, - Branche, - Geburtsort, Geburtsstaat, Geburtsdatum, Todesort, Todesdatum, - Geschlecht, - Staatsangehörigkeit, Heimatort, - Zivilstand, - Beruf, Tätigkeit, Arbeitsort, Arbeitgeberin oder Arbeitgeber, - Sprache, - Wohn- und Aufenthaltsort bzw. Sitz, - Eltern, Kinder, - Ehegattin oder Ehegatte, eingetragene Partnerin oder eingetragener Partner, Lebenspartnerin oder Lebenspartner, - Religion, Konfession, - Vertreterin oder Vertreter, Vormundin oder Vormund, Beiständin oder Beistand, Organe, - Aufenthaltsstatus, Aufenthaltsdaten, Reisedokumente, Daten im Zusammenhang mit Grenzübertritten, - Personenbeschreibung und erkennungsdienstliche Daten, - Angaben zu Informations- und Kommunikationsmitteln einschliesslich Registrierungs- und Zugangsdaten, - Angaben zu Ausweisen,

- s. Hinweise zu strafrechtlichen, verwaltungsrechtlichen und zivilrechtlichen Verfahren und Massnahmen,
- t. Personen- und Fahndungshinweise,
- u. Verbindungen zu Personen,
- v. bevorzugte Vorgehensweisen,
- w. Effekten und mitgeführte Gegenstände,
- x. AHV-Nummer.

§ 5. ¹ Fall- und Ereignisdaten sind polizeiliche Feststellungen und Erkenntnisse, die physisch oder elektronisch festgehalten werden. Fall- und Ereignisdaten

² Als Fall- und Ereignisdaten können Angaben bearbeitet werden zu:

- a. Ort, Zeit, Ablauf und Umständen,
- b. rechtlicher Einordnung einschliesslich Tatbeständen,
- c. beteiligten Personen und Art der Beteiligung,
- d. vorliegendem Sachverhalt,
- e. Tatvorgehen und -mittel,
- f. Art und Schwere von Verletzungen,
- g. benutzten, mitgeführten, sichergestellten, gesuchten und aufgefundenen Gegenständen,
- h. Waffen,
- i. Fahrzeugen und Kontrollschildern,
- j. Aufzeichnungen einschliesslich polizeilicher Aufzeichnungen mittels Schrift, Bild, Audio- oder Videodaten,
- k. physischen und digitalen Spuren und Spurenträgern,
- l. Referenz- und Vergleichsmaterialien,
- m. forensischen Berichten und Untersuchungen,
- n. Ermittlungen,
- o. Aussagen und Einvernahmen,
- p. Fahndungen und Ausschreibungen,
- q. Verhaftungen,
- r. Strafanzeigen und -anträgen,
- s. finanziellem Schaden, Vermögenswerten, Zahlungsmitteln und Geldflüssen,
- t. Gewaltschutzmassnahmen,
- u. Verbindungen zu anderen Fällen und Ereignissen.

- Journaldaten § 6. ¹ Journaldaten sind Daten, die polizeiliches Handeln dokumentieren.
- ² Als Journaldaten können bearbeitet werden:
- a. Ereignisse, Meldungen und Anzeigen einschliesslich Tonaufzeichnungen von Notrufen,
 - b. beteiligte Personen und Art der Beteiligung,
 - c. Massnahmen und Anordnungen,
 - d. Standortdaten von Personen, die einen Notruf tätigen.
- Haftdaten § 7. ¹ Haftdaten sind Daten, welche die Durchführung von Inhaftierungen sowie Vor-, Zu- und Rückführungen und die Koordination der damit zusammenhängenden polizeilichen Tätigkeiten betreffen.
- ² Als Haftdaten können bearbeitet werden:
- a. Angaben zur Person,
 - b. Hinweise auf mögliche Beeinflussungen von Personen oder Einwirkungen auf Beweismittel,
 - c. Ort, Zeit und Datum der Inhaftierung und Entlassung,
 - d. Planung und Dokumentation der Vollzugsanordnungen und -handlungen,
 - e. Haftart, Haftstatus, Haftregime und Haftgrund,
 - f. zuständige Behörde,
 - g. noch nicht vollzogene Strafen und Massnahmen,
 - h. zugehörige administrative Hinweise.
- Gäste-
kontrolldaten § 8. Als Gästekontrolldaten können bearbeitet werden:
- a. Name, Vornamen,
 - b. Geschlecht,
 - c. Geburtsdatum,
 - d. Staatsangehörigkeit,
 - e. Adresse,
 - f. Aufenthaltsdaten,
 - g. Fahrzeugdaten,
 - h. bei ausländischer Staatsangehörigkeit ausserdem Ausweispapier und Ausweisnummer.

§ 9. ¹ Grenzkontrolldaten sind Angaben im Zusammenhang mit Grenzübertritten von Personen an der Schengen-Aussengrenze. Grenzkontrolldaten

² Als Grenzkontrolldaten können bearbeitet werden:

- a. Angaben zur Person und Erfassungsgrund,
- b. Ein- und Ausreisedaten einschliesslich Einreiseverweigerungsgründe,
- c. Ausweis- und Visa-Daten,
- d. Herkunfts- und Destinationsdaten,
- e. Flugpassagierdaten,
- f. Gepäckdaten,
- g. Vollzugsdaten einschliesslich solcher zu Asylverfahren und Wegweisungen,
- h. Angaben zu den für den Aufenthalt notwendigen finanziellen Mitteln.

C. Verantwortung und Datenzugriff

§ 10. ¹ Für die Datenaufbewahrung und -pflege ist diejenige Polizei verantwortlich, welche die Daten zur Erfüllung ihrer Aufgaben bearbeitet oder bearbeiten lässt. Verantwortung

² Die Polizei bestimmt für jedes Informationssystem eine Datenverantwortliche oder einen Datenverantwortlichen.

³ Die Datenverantwortlichen kontrollieren die Einhaltung dieser Verordnung und der gestützt darauf erlassenen Weisungen.

§ 11. ¹ Die Benutzerinnen und Benutzer der Informationssysteme haben auf diejenigen Daten Zugriff, die sie zur Erfüllung ihrer gesetzlichen Aufgaben benötigen. Datenzugriff

² Die Polizei erlässt Weisungen über die Zugriffsrechte. Sie legt die Benutzergruppen fest.

³ Die Freigabe an die einzelnen Benutzerinnen und Benutzer erfolgt unter der Verantwortung der oder des jeweiligen Datenverantwortlichen.

D. Schnittstellen und Datenübermittlung

§ 12. Schnittstellen zwischen eigenen Informationssystemen sind zulässig, sofern dadurch keine Berechtigungsbeschränkungen anderer Systeme umgangen werden. Schnittstellen zwischen eigenen Systemen

Übermittlung
in polizeiliche
Informationssy-
steme des
Bundes

§ 13. ¹ Personalien, Fall- und Ereignisdaten, Journaldaten und Gästekontrolldaten können in Systeme gemäss Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes übermittelt werden.

² Fehlen bundesrechtliche Bestimmungen, gelten diejenigen dieser Verordnung.

E. Rechte von Betroffenen und Dritten

Akteneinsicht

§ 14. ¹ Gesuche um Akteneinsicht sind schriftlich bei einer Polizei des Kantons Zürich einzureichen.

² Sie enthalten die folgenden Angaben:

- a. Name, Adresse und Telefonnummer der gesuchstellenden Person,
- b. Begründung des Gesuchs,
- c. Art, Ort und Zeit des Ereignisses,
- d. Namen und Adressen der Beteiligten,
- e. bei Privatpersonen, die für sich selbst handeln, einen Identitätsnachweis,
- f. bei Anfragen für Dritte, einen Nachweis über die Einwilligung der betroffenen Person oder deren Vollmacht.

³ Die Akteneinsicht kann eingeschränkt oder verweigert werden, wenn

- a. in laufenden Verfahren der Untersuchungszweck gefährdet würde oder
- b. eine der Voraussetzungen gemäss § 23 Abs. 1 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 (IDG) erfüllt ist.

⁴ Gesuche werden von derjenigen Polizei bearbeitet, die für die entsprechenden Daten verantwortlich ist. Entspricht die Polizei dem Gesuch nicht, erlässt sie einen begründeten Entscheid.

⁵ Für die Bearbeitung der Gesuche kann eine Gebühr erhoben werden.

Auskunftsrecht

§ 15. ¹ Die Wahrnehmung des Auskunftsrechts gemäss § 20 Abs. 2 IDG erfolgt im gleichen Verfahren wie die Akteneinsicht. § 14 Abs. 5 dieser Verordnung ist nicht anwendbar.

² Gesuche enthalten die Angaben gemäss § 14 Abs. 2 lit. a, b und e oder f.

§ 16. ¹ Gesuche zur Wahrnehmung von anderen Rechten, insbesondere des Berichtigungsrechts gemäss § 21 IDG, sind schriftlich bei der verantwortlichen Polizei einzureichen. Berichtigung und andere Rechte

² Gesuche enthalten die Angaben gemäss § 14 Abs. 2 lit. a, b und e oder f.

§ 17. Die betroffene Person kann unter Vorlage des formell rechtskräftigen Entscheids die Nachführung von Datensystemen gemäss § 54 f PolG verlangen. Nachführung von Datensystemen

F. Aufbewahrung und Löschung der Daten

§ 18. ¹ Die Aufbewahrung und Löschung von Daten richten sich nach diesem Abschnitt, soweit sie nicht durch übergeordnetes Recht festgelegt sind. Allgemeines

² Die Aufbewahrungsfrist beginnt mit Erfassung der Daten im System.

³ Nach Ablauf der Aufbewahrungsfrist sind die betroffenen Daten zu löschen oder zu anonymisieren.

⁴ Vorbehalten bleiben die Bestimmungen über die Archivierung.

§ 19. Personalien werden gelöscht, wenn keine Verbindung zu Fall- und Ereignisdaten oder Journaldaten mehr besteht. Personalien

§ 20. ¹ Bei Fall- und Ereignisdaten mit Bezug zu Straftaten richtet sich die Aufbewahrungsfrist nach der Dauer der Verfolgungsverjährung der darin registrierten Straftat mit der längsten Verjährungsfrist. Fall- und Ereignisdaten

² Bei Fall- und Ereignisdaten ohne Bezug zu Straftaten gelten die folgenden Aufbewahrungsfristen:

- | | |
|--|-----------|
| a. aussergewöhnliche Todesfälle: | 30 Jahre, |
| b. Grossereignisse, Katastrophen: | 30 Jahre, |
| c. Ausweisverluste: | 15 Jahre, |
| d. fürsorgerische Unterbringungen: | 15 Jahre, |
| e. Berichte des Forensischen Instituts Zürich: | 15 Jahre, |
| f. aufzubewahrende Zuschriften: | 10 Jahre, |
| g. Einvernahmen: | 10 Jahre, |
| h. Gewaltschutzverfahren: | 10 Jahre, |
| i. Leumunds- und Bürgerrechtsberichte: | 10 Jahre, |
| j. Selbsttötungsversuche: | 10 Jahre, |
| k. Aufenthaltsnachforschungen: | 5 Jahre, |
| l. Entweichen und Entlaufen: | 5 Jahre, |

- m. Fundsachen: 5 Jahre,
- n. geklärte Vermisstenfälle: 5 Jahre,
ungeklärte Vermisstenfälle: 90 Jahre,
- o. Personen- und Fahrzeugkontrollberichte: 5 Jahre,
- p. übrige Berichte: 5 Jahre,
- q. andere Ereignisse: 5 Jahre.

³ Besteht zwischen verschiedenen Fall- und Ereignisdaten ein für die weitere Bearbeitung relevanter Sachzusammenhang, kann die verantwortliche Polizei die Aufbewahrungsfrist sämtlicher betroffener Fall- und Ereignisdaten an die zuletzt endende Aufbewahrungsfrist angleichen.

Journaldaten § 21. ¹ Bei Journaldaten mit Verbindung zu Fall- und Ereignisdaten richtet sich die Aufbewahrungsfrist nach der für die entsprechenden Fall- und Ereignisdaten geltenden Aufbewahrungsfrist.

² Bei Journaldaten ohne Verbindung zu Fall- und Ereignisdaten beträgt die Aufbewahrungsfrist 10 Jahre.

³ Besteht zwischen verschiedenen Journaldaten ein für die weitere Bearbeitung relevanter Sachzusammenhang, kann die verantwortliche Polizei die Aufbewahrungsfrist sämtlicher betroffener Journaldaten an die zuletzt endende Aufbewahrungsfrist angleichen.

Haftdaten § 22. Bei Haftdaten beträgt die Aufbewahrungsfrist 5 Jahre.

Gäste- § 23. Bei Gästekontrolldaten beträgt die Aufbewahrungsfrist
kontrolldaten 3 Jahre.

Grenz- § 24. Bei Grenzkontrolldaten beträgt die Aufbewahrungsfrist
kontrolldaten 5 Jahre.

Ausnahmen § 25. Die Polizei kann in Ausnahmefällen zur Wahrung wichtiger polizeilicher oder anderer öffentlicher Interessen die Aufbewahrungsfrist der Daten angemessen verlängern, längstens auf 50 Jahre nach deren Erfassung.

2. Abschnitt: Einsatz von Analysesystemen

Analyse- § 26. Die Polizei kann mit intelligenten Analysesystemen gemäss
systeme zum § 52 a Abs. 4 PolG nachträglich abgleichen:
Abgleich von
Bildern

- a. zur Identifikation einer Person: Bilder von Personen mit vorhandenen erkennungsdienstlichen Bildern,

- b. zur Erkennung von Tatzusammenhängen und Serien: Bilder von Personen mit Bildern von anderen Fällen,
- c. zur Identifikation einer dazugehörenden Person oder zur Erkennung von Tatzusammenhängen und Serien: Bilder von Gegenständen mit bereits vorhandenen Bildern von Gegenständen.

§ 27. ¹ Die eingesetzten Analysesysteme im Bereich der seriellen Kriminalität unterstützen die Polizei dabei, Deliktserien oder Tendenzen zu solchen Serien, wiederkehrende Muster sowie Wiederholungstäterinnen und -täter zu erkennen und in der Folge polizeiliche Massnahmen darauf abzustimmen.

Analyse-
systeme im
Bereich der
seriellen
Kriminalität

² In den Systemen können die Personalien und die Fall- und Ereignisdaten ausgetauscht werden, soweit diese Daten für die Analyse notwendig sind.

³ Zur Datenbearbeitung in den Analysesystemen sind ausschliesslich Mitarbeitende der Polizei mit spezialisierter Ausbildung in der Kriminalanalyse berechtigt. Die übrigen Mitarbeitenden der Polizei dürfen von den Analyseergebnissen Kenntnis nehmen.

3. Abschnitt: Polizei-Informationssystem POLIS

§ 28. Das POLIS besteht aus den folgenden Modulen:

Inhalt

- a. Rapportierungs- und Vorgangsbearbeitungssystem,
- b. Systeme zur mobilen Rapportierung,
- c. Forensisches Asservate Tracking System,
- d. System zur Archivierung und Recherche,
- e. System für die Gästekontrolle,
- f. Webportal für die Übermittlung von Formularen.

§ 29. ¹ Gesuche weiterer kommunaler Polizeien um Zugriff auf POLIS gemäss § 54 Abs. 4 PolG sind bei der Kantonspolizei einzureichen.

Zugriffs-
berechtigte

² Für den Umgang mit den in POLIS gespeicherten Daten unterstehen die weiteren kommunalen Polizeien und das Forensische Institut Zürich den gleichen Vorschriften wie die Betreiber.

³ Die Sicherheitsdirektion regelt für die einzelnen Benutzergruppen die Zugriffsrechte. Die Freigabe an die einzelnen Benutzerinnen und Benutzer erfolgt unter der Verantwortung der jeweiligen Datenverantwortlichen der beteiligten Polizeien.

Hauptverantwortung

§ 30. Die Hauptverantwortung für Daten in POLIS liegt bei der oder dem Datenverantwortlichen der Kantonspolizei. Sie oder er koordiniert die Tätigkeiten der Datenverantwortlichen gemäss § 10.

Protokollierung von Benutzerzugriffen

§ 31. ¹ Zugriffe in POLIS werden protokolliert. Die Protokolle sind während mindestens eines Jahres zugriffs- und schreibgeschützt aufzubewahren.

² Die Datenverantwortlichen können zur Verhinderung von Missbrauch von in POLIS gespeicherten Daten Kontrollen oder Auswertungen von Benutzerzugriffen anordnen.

Bekanntgabe von Daten im Abrufverfahren
a. zulässige Attribute

§ 32. Die Polizei kann gemäss § 54 b PolG folgende Daten im Abrufverfahren bekannt geben:

- a. alle Attribute aus den Personalien gemäss § 4 Abs. 2,
- b. aus den Attributen der Fall- und Ereignisdaten gemäss § 5 Abs. 2:
 1. allgemein: Ereignis, Ereigniszusatz, Ereigniszeit, Ereignisort einschliesslich Koordinaten, Tatbestand, Verfahrensrollen, Aktenart, Aktennummer, Deliktsumme, Schadenssumme, Tatvorgehen, Warnungen,
 2. zu Sachen: Erfassungsgrund, Massnahmehinweis, zu erhebende Information, Sachbezeichnung, Kategorie, Anzahl, Serie, Grösse, Marke, Modell, Typ, Staat, Kanton, Identifikationsnummer, Sachwert, Detailangaben, Gravuren, Massangaben, Stein, Bilder,
 3. zu digitalen Tatmitteln: Kategorie, Wert, Typ,
 4. zu Fahrzeugen und Kontrollschildern: Erfassungsgrund, Massnahmehinweis, zu erhebende Information, Fahrzeugart, Kategorie, Karosserieform, Marke, Modell, Typ, Farbe, Fahrzeugidentifikationsnummer, Stammnummer, Motorennummer, Typengenehmigung, Kennzeichen, Staat, Kennzeichenart, Kennzeichenfarbe, Position, Detailangaben, Sachfahndungsnummer,
 5. zu Revokationen: Revokationsdatum, Revokationsgrund, Ermittlungsdatum, Ermittlungsort,
 6. administrative Angaben: Sachbearbeiterin oder Sachbearbeiter, Dienststelle, Kanton, Fallnummer, Ereignisnummer, Fallstatus, Aktualisierungen, Löschdatum,
- c. alle Attribute aus den Haftdaten gemäss § 7 Abs. 2 lit. a–c, e und f.

§ 33. ¹ Auf die Protokollierung der Abfragen ist § 31 sinngemäss anwendbar. b. Protokollierung von Abfragen

² Zusätzlich werden bei Abfragen im Abrufverfahren folgende Daten protokolliert:

- a. Organisation und Benutzeridentifikation,
- b. Kontext der Abfrage,
- c. Auftraggeberin oder Auftraggeber.

§ 34. Die Herausgabe der Protokolldaten an andere als die zuständigen eidgenössischen oder kantonalen Aufsichtsbehörden erfolgt anonymisiert mit dem Hinweis auf die Organisationszugehörigkeit der abfragenden Person. c. Herausgabe von Protokolldaten

§ 35. ¹ Die Betreiber tragen die Anschaffungs- und Betriebskosten der erforderlichen Hard- und Software. Kostentragung

² Sie tragen die Kosten für die Weiterentwicklung nach vereinbartem Kostenschlüssel.

³ Die weiteren beteiligten Polizeien entrichten für ihre Beteiligung eine Entschädigung. Diese wird in einer Vereinbarung mit den Betreibern festgesetzt.

4. Abschnitt: Übergangsbestimmung

§ 36. Für Erfassungen vor Inkrafttreten dieser Verordnung bleiben die Aufbewahrungsfristen gemäss § 18 der Verordnung über das Polizei-Informationssystem POLIS vom 13. Juli 2005 anwendbar. Aufbewahrungsfristen

Waffenverordnung (WafVO)

(Änderung vom 23. September 2026)

Der Regierungsrat beschliesst:

Die Waffenverordnung vom 16. Dezember 1998 wird wie folgt geändert:

Elektronisches
Informations-
system

§ 10. ¹ Die Kantonspolizei führt das elektronische Informationssystem über den Erwerb und den Besitz von Feuerwaffen gemäss Art. 32 a Abs. 2 des Waffengesetzes. Dieses dient als Teil des interkantonalen harmonisierten Informationssystems gemäss Art. 32 a Abs. 3 des Waffengesetzes. Die Kantonspolizei registriert die im Kanton erteilten Bewilligungen im Bereich des Waffenrechts. Die Statthalterämter stellen der Kantonspolizei laufend Kopien der von ihnen erteilten Bewilligungen zu.

Abs. 2 und 3 unverändert.

Bericht

A. Ausgangslage

Am 13. Juli 2005 erliess der Regierungsrat die Verordnung über das Polizei-Informationssystem POLIS (POLIS-Verordnung [LS 551.103]). Diese regelt die Details eines einzelnen, genau bezeichneten Systems. Die Technologieentwicklung im Informatikbereich ist indessen rasant. Entsprechend müssen polizeiliche Systeme laufend weiterentwickelt oder ersetzt werden.

Zudem hat der Kantonsrat mit der Änderung vom 30. März 2026 des Polizeigesetzes vom 23. April 2007 (PolG, LS 550.1; ABI 2026-04-10) die Grundzüge der polizeilichen Datenbearbeitung neu geregelt. Mit der Ausführung der Details betraute er an verschiedenen Stellen den Regierungsrat.

B. Ziele und Umsetzung

Mit der vorliegenden Verordnung werden die verlangten Detailregelungen erlassen und gleichzeitig die bestehende POLIS-Verordnung ersetzt. Zudem trägt sie der bundesgerichtlichen Rechtsprechung Rechnung, indem sie gewisse Gesetzesbestimmungen konkretisiert. Im Zentrum stehen die Bezeichnung der bearbeiteten Daten, die Detailregelungen über deren Schutz, Sicherheit, Bekanntgabe und Löschung sowie die neuen Vorschriften über den Einsatz von Analysesystemen und die elektronische Zusammenarbeit mit anderen Behörden.

Die rechtlichen Grundlagen polizeilicher Datenbearbeitung sollen aufgrund der erwähnten rasanten Entwicklung der Technik grundsätzlich systemunabhängig ausgestaltet sein, gilt es doch, die Schranken unabhängig von der verwendeten Technologie festzulegen. Die Einhaltung des vorgeschriebenen Grundrechtsschutzes durch neue oder weiterentwickelte Systeme ist mittels Datenschutz-Folgenabschätzung und Vorabkontrolle sicherzustellen (vgl. § 10 Gesetz über die Information und den Datenschutz vom 12. Februar 2007 [IDG, LS 170.4]). Die Regelung einzelner, bezeichneter Systeme je in einer eigenen Verordnung, wie dies bisher mit der POLIS-Verordnung der Fall war, würde die Gefahren von Lücken, Überschneidungen und laufender Anpassungsbedürftigkeit bergen. In der vorliegenden Verordnung werden daher zuerst allgemein und systemunabhängig die Vorgaben für die gesamte polizeiliche Datenbearbeitung festgelegt. Um der besonders hohen Sensibilität der im Polizei-Informationssystem POLIS bearbeiteten Daten Rechnung zu

tragen, werden die für dieses System spezifischen Vorschriften im 3. Abschnitt geregelt. Aufgrund der zum jetzigen Zeitpunkt nicht abschätzbaren konkreten Ausgestaltung des neuen Polizeiinformationssystems bezieht sich die vorliegende Verordnung auf das bestehende Polizei-Informationssystem POLIS. Auf eine spezifische Regelung weiterer Systeme wird verzichtet. Diese richten sich nach den allgemeinen Bestimmungen dieser Verordnung.

C. Ergebnis der Vernehmlassung

Mit Schreiben vom 29. Mai 2026 eröffnete die Sicherheitsdirektion die Vernehmlassung zur vorliegenden Verordnung über die polizeiliche Datenbearbeitung und lud den Verband der Gemeindepräsidenten des Kantons Zürich, die Städte Zürich und Winterthur sowie die Datenschutzbeauftragte zur Stellungnahme ein.

Der Verband der Gemeindepräsidenten begrüsst den Inhalt der Verordnung und beantragte lediglich eine dahingehende Ergänzung von § 11, dass der Datenzugriff eine wirksame und zeitnahe Aufgabenerfüllung gewährleiste, was jedoch bereits im Rahmen von § 11 ermöglicht wird.

Die Stadt Zürich regte Korrekturen oder Präzisierungen zu einzelnen Bestimmungen an, die mehrheitlich entweder übernommen oder auf die an der betreffenden Stelle in den Erläuterungen eingegangen wird (vgl. Erläuterungen zu §§ 4 f., 7, 14 f., 20, 26 und 33). Auf eine umfassende Regulierung der Gästekontrolldaten wurde verzichtet.

Die Stadt Winterthur verzichtete auf eine Stellungnahme.

Dem Anliegen der Datenschutzbeauftragten, verschiedene Präzisierungen vorzunehmen, wurde entsprochen.

D. Erläuterungen zu den einzelnen Bestimmungen

1. Abschnitt: Allgemeine Bestimmungen

A. Gegenstand und Zweck

§ 1. Gegenstand

Die Verordnung regelt jegliche polizeiliche Bearbeitung von Daten, die den in § 2 genannten Zwecken dienen. Die Datenbearbeitung betrifft jeden Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten (§ 3 Abs. 5 IDG). Auch der Begriff Informationssysteme ist weit zu fassen und um-

fasst jedes System, in dem Daten bearbeitet werden (vgl. auch § 54a Abs. 2 und § 54b Abs. 1 PolG). Mit Polizei sind in der vorliegenden Verordnung alle Polizeibehörden im Sinne von §§ 2, 2a und 3 des Polizeiorganisationsgesetzes vom 29. November 2004 (POG, LS 551.1) gemeint.

§ 2. Zweck der polizeilichen Datenbearbeitung

Die Bestimmung konkretisiert § 52 Abs. 1 PolG, der generell die Datenbearbeitung zur Erfüllung der Aufgaben der Polizei erlaubt. Sie entspricht weitgehend § 4 der POLIS-Verordnung, der sich jedoch nur auf das System POLIS bezog, und ergänzt diesen insofern, als nun der Zweck für die gesamte polizeiliche Datenbearbeitung beschrieben wird.

Lit. b erwähnt zusätzlich zu § 4 lit. c der POLIS-Verordnung Untersuchungen, die anhand von wissenschaftlichen Abklärungen und Auswertungen den Sachverhalt feststellen.

Lit. d ergänzt § 4 lit. e der POLIS-Verordnung insofern, als die Datenbearbeitung nicht nur der Recherche, sondern auch der Analyse der Daten dient, wobei §§ 52a und 52b PolG als formell-gesetzliche Grundlage dienen.

Lit. e ergibt sich aus § 54 Abs. 2 PolG.

Lit. f verzichtet im Gegensatz zu § 4 lit. g–j der POLIS-Verordnung auf die Nennung der Behörden, da der Daten- und Informationsaustausch unabhängig von der Bezeichnung in diesem Paragraphen eine formell-gesetzliche Grundlage voraussetzt. Diese ergibt sich aus §§ 54a–54c und 54e PolG.

Lit. h stellt klar, dass die Polizei Daten auch für das Planen und Führen von Einsätzen bearbeiten darf. Dies dient der Entgegennahme von Notrufen, der Lageerfassung, der Disposition von Einsatzkräften, der Informationsweitergabe sowie der Einsatzdokumentation.

Lit. k nennt das Führen von Geschäftskontrollen, was § 52 Abs. 1 PolG bereits vorsieht. Eine solche umfasst die gesamte organisatorische und administrative Dokumentation. Sie dient zudem der Kontrolle über die Einhaltung der Fristen und gesetzlichen Richtlinien. Lit. a, c, g, i und j entsprechen § 4 lit. b, d, f, m und k der POLIS-Verordnung.

B. Bearbeitete Daten

§ 3. Datentypen

Die bisherige Regelung in § 5 der POLIS-Verordnung bezog sich nur auf das System POLIS und regelte die dazugehörigen Datenbanken. Eine systemunabhängige Regelung erfordert die Beschreibung von Datentypen, die losgelöst von der Bezeichnung bestimmter Systeme bearbeitet werden können.

Sämtliche von der Polizei bearbeiteten Daten (mit Ausnahme solcher über administrative Tätigkeiten, wie Personal- und Finanzverwaltung, Gebäude- und Materialbewirtschaftung, die sich auf allgemeine verwaltungsrechtliche Regelungen stützen) lassen sich in die in §§ 4–9 ausgeführten Datentypen einordnen, wobei die Haftdaten, die Gästekontrolldaten und die Grenzkontrolldaten separat geführt werden. Diese Datentypen unterscheiden sich von den übrigen insofern, als sie zu spezifisch geregelten Zwecken erhoben werden. Sie sind daher abge sondert zu halten. Die übrigen Datentypen können in sich und miteinander verbunden werden.

§ 4. Personalien

Die Regelung entspricht grundsätzlich § 7 der POLIS-Verordnung. Änderungen gegenüber jener Bestimmung sind wie folgt begründet:

Abs. 1: Es gilt zu präzisieren, dass mit Personen nicht nur natürliche, sondern auch juristische Personen oder ähnliche Gebilde wie formlose Zusammenschlüsse gemeint sind. Ob Daten über Personen oder Personengesamtheiten bearbeitet werden dürfen, soll nicht von deren Rechtsform abhängen.

Abs. 2: Die Kann-Formulierung impliziert, dass jeweils nur die für die polizeiliche Aufgabenerfüllung notwendigen Personalien zu erheben sind.

Auf das Attribut Spitzname gemäss § 7 Abs. 1 lit. a der POLIS-Verordnung ist zu verzichten, da es als Unterkategorie der ebenfalls angeführten Genannt(vor)namen in § 4 Abs. 2 lit. a zu verstehen ist. Die Begriffe Geburtsname, Sterbeort/Sterbedatum und Nationalität werden in Übereinstimmung mit der Terminologie bestehender Rechtserlasse in Ledigname, Todesort/Todesdatum bzw. Staatsangehörigkeit geändert und Vorname, Rufname, Genanntname, Genanntvorname und Aliasname in den Plural gesetzt, da Personen zum Teil mehrere dieser Namen haben können. Sodann ist zu präzisieren, dass mit dem Begriff Geschlecht nicht das biologische, sondern das aus den Ausweisen ersichtliche, behördlich verkündete Geschlecht gemäss Art. 8 Bst. b (und Art. 7 Abs. 2 Bst. o) der Zivilstandsverordnung vom 28. April 2004 (SR 211.112.2) gemeint ist.

Teilweise sind die übrigen Attribute gemäss § 7 der POLIS-Verordnung mit verwandten Begriffen zu ergänzen, um Unklarheiten über den Anwendungsbereich zu beseitigen: Lit. h stellt klar, dass nicht nur der Beruf, sondern auch eine regelmässige Beschäftigung registriert werden kann, wenn sie den Charakter eines Berufes aufweist. Lit. j präzisiert, dass nicht nur der Wohnsitz (Adresse und Niederlassungsgemeinde im Sinne von §§ 1 lit. a und 3 Abs 1 lit. a Gesetz über das Meldewesen und die Einwohnerregister vom 11. Mai 2015 [LS 142.1] sowie Art. 3 Bst. b Bundesgesetz vom 23. Juni 2006 über die Harmonisierung der

Einwohnerregister und anderer amtlicher Personenregister [SR 431.02]), sondern bei dessen Fehlen auch der Aufenthaltsort bzw. bei juristischen Personen der Sitz vermerkt werden kann. Lit. l verdeutlicht, dass nicht nur Ehegatten und (faktische) Lebenspartner, sondern auch eingetragene Partner registriert werden dürfen (obschon die Gründung von eingetragenen Partnerschaften seit 2022 in der Schweiz nicht mehr möglich ist, bestehen noch viele davon). Lit. m stellt klar, dass nicht nur die Konfession als Unterkategorie einer Religion, sondern auch die Religion selbst festgehalten werden darf. Lit. n ergänzt, dass neben der Vormundin oder dem Vormund bzw. der Beiständin oder dem Beistand auch die (vertragliche oder gesetzliche) Vertreterin oder der (vertragliche oder gesetzliche) Vertreter bzw. bei juristischen Personen die Organe registriert werden dürfen. Lit. p, t und u lassen die Registrierung von Personenbeschreibungen und erkennungsdienstlichen Daten, von Hinweisen zur Person und zu deren Verbindungen zu und führen damit die Attribute von § 7 Abs. 1 lit. r und u der POLIS-Verordnung geordneter aus. Lit. q präzisiert, dass mit den Angaben zu Informations- und Kommunikationsmitteln (in § 7 Abs. 1 lit. s POLIS-Verordnung noch einzelne Mittel aufgezählt) auch Registrierungs- und Zugangsdaten wie E-Mail-Adressen, IP-Adressen und Passwörter für Accounts erfasst werden können.

Schliesslich besteht auch das Bedürfnis, einzelne Attribute auszuweiten, um eine einwandfreie Zuordnung der Falldaten zu einer bestimmten Person zu gewährleisten oder wichtige Zusammenhänge zu registrieren: Lit. d lässt neben dem Datum (vgl. § 7 Abs. 1 lit. v POLIS-Verordnung) neu auch Angaben über den Ort des Versterbens einer Person zu. Lit. h erlaubt zusätzlich zum Vermerk des Arbeitsortes auch denjenigen des Arbeitgebers. Lit. k lässt nicht nur die Angabe der Anzahl Kinder, sondern auch von deren Personalien zu. Während bislang unter Ausweispapieren (vgl. § 7 Abs. 1 lit. q POLIS-Verordnung) sämtliche Angaben zum Aufenthalt von Ausländern vermerkt werden mussten, werden nun in § 4 Abs. 2 lit. o die Angaben zum Aufenthaltsstatus, Aufenthaltsdaten, Reisedokumente und Daten im Zusammenhang mit Grenzübertritten festgehalten. Diese Angaben sind neben den Grenzkontrolldaten gemäss § 9 auch bei Personenkontrollen im Inland und in Strafverfahren im Kontext des Bundesgesetzes vom 16. Dezember 2005 über die Ausländerinnen und Ausländer und über die Integration (AIG, SR 142.20) wichtig. Ebenso sind die gemäss lit. s aufgeführten Hinweise zu Verfahren und Massnahmen für Personenkontrollen oder auch zur Abwehr von Gefahren, die von einer Person ausgehen, für die involvierten Polizeikräfte relevant, um Sicherheitsvorkehrungen zu treffen oder die Einhaltung bereits verfügbarer Auflagen zu kontrollieren. Lit. v erlaubt sodann die Erfassung des Modus Operandi bei Täterinnen und Tätern und kann somit Anhaltspunkte für die Aufklärung von Delik-

ten mit ähnlicher Vorgehensweise liefern. Die Erfassung von Effekten und mitgeführten Gegenständen gemäss lit. w, die einer Person bei der Verhaftung abgenommen werden, dienen z.B. der Erstellung eines Inventars, um bei der Entlassung eine vollständige Rückgabe zu gewährleisten. Die Dokumentation mitgeführter Gegenstände kann aber auch für den Beweis des beabsichtigten oder bereits verübten Handelns der Person wichtig sein, z.B. wenn sie klassisches Einbruchswerkzeug wie Brecheisen oder Glasschneider oder im Umfeld einer eskalierten Demonstration Farbspraydosen, Masken usw. mit sich führt. Die Registrierung der AHV-Nummer gemäss lit. x dient der eindeutigen Bestimmbarkeit der erfassten Person. Art. 153b ff. des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (SR 831.10) schafft die ausdrückliche gesetzliche Grundlage für die Verwendung der AHV-Nummer als Personenidentifikator. Die in § 7 Abs. 1 lit. t der POLIS-Verordnung genannte Personen-Nummer und der Personencode sind POLIS-spezifische Angaben und werden daher nicht mehr genannt.

§ 5. Fall- und Ereignisdaten

Diese Daten umfassen die Gesamtheit aller möglichen Angaben, die für die Polizei neben den Datentypen gemäss §§ 4 und 6 ff. bei der Bearbeitung von Fällen und Ereignissen notwendig sind. In der Aufzählung in § 5 wird umschrieben, welche Art von Angaben als Fall- oder Ereignisdaten erfasst werden. Mit dem vorliegenden Sachverhalt gemäss § 5 Abs. 2 lit. d ist der Sachverhalt gemeint, wie er sich zur Zeit der Aufnahme präsentiert.

§ 6. Journaldaten

Bislang wurde das Journal unter § 5 lit. a der POLIS-Verordnung als Bestandteil von POLIS aufgeführt und ist nun als Datentyp systemunabhängig beschrieben. Mit der erneuten Nennung der Ereignisse, der beteiligten Personen und der Art der Beteiligung in Abs. 2 lit. a und b soll klargestellt werden, dass auch in Journalen die Personen und ihre Beteiligungsart erfasst werden und dass nicht nur dann polizeiliche Tätigkeiten dokumentiert werden, wenn sie durch Meldungen oder Anzeigen ausgelöst wurden, sondern auch, wenn sie durch ein von der Polizei selbst wahrgenommenes Ereignis in Gang gesetzt werden. Abs. 2 lit. d nennt die Registrierung der Standortdaten von Personen, die einen Notruf tätigen, um sie in einer Notlage rasch orten zu können, was für die Rechtzeitigkeit der angeforderten Hilfe entscheidend sein kann.

§ 7. Haftdaten

Die Kantonspolizei hat im Rahmen von § 14 Abs. 2 POG den Justizvollzug beim Betrieb der Polizeigefängnisse zu unterstützen (vgl. §§ 6 lit. b und 136a ff. Justizvollzugsverordnung vom 6. Dezember 2006 [LS 331.1]). Entsprechend muss sie hierfür die notwendigen Daten er-

fassen. § 7 regelt, welche Daten in diesem Zusammenhang erfasst und bearbeitet werden dürfen. Zu den Angaben zur Person gemäss Abs. 2 lit. a gehören die im Haftkontext relevanten Personalien (einschliesslich gesetzlicher Vertretung) sowie die Hafterstehungsfähigkeit und haftrelevante Hinweise zu Schwangerschaften, Krankheiten, Behinderungen usw. Zur Registrierung der Planung und Dokumentation der Vollzugsanordnungen und -handlungen gemäss Abs. 2 lit. d gehören z. B. Angaben zu Ort und Zeit von Hafteninvernahmen und Massnahmen zur Verhinderung von Kollusionshandlungen. Unter Abs. 2 lit. h können administrative Hinweise wie solche zur Durchführung der Haft und allfälliger Transporte, zu getroffenen Anordnungen im Zusammenhang mit einer Krankheit oder mit einer Schwangerschaft vermerkt werden.

§ 8. Gästekontrolldaten

§ 8 entspricht § 7b der POLIS-Verordnung und stützt sich auf § 21 Abs. 4 und 5 PolG. Der Begriff Nationalität ist an die Terminologie bestehender Erlasse anzupassen und daher in Staatsangehörigkeit umzuwandeln (vgl. Erläuterungen zu § 4 Abs. 2).

§ 9. Grenzkontrolldaten

Die Personenkontrolle an der Schengen-Aussengrenze ist grundsätzlich Aufgabe der Kantone (Art. 9 Abs. 1 AIG, Art. 31 Abs. 2 Verordnung vom 15. August 2018 über die Einreise und die Visumerteilung [VEV, SR 142.204]). Mit dem Flughafen Zürich liegt die grösste Schengen-Aussengrenze der Schweiz im Kanton Zürich. Die Grenzkontrolle wird dort und bei den seltenen Grenzübertritten über andere Flugplätze im Kanton von der Kantonspolizei wahrgenommen. Sie hat sich dabei an die Vorgaben des Schengener Grenzkodex zu halten (Art. 7 Abs. 1 und 2 AIG, Art. 28 VEV). Das umfasst insbesondere auch das Verfahren zur Wegweisung an der Grenze (Art. 64 Abs. 1 Bst. b und Art. 65 AIG). Mit dem Vermerk des Erfassungsgrundes gemäss Abs. 2 lit. a wird festgehalten, was Anlass zur Bearbeitung des Grenzübertritts bot. Bei den Flugpassagierdaten gemäss Abs. 2 lit. e handelt es sich um die Buchungsdaten der Fluggesellschaften über die Passagiere. Die für den Aufenthalt notwendigen finanziellen Mittel gemäss Abs. 2 lit. h sind eine Einreisevoraussetzung für Drittstaatsangehörige (vgl. Art. 6 Abs. 1 Bst. c Schengener Grenzkodex).

C. Verantwortung und Datenzugriff

§ 10. Verantwortung

Für die Datenaufbewahrung und -pflege ist jeweils diejenige Polizei verantwortlich, welche die Daten bearbeitet oder bearbeiten lässt (vgl. § 10 Abs. 1). Zwar trägt die Kantonspolizei gemäss § 54 Abs. 5 PolG die Hauptverantwortung über den Daten- und Informationsbestand im gemein-

samen Polizei-Informationssystem POLIS. Bei den einzelnen Bearbeitungen trägt aber auch hier jede Polizeibehörde die Verantwortung für ihr eigenes Handeln (vgl. auch § 27 Verordnung über die Information und den Datenschutz vom 28. Mai 2008 [LS 170.41]). Bei Systemen anderer Polizeibehörden, wie Systeme des Forensischen Instituts Zürich oder der Stadtpolizeien, bei denen die Kantonspolizei nicht involviert ist, kann sie auch nicht die Hauptverantwortung übernehmen. Bei der Bearbeitung eines gemeinsamen Informationsbestandes durch mehrere Polizeibehörden ist eine Regelung über die Verantwortlichkeiten zu treffen (vgl. § 5 Abs. 1 IDG).

Abs. 2 und 3 entsprechen weitgehend § 14 Abs. 2 der POLIS-Verordnung. Die noch in § 14 Abs. 3 der POLIS-Verordnung geregelte datenschutzrechtliche Aufsicht obliegt gemäss § 34 lit. c IDG der oder dem Datenschutzbeauftragten.

Im Übrigen trifft die Polizei angemessene organisatorische und technische Massnahmen zum Schutz ihrer Informationssysteme (vgl. § 7 IDG).

§ 11. Datenzugriff

Die Bestimmung ergänzt § 52 Abs. 3 PolG insofern, als der Zugriff auf Daten nicht nur für die Polizeibehörden als Ganzes, sondern innerhalb der Polizeibehörden auch für deren Benutzerinnen und Benutzer nur für das für die Erfüllung der jeweiligen Aufgabe Notwendige erlaubt ist. § 11 Abs. 1 entspricht § 15 Abs. 1 der POLIS-Verordnung.

Da in der Regel Mitarbeitende gleicher Dienststellen die gleichen Zugriffsrechte benötigen, werden durch die Polizei Benutzergruppen gebildet. Die Freigabe an die einzelnen Benutzenden erfolgt unter der Verantwortung der jeweiligen Datenverantwortlichen der Polizei. Das erlaubt es, bei heiklen Fallbearbeitungen, z.B. Ermittlungsverfahren mit Gefährdungspotenzial, die Zugriffsrechte auf einen kleinen Benutzerkreis zu beschränken.

D. Schnittstellen und Datenübermittlung

§ 12. Schnittstellen zwischen eigenen Systemen

§ 54a Abs. 2 PolG erlaubt der Polizei die Schaffung von Schnittstellen zwischen ihren Systemen und denjenigen des Bundes, der anderen Kantone und der Gemeinden. § 54d lit. a PolG beauftragt den Regierungsrat mit der Regelung. Vorliegend wird klargestellt, dass beim Einbau von Schnittstellen unter den eigenen Systemen stets sichergestellt werden muss, dass Personen, die auf ein System Zugriff haben, nicht mittels der Schnittstelle an Daten eines anderen Systems gelangen, für die sie keine Berechtigung haben.

§ 13. Übermittlung in polizeiliche Informationssysteme des Bundes

Die Leistung von Amts- und Rechtshilfe gegenüber dem Bund ist in § 52 Abs. 4 PolG geregelt und berechtigt zur Übermittlung von Daten in polizeiliche Informationssysteme des Bundes. Das Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes (BPI, SR 361) führt in Art. 2 die vom Bund betriebenen Systeme auf und hält in den nachfolgenden Bestimmungen, die jedes einzelne System regeln (Art. 9 ff. BPI), detailliert fest, welche Daten in welchem System und von welchen Behörden bearbeitet werden dürfen. Darüber hinaus verlangt das BPI für gewisse Systeme eine kantonale Rechtsgrundlage zur Übermittlung von Daten an Bundessysteme (vgl. z. B. Art. 13 BPI), die hiermit vorliegt. Eine Übermittlung der Daten ist jedoch nur zulässig, soweit diese erforderlich ist.

E. Rechte von Betroffenen und Dritten

§ 14. Akteneinsicht

Diese Bestimmung betrifft Gesuche, die nicht im Rahmen der Amts- und Rechtshilfe zu erledigen sind. Da § 52 Abs. 4 PolG die Leistung von Amts- und Rechtshilfe der Polizei gegenüber anderen öffentlichen Organen sowie den Organen anderer Kantone oder des Bundes und Dritten unter den Voraussetzungen des IDG regelt, braucht es keine Aufzählung einzelner Behörden wie in § 10 der POLIS-Verordnung. § 10 der POLIS-Verordnung schreibt im Übrigen Selbstverständlichkeiten vor, weshalb auf eine Übernahme in die vorliegende Verordnung verzichtet wird. § 14 entspricht § 11 der POLIS-Verordnung. Der Begriff Akteneinsicht weicht von der Terminologie des IDG ab, wo § 20 IDG allgemeiner den Zugang zu Informationen regelt. Da es bei polizeilichen Daten meist um solche aus Ermittlungen geht, entspricht der Begriff Akteneinsicht vorliegend demjenigen in Art. 101 f. der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (StPO, SR 312.0).

§ 15. Auskunftsrecht und § 16. Berichtigung und andere Rechte

Die Bestimmungen entsprechen §§ 12 und 13 der POLIS-Verordnung. Der Begriff Auskunftsrecht stimmt mit demjenigen von § 20 Abs. 2 IDG bzw. § 43 f. des totalrevidierten Gesetzes über die Information und den Datenschutz vom 23. März 2026 (nIDG, ABI 2026-04-02, noch nicht in Kraft) überein. Gemäss IDG und nIDG ist die Auskunft kostenlos, weshalb § 12 Abs. 2–4 der POLIS-Verordnung nicht übernommen wurde. Gemäss §§ 12 Abs. 1 und 13 Abs. 2 der POLIS-Verordnung müssen bei Gesuchen nur die Angaben gemäss § 11 Abs. 2 lit. a und e oder f derselben Verordnung gemacht und gegebenenfalls ein schützenswertes Interesse nachgewiesen werden. Dies verursachte in der Praxis Abgren-

zungsprobleme, da oft nicht ersichtlich war, in welchem Kontext die Gesuche standen (Auskunftsrecht oder andere Rechte wie das Berichtigungsrecht), weshalb nun auch eine Begründung des Ersuchens erfolgen soll (vgl. §§ 15 Abs. 2 und 16 Abs. 2). Auf den Nachweis eines schutzwürdigen Interesses ist zu verzichten, da dies nicht den Vorgaben des nIDG entspricht.

§ 17. Nachführung von Datensystemen

Die Bestimmung entspricht inhaltlich § 13 Abs. 3 der POLIS-Verordnung.

F. Aufbewahrung und Löschung der Daten

§ 18. Allgemeines

In Bezug auf die Aufbewahrung und Löschung von Daten bestehen teilweise übergeordnete Vorschriften wie in Art. 103 und 276 StPO oder § 53 PolG. Die vom Regierungsrat zu erlassenden Bestimmungen gelten daher insoweit, als keine übergeordneten Vorschriften bestehen (vgl. § 54 Abs. 7 PolG).

Art. 99 Abs. 2 in Verbindung mit Art. 103 Abs. 1 StPO schreibt vor, dass Akten im Zusammenhang mit Strafermittlungen mindestens bis zum Ablauf der Verfolgungs- und Vollstreckungsverjährung aufzubewahren sind. Die Verfolgungsverjährung beginnt im Zeitpunkt der Begehung des Delikts oder, wenn das strafbare Verhalten andauert, mit dem Tag, an dem es aufhört (Art. 98 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 [StGB, SR 311.0]). Dieser Zeitpunkt ist bei der Erfassung jedoch oft noch nicht bekannt und ergibt sich allenfalls erst aus späteren Ermittlungen oder gar erst mit Eintritt der Rechtskraft einer Verurteilung. Die Festlegung der automatischen Löschung von Daten erfolgt aber bei deren Erfassung im System. Der Begehungszeitpunkt eignet sich daher nicht für die Auslösung des Fristenlaufs. Es ist stattdessen einheitlich auf den Zeitpunkt der Erfassung des Vorfalls abzustellen. Da dieser logischerweise immer nach der Begehung des registrierten Delikts liegt und die Aufbewahrungsdauer derjenigen der Verfolgungsverjährung entspricht, ist gewährleistet, dass das Ereignis entsprechend der Vorgabe von Art. 103 Abs. 1 StPO mindestens bis zu deren Eintritt registriert bleibt.

Der Beginn der Aufbewahrungsfrist richtet sich entgegen § 5 Abs. 2 und 3 IDG (§ 9 nIDG) nicht nach dem Zeitpunkt, ab dem das öffentliche Organ die Informationen für sein Verwaltungshandeln nicht mehr benötigt. Wie aus § 9 Abs. 1 nIDG hervorgeht, sind besondere Regelungen zulässig; die betreffende Bestimmung im IDG soll lediglich als Auffangtatbestand dienen. § 54 Abs. 7 PolG sieht eine solche Regelung vor. Das Abstellen auf den genannten Zeitpunkt gemäss IDG ist bei polizeilichen Daten nicht sinnvoll, werden diese doch unter anderem gerade

im Hinblick auf künftige, mit den betroffenen Personen in Zusammenhang stehende Ereignisse oder Kontrollen registriert, sodass es keinen bestimmbaren Zeitpunkt gibt, ab dem sie nicht mehr benötigt werden.

Wird die Täterin oder der Täter verurteilt, fordert Art. 103 Abs. 1 StPO überdies die weitere Aufbewahrung der Akten bis zum Eintritt der Vollstreckungsverjährung. Gemeint sind die Verfahrensakten, die zur Verurteilung geführt haben. Die Daten in den polizeilichen Informationssystemen gehören grundsätzlich nicht dazu, soweit sie nicht an die Justizbehörden übermittelt und in jenen Akten abgelegt wurden. Eine Aufbewahrung während der Dauer der Vollstreckungsverjährung würde daher wenig Sinn machen. Die Polizei ist in den betreffenden Verfahren vor der Justiz in der Regel nicht beteiligt und erfährt entsprechend nicht, wann die Verjährung der betreffenden Verurteilungen eintritt. Die Daten sind daher wie ausgeführt nach der Dauer der Verfolgungsverjährungsfrist seit der Registrierung zu löschen.

§ 11 Abs. 2 IDG bzw. § 30 Abs. 2 nIDG schreibt den öffentlichen Organen vor, Personendaten zu löschen oder zu anonymisieren, sobald und soweit es der Bearbeitungszweck erlaubt. Daten sind nach Ablauf der Aufbewahrungsfrist dem zuständigen Archiv anzubieten (§ 5 Abs. 3 IDG bzw. § 9 Abs. 2 nIDG). Sie sind somit nach dem Ablauf der Frist zwar zu erhalten, aber die Mitarbeitenden können nicht mehr darauf zugreifen. Vernichtet werden dürfen sie erst, wenn sie nicht zu archivieren sind (vgl. § 8 Archivgesetz vom 24. September 1995 [LS 170.6]). Daten werden dann anonymisiert, wenn sie zu Schulungszwecken, Forschungszwecken oder statistischen Zwecken weiter aufbewahrt werden.

§ 19. Personalien

Personalien müssen genau so lange abrufbar bleiben, wie sie mit darin registrierten Fällen verknüpft sind. Sobald alle diese Fälle gelöscht sind, dürfen auch die Personalien nicht mehr abrufbar sein.

§ 20. Fall- und Ereignisdaten

Die Dauer der Aufbewahrung von Daten über strafbare Vorfälle richtet sich nach derjenigen der längsten Verjährungsfrist der im betreffenden Fall registrierten Straftaten (vgl. Art. 97, 101 und 109 StGB). Der Beginn der Frist für die Aufbewahrung der Daten richtet sich indessen nicht nach dem Zeitpunkt der Begehung der Delikte (vgl. Art. 98 StGB), sondern nach dem Tag der Erfassung (vgl. Erläuterungen zu § 18).

Soweit das Gesetz keine Aufbewahrungsfristen vorschreibt, beauftragt es in § 54 Abs. 7 PolG den Ordnungsgeber mit deren Festlegung. Dieser ist seiner Aufgabe bisher in § 18 Abs. 5 der POLIS-Verordnung nachgekommen. Die dort noch nicht geregelten Aufbewahrungsfristen werden daher in § 20 Abs. 2 nach Ermessen festgelegt. Massgebend ist die Dauer, während der damit zu rechnen ist, dass die betreffenden Daten nach dem Ereignis abrufbar sein müssen.

In lit. n wird für die Aufbewahrung von Daten betreffend Vermisstenfällen zwischen solchen unterschieden, die geklärt, und solchen, die ungeklärt sind. Art. 16 Abs. 2 Bst. c der Verordnung vom 26. Oktober 2016 über das automatisierte Polizeifahndungssystem (SR 361.0) schreibt vor, dass die Daten über Vermisstmeldungen bis zum Ablauf der Gültigkeit, jedoch höchstens bis zum 100. Altersjahr aufbewahrt werden. Dies hat in der Praxis zur Folge, dass die vermisste Person bei ungeklärten Fällen im automatisierten Polizeifahndungssystem (RIPOL) länger ausgeschrieben ist, als die dazugehörigen Daten im kantonalen System registriert bleiben. Mit der Aufteilung in geklärte und ungeklärte Vermisstenfälle wird diese Problematik behoben und eine ungefähre Angleichung an die Bundesgesetzgebung vorgenommen. Die allenfalls daraus folgende längere Registrierung in den kantonalen Polizeisystemen als im RIPOL führt im Gegensatz zum umgekehrten Fall zu keinen Problemen.

In lit. o wird der veraltete Begriff Personen- und Fahrzeugmeldekarten durch Personen- und Fahrzeugkontrollberichte ersetzt, ohne die Bestimmung inhaltlich zu verändern.

In Abs. 3 wird festgelegt, dass die Aufbewahrungsfristen mehrerer Fall- und Ereignisdaten an die zuletzt endende angepasst werden können, wenn zwischen ihnen ein für die weitere Bearbeitung relevanter Sachzusammenhang besteht. Das ist der Fall, wenn umfangreiche Ermittlungsverfahren zur besseren Übersicht oder aus polizeitaktischen Überlegungen in mehrere Geschäfte aufgeteilt werden (Strukturierung), wenn Dokumente eines Ereignisses initial unter verschiedenen Geschäften abgelegt wurden oder wenn Serieldelikte (z. B. ungeklärte Einbruchdiebstähle) nachträglich einer Täterschaft zugeordnet werden können. Die Daten werden in solchen Fällen in der Regel im System verknüpft.

§ 21. Journaldaten

Journaldaten dokumentieren das polizeiliche Handeln. Meist wird dabei auch ein Fall eröffnet, sodass die Journaldaten sinnvollerweise mit dessen Daten zu löschen sind. Dafür gelten die Fristen gemäss § 20. Gelegentlich werden im Journal Vorfälle registriert, die keine nennenswerte polizeiliche Intervention erfordern und daher auf die Eröffnung eines Falles verzichtet werden kann. Abs. 2 soll sicherstellen, dass auch diese Daten gelöscht werden.

§ 22. Haftdaten, § 23. Gästekontrolldaten und § 24. Grenzkontrolldaten

§ 23 entspricht § 18 Abs. 5 lit. r der POLIS-Verordnung. Die Löschung der Haft- und Grenzkontrolldaten wurde nach der Dauer festgelegt, während der die Daten z. B. für die Bearbeitung weiterer Fälle in Bezug auf dieselbe Person oder Staatshaftungsforderungen, Beschwerden usw. relevant sein können.

§ 25. Ausnahmen

Eine Verlängerung der genannten Aufbewahrungsfristen in Ausnahmefällen muss sachlich begründet sein. Eine solche kann sich z. B. bei Kulturgüterfällen, Raubkunst oder bei der Revision eines Strafurteils mit allfälligem neuem Ermittlungsbedarf ergeben.

2. Abschnitt: Einsatz von Analysesystemen

§ 26. Analysesysteme zum Abgleich von Bildern

Diese Bestimmung hält in Bezug auf § 52a Abs. 4 PolG drei Anwendungsfälle fest. Da es sich immer um den Einsatz von Analysesystemen zur Erkennung von Personen und Sachen durch einen Abgleich mit vorhandenen Datensätzen im Einzelfall handelt, ist eine automatisierte Massenüberwachung ausgeschlossen. Die genannte Gesetzesbestimmung verbietet auch die Echtzeit-Gesichtserkennung, worauf mit dem Wort «nachträglich» in § 26 hingewiesen wird. Damit ist es nicht zulässig, die Aufnahmen einer Überwachungskamera unmittelbar mit polizeilichen Datenbanken abzugleichen und so in Echtzeit die Personen zu identifizieren, die den gefilmten Bereich passieren.

Verfügt die Polizei über ein Bild (z. B. Foto oder frühere Videoaufzeichnung) einer ihr unbekannten (z. B. tatverdächtigen, vermissten) Person, kann sie dieses gemäss lit. a mit vorhandenen erkennungsdienstlichen Aufnahmen abgleichen, um sie zu identifizieren. Ist sie im Besitz des Bildes einer Zielperson oder eines auffälligen Gegenstandes, kann sie es gestützt auf lit. b bzw. lit. c mit anderen Bildern in ihren Systemen abgleichen, um zu prüfen, ob diese in einem anderen Verfahren auftauchen. Diese Möglichkeiten helfen der Polizei, Tatzusammenhänge zu erkennen.

§ 27. Analysesysteme im Bereich der seriellen Kriminalität

Diese Bestimmung führt § 52b PolG näher aus und lehnt sich an § 3b der Verordnung über die Luzerner Polizei vom 6. April 2004 (SRL 351) an, der vom Bundesgericht für gesetzeskonform befunden wurde (BGE 151 I 137 E. 4). Grundsätzlich kann die Polizei gemäss § 52 Abs. 2 PolG in ihren Informationssystemen alle Datentypen bearbeiten, soweit dies zur Erfüllung der ihr gesetzlich übertragenen Aufgaben unentbehrlich ist und den Zwecken in § 2 entspricht. Die Datentypen, welche die Polizei bearbeiten kann, sind in § 3 aufgeführt. Zusätzlich gelten beim Einsatz von Analysesystemen im Bereich der seriellen Kriminalität die Einschränkungen von § 52b PolG. Die Bearbeitung wird in § 27 Abs. 2 weiter eingeschränkt, indem nur gewisse Datentypen mit anderen Behörden gemäss § 52b Abs. 2 PolG ausgetauscht werden dürfen.

Zudem muss für jedes System gestützt auf § 10 IDG eine Datenschutz-Folgenabschätzung erstellt werden, die bei besonderen Risiken für die Grundrechte der betroffenen Personen der oder dem Beauftragten für den Datenschutz zur Prüfung vorgelegt wird.

Nur in der Kriminalanalyse besonders geschulte Mitarbeitende der Polizei dürfen die für die Analyse notwendigen Daten bearbeiten. Die Auswertungen der Analyse dürfen hingegen auch den anderen Mitarbeitenden zur Verfügung gestellt werden.

3. Abschnitt: Polizei-Informationssystem POLIS

§ 28. Inhalt

Der 3. Abschnitt regelt das Polizei-Informationssystem ergänzend zu den allgemeinen Bestimmungen im 1. Abschnitt. Die Regelungen stützen sich auf § 54 PolG und entsprechen weitgehend denjenigen der POLIS-Verordnung. Da die im POLIS verwalteten Daten besonders sensibel sind, sollen dafür weiterhin zusätzliche spezifische Regeln gelten. Die in § 28 aufgezählten Module lehnen sich inhaltlich an § 5 der POLIS-Verordnung an und entsprechen den veränderten Gegebenheiten.

§ 29. Zugriffsberechtigte

§ 29 entspricht §§ 3 und 15 Abs. 2 der POLIS-Verordnung.

§ 30. Hauptverantwortung

Die Kantonspolizei trägt die Hauptverantwortung für die Daten im POLIS, wobei sie diese intern einem oder einer Datenverantwortlichen überträgt, die bzw. der die Tätigkeiten der Datenverantwortlichen gemäss § 10 koordiniert.

§ 31. Protokollierung von Benutzerzugriffen

Die Bestimmung entspricht § 17 der POLIS-Verordnung.

§ 32. Bekanntgabe von Daten im Abrufverfahren, a. zulässige Attribute

Die bundesgerichtliche Rechtsprechung (BGE 151 I 137 E. 6.6) verlangt eine sehr detaillierte Regelung der von den Polizeibehörden anderer Kantone abrufbaren Daten. Die Datentypen für den Datenaustausch im Rahmen der gesamtschweizerischen polizeilichen Abfrageplattform (POLAP) sind bereits in § 54b Abs. 5 PolG festgelegt. § 32 bezeichnet nun noch die abrufbaren Attribute, die für eine effiziente Polizeiarbeit unverzüglich eingesehen werden müssen (vgl. § 54d lit. b PolG). Selbstverständlich gelten dabei die Einschränkungen des PolG, z. B. in Bezug auf Übertretungen (vgl. § 54b Abs. 5 lit. d).

§ 33. b. Protokollierung von Abfragen

§ 33 regelt die Protokollierung der Zugriffe auf die Daten spezifisch im Rahmen von POLAP. Für den funktionierenden Betrieb von POLAP ist eine kongruente Regelung der beteiligten Gemeinwesen für Zugriffe von Behörden anderer Gemeinwesen auf ihre polizeilichen Datenban-

ken notwendig. Neben den Angaben über die Organisation und Benutzer-ID der abfragenden Person sowie den Kontext ist die Auftraggeberin oder der Auftraggeber der Abfrage anzugeben, soweit sie nicht auf eigene Initiative der abfragenden Person erfolgte. Dies ist insbesondere der Fall, wenn Frontmitarbeitende die Einsatzzentrale oder bei grösseren Aktionen eine rückwärtige Stelle mit der Systemabfrage betrauen. Für die nachträgliche Überprüfung der erfolgten Abfragen ist von Belang, wer der eigentliche Urheber der Abfrage ist, da die aufgrund der Benutzer-ID im System registrierte Person oft deren Hintergrund nicht kennt.

§ 34. c. Herausgabe von Protokolldaten

Bei der vorliegenden Herausgabe von Protokolldaten handelt es sich um eine Herausgabe an Private.

§ 35. Kostentragung

§ 35 entspricht § 19 der POLIS-Verordnung. Die Betreiber sind in § 54 Abs. 1 PolG geregelt.

4. Abschnitt: Übergangsbestimmung

§ 36. Aufbewahrungsfristen

Die Anwendung der in §§ 18 ff. geregelten Aufbewahrungs- und Löschfristen auf Daten, die vor dem Inkrafttreten der vorliegenden Verordnung erfasst wurden, würde zumindest im Falle einer Verlängerung der Fristen gegen das Rückwirkungsverbot verstossen. Zudem werden die Löschtermine technisch im Zeitpunkt der Erfassung festgelegt. Eine Überprüfung und Anpassung all dieser Termine an die neuen Bestimmungen wären äusserst aufwendig. Die genannten Vorschriften sollen daher nur auf Daten Anwendung finden, die nach dem Inkrafttreten der Verordnung erfasst werden.

Änderung der Waffenverordnung

§ 10. Elektronisches Informationssystem

Das kantonale Waffenregister stützt sich heute auf Art. 32a Abs. 2 des Bundesgesetzes vom 20. Juni 1997 über Waffen, Waffenzubehör und Munition (WG, SR 514.54). Dessen Abs. 3 sieht vor, dass die Kantone zusätzlich ein gemeinsames harmonisiertes Informationssystem führen können. Die Zugriffsrechte sind in Art. 61 Abs. 1 der Verordnung vom 2. Juli 2008 über Waffen, Waffenzubehör und Munition (WV, SR 514.541) geregelt. Die Kantone planen nun, sich durch die Plattform POLAP gegenseitig Abfragemöglichkeiten zu gewähren. Das entspricht der gesetzgeberischen Absicht eines gemeinsamen harmonisierten Systems. Durch die Ergänzung von § 10 der Waffenverordnung vom 16. Dezember 1998

(LS 552.1) mit einer Verweisung auf Art. 32a Abs. 3 WG wird klargestellt, dass das Zürcher Waffenregister Teil des gemeinsamen harmonisierten Informationssystems sein soll und ausserkantonale Behörden im Rahmen von Art. 61 Abs. 1 WV im Abfrageverfahren darauf zugreifen können.

E. Auswirkungen für Private, Gemeinden und den Kanton

Die vorliegende Verordnung bringt keine neuen Verpflichtungen mit sich und verursacht keine Kosten. Sie führt lediglich die Neuerungen der Änderung vom 30. März 2026 des Polizeigesetzes aus.

F. Regulierungsfolgenabschätzung

Eine Regulierungsfolgenabschätzung im Sinne des Standortförderungs- und Unternehmensentlastungsgesetzes vom 27. Oktober 2025 (LS 930.1) ist vorliegend nicht nötig, da die Vorlage keine direkten administrativen Mehrbelastungen von Unternehmen zur Folge hat.

G. Vereinbarkeit mit den Vorgaben der Behindertenrechtskonvention

Neuerlasse oder Änderungen rechtsetzender Bestimmungen sind auf ihre Vereinbarkeit mit dem Übereinkommen vom 13. Dezember 2006 über die Rechte von Menschen mit Behinderungen (Behindertenrechtskonvention, SR 0.109) zu überprüfen (Richtlinien zur Überprüfung von Rechtsetzungsvorhaben auf ihre Vereinbarkeit mit der Behindertenrechtskonvention vom 11. Dezember 2024). Die vorliegende Verordnung hat keine Auswirkungen auf die Rechtsstellung von Menschen mit Behinderungen.

H. Inkraftsetzung

Mit Verfügung vom 16. Juni 2026 stellte die Direktion der Justiz und des Innern fest, dass gegen die Änderung vom 30. März 2026 des Polizeigesetzes kein Referendum ergriffen wurde (ABI 2026-06-19). Diese Verfügung ist rechtskräftig.

Gegen die Änderung des Polizeigesetzes ist eine Beschwerde beim Bundesgericht hängig. Da das Bundesgericht das Gesuch der Beschwerdeführenden um Erteilung der aufschiebenden Wirkung abgewiesen hat, steht dem Inkrafttreten des Gesetzes nichts entgegen. Der

Regierungsrat hat nunmehr den Zeitpunkt des Inkrafttretens der Gesetzesänderung zu bestimmen. Die Änderung soll, zusammen mit der neuen Verordnung und der Änderung der Waffenverordnung, baldmöglichst und daher auf den 1. Dezember 2026 in Kraft gesetzt werden. Die POLIS-Verordnung wird auf dasselbe Datum aufgehoben.

Im Namen des Regierungsrates

Die Präsidentin:	Die Staatsschreiberin:
Carmen Walker Späh	Kathrin Arioli