

Digitale Gesellschaft, CH-4000 Basel

Departement für Justiz, Sicherheit und Gesundheit
Hofgraben 5
7000 Chur

Per E-Mail an: info@djsg.gr.ch

Basel, 28. August 2024

Stellungnahme zu den Teilrevisionen des Polizeigesetzes im Kanton Graubünden

Sehr geehrter Herr Regierungsrat Peyer,
Sehr geehrte Empfänger:innen

Am 1. Juni 2024 eröffnete das Departement für Justiz, Sicherheit und Gesundheit Graubünden die Vernehmlassung zu den Teilrevisionen des Polizeigesetzes des Kantons Graubünden. Wir bedanken uns für die Möglichkeit zur Stellungnahme.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zur Vereinbarung wie folgt Stellung:

Grundsätzliches

Mit den zwei Teilrevisionen soll das Polizeigesetz des Kantons Graubünden angepasst werden, um den neuen Konflikt- und Problemlagen und dem gestiegenen Sicherheitsbedürfnis der Bevölkerung Rechnung zu tragen. Die Digitale Gesellschaft befürwortet die Aufteilung der Revision in zwei Teile ausdrücklich. Insbesondere im zweiten Teil finden sich aber Aspekte, die unter Berücksichtigung von datenschutzrechtlichen Überlegungen problematisch erscheinen und nicht unkommentiert hingenommen werden können. Auf diese – unsere Kernanliegen betreffenden Bestimmungen – möchten wir in den folgenden Abschnitten näher eingehen.

Teil 1

KBM Prozess (Einschätzen):

Gemäss dem erläuternden Bericht wird das Ergebnis der Vorprüfung aktenkundig gemacht, wenn die Vorprüfung zeigt, dass es sich nicht um eine gewaltbereite Person handelt. Für uns ist unklar, was in diesem Fall unter «aktenkundig» zu verstehen ist. Wird der Kantonspolizei bei einer erneuten Meldung angezeigt, dass die potenziell gewaltbereite Person bereits früher einmal gemeldet worden ist und falls ja, wie lange? Aus Gründen der Gewaltprävention erachten wir es als richtig, dass eine Meldung für eine gewisse Zeit bei der richtigen Stelle angezeigt wird. Hingegen ist auf jeden Fall zu verhindern, dass eine solche Meldung z.B. bei einer Verkehrskontrolle einem Verkehrspolizisten oder einer Verkehrspolizistin angezeigt wird.

Teil 2

Verbot der biometrischen Überwachung

Biometrische Erkennungssysteme werden einerseits zur Authentifizierung von Individuen eingesetzt (one-to-one matching). Andererseits kommen biometrische Erkennungssysteme auch zur Identifizierung eines Individuums aus einer Masse heraus zum Einsatz (one-to-many matching), wobei auf eine Datenbank von biometrischen Daten zurückgegriffen wird. Eine immer häufiger verwendete Form biometrischer Erkennungssysteme ist die Gesichtserkennung. Es gibt jedoch auch Systeme zur Identifizierung von Personen anhand ihres Ganges, ihrer Augen, ihrer Stimme oder anderer biometrischer Daten (vgl. Positionspapier gesichtserkennung-stoppen.ch). Der unterschiedslose Einsatz solcher Systeme im öffentlich zugänglichen Raum kann eine anlasslose, willkürliche oder gezielt diskriminierende biometrische Massenüberwachung ermöglichen, die nicht mit den Grundrechten vereinbar ist. Dabei besteht nur wenig Transparenz darüber, wo und von wem biometrische Erkennungssysteme eingesetzt werden. Es existiert weder eine umfassende Erlaubnis, noch ein explizites Verbot für deren Bearbeitung. Für ihre Verwendung ist aber eine gesetzliche Grundlage erforderlich. Biometrische Daten gelten im revidierten schweizerischen Datenschutzgesetz (DSG), welches am 1. September 2023 in Kraft trat, als besonders schützenswert, wenn sie eine natürliche Person eindeutig identifizieren. Das DSG gilt nur für Bundesbehörden und private Akteure, jedoch nicht für Kantone. Eine gesetzliche Grundlage wäre aber auch für den Einsatz von biometrischen Erkennungssystemen durch die Kantonspolizei notwendig, sofern dieser als zulässig erachtet werden könnte. Die Identifizierung und Überwachung mittels biometrischen Erkennungssystemen stellen eine Verletzung des Rechts auf Privatsphäre (Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II) und des Rechts auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) dar. Das VE-PolG enthält keine Bestimmungen zur (Un-)Zulässigkeit der biometrischen Überwachung. Dies bedauern wir ausdrücklich. Mit der Teilrevision bietet sich die Gelegenheit, ein Verbot der biometrischen Überwachung (konkret Gesichtserkennung) im PolG zu verankern. Biometrische Erkennungssysteme im öffentlichen Raum sind schwere, nicht verhältnismässige Eingriffe in die Grund- und Menschenrechte und daher zu verbieten.

Wir fordern, ein Verbot von biometrischen Erkennungssystemen im öffentlich zugänglichen Raum durch die Polizei im PolG zu verankern.

Art. 21a VE-PolG

Die Digitale Gesellschaft begrüsst, dass betroffene Personen bei präventiven verdeckten Fahndungen – entsprechend der bundesgerichtlichen Rechtsprechung – neu stets informiert werden müssen, sobald der mit der Massnahme verbundene Zweck dies zulässt.

Bei präventiven Überwachungsmassnahmen stellt sich allerdings immer die Frage nach der Vereinbarkeit mit dem Recht auf Privatsphäre (Art. 13 BV, Art. 8 EMRK). Wir vertreten die Ansicht, dass in keinem Fall eine Ausnahme von der Mitteilungspflicht bestehen darf. Zum gleichen Schluss kam das Bundesgericht in BGE 140 I 381, wo die Bestimmungen des Genfer Polizeigesetzes aufgehoben wurden, weil keine nachträgliche Benachrichtigung der betroffenen Person vorgesehen war. Es müssen analog mindestens die Rechte nach der Strafprozessordnung gewährleistet sein, wenn ein Strafverfahren eröffnet ist. Zwar kann auch im

Strafverfahren eine Mitteilung aufgeschoben oder unterlassen werden (vgl. Art. 283 Abs. 2, Art. 298 Abs. 2 StPO), allerdings erfährt die betroffene Person aufgrund der Natur des Strafverfahrens (Aktenaufbewahrung und Akteneinsichtsrecht) spätestens am Ende des Verfahrens von der Massnahme. Um gegen eine Massnahme im Sinne von Art. 21a das Recht auf wirksame Beschwerde gemäss Art. 13 EMRK wahrnehmen zu können, bedarf es in jedem Fall einer Mitteilung an die betroffene Person.

Art. 21b Abs. 1^{bis} VE-PolG

Wie im erläuternden Bericht erwähnt, gelten – gemäss bundesgerichtlicher Rechtsprechung – für den Einsatz von GPS-Ortungsgeräten im Rahmen präventiver polizeilicher Observationen mindestens dieselben Verfahrensgarantien wie für GPS-Überwachungen gemäss der Strafprozessordnung (vgl. BGE 147 I 103 E. 17). Da die technischen Instrumente vorliegend nur zur Standortbestimmung eingesetzt und die Standortdaten weder gespeichert noch als Beweise im Strafverfahren verwendet werden, handelt es sich nicht um eine Überwachung mit technischen Überwachungsgeräten im Sinne von Art. 280 lit. c StPO. Der Eingriff in die Privatsphäre (Art. 13 BV, Art. 8 EMRK) wiegt folglich weniger schwer. Es gibt dennoch gewisse Verfahrensgarantien, die auch bei einer Standortbestimmung mittels technischer Geräte eingehalten werden müssen. Daher beantragen wir, dass technische Geräte zur Standortbestimmung nur zur Erkennung oder Verhinderung schwerer Straftaten eingesetzt werden dürfen und dass der Einsatz von technischen Geräten zur Standortermittlung vorgängig gerichtlich genehmigt wird.

Art. 22a^{bis} VE-PolG

Die Kantonspolizei soll, ohne konkreten Tatverdacht und ohne Verkehrskontrollen gemäss dem eidgenössischen Strassenverkehrsrecht durchzuführen, mittels Bildüberwachungs- und Bildaufzeichnungsgeräten den Strassenverkehr überwachen können. Ungeachtet der Einzelheiten erachten wir eine derartige anlasslose Massenüberwachung als unrechtmässig.

Die Überwachung im öffentlichen Raum (hier: öffentliche Strassen) geht mit wesentlichen Einschränkungen der Grundrechte einher. Dabei wird nicht nur das Grundrecht auf Privatsphäre potentiell verletzt, sie erzeugt auch eine abschreckende Wirkung, die Menschen davon abhält, andere Grundrechte wie die Meinungsäusserungs- und Versammlungsfreiheit wahrzunehmen (sog. chilling effect). Diese Auswirkungen zeigen sich insbesondere bei benachteiligten oder von Diskriminierung betroffenen Personen und Gruppen sowie politischen Aktivist:innen verstärkt. Wir lehnen die Überwachung des öffentlichen Raums daher generell ab.

Wir beantragen, dass Art. 22a^{bis} VE-PolG ersatzlos gestrichen wird

Art. 22b VE-PolG

Die vorliegende Bestimmung sieht die automatisierte Erfassung von Fahrzeugen, deren Kontrollschildern und neu auch von den Insassinnen und Insassen vor sowie den automatisieren Abgleich der erhobenen Daten mit Datenbanken, die Analyse sowie die Erstellung von Bewegungsprofilen. Dies verletzt den Anspruch auf persönliche Freiheit (Art. 10 Abs. 2 BV), das Recht auf Privatsphäre, auf Schutz vor Missbrauch der persönlichen Daten und informationelle Selbstbestimmung (Art. 13 BV; Art. 8 EMRK; Art. 17 UNO-Pakt II sowie das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 [Konvention Nr. 108 des Europarates [SR 0.235.1]), den Anspruch auf ein faires Verfahren und die Unschuldsvermutung (Art. 6 EMRK, Art. 32 BV) und das Recht auf wirksame Beschwerde (Art. 13 EMRK). Diese Normen verleihen jeder Person das Recht, frei von staatlicher Überwachung zu bleiben, vor jedem staatlichen Erheben, Sammeln, Verarbeiten, Aufbewahren und Weitergeben von Angaben, die einen Bezug zur Privatsphäre einer Person haben, frei zu sein und sich frei hiervon bewegen zu können (vgl. JÖRG PAUL MÜLLER/MARKUS SCHEFER, Grundrechte in der Schweiz, S. 167).

Die Bestimmung führt dazu, dass Halterinnen und Halter sowie Insassinnen und Insassen von Fahrzeugen damit rechnen müssen, dass sie bzw. ihr Fahrzeug alleine aufgrund des Umstands, dass sie bzw. ihr

Fahrzeug sich auf einer öffentlichen Strasse durch den Kanton Graubünden bewegen, von der Kantonspolizei Graubünden automatisiert optisch erfasst werden, und dass die dabei erfassten Daten automatisiert bearbeitet werden, namentlich, indem die erfassten Daten mit Daten aus anderen Datenbanken automatisiert abgeglichen, analysiert und zur Erstellung von Bewegungsprofilen genutzt werden. Der Anspruch, sich frei von Überwachung bewegen zu können und insbesondere bei der eigenen Nutzung seines Fahrzeugs oder der Nutzung durch Dritte und bei Fahrten mit Fahrzeugen nicht von optisch vom Staat erfasst zu werden und dadurch in die Datenbearbeitung eingespeist zu werden, welche die angefochtene Bestimmung vorsieht, ist damit nicht gewährleistet. Stattdessen müssen Halterinnen und Halter sowie Insassinnen und Insassen von Fahrzeugen jederzeit damit rechnen, bei einer Fahrt durch den Kanton Graubünden der Bestimmung entsprechend in eine automatische Fahrzeugfahndung einbezogen zu werden. Dies verletzt ihren Anspruch auf die vorstehend genannten Grundrechte.

Das Bundesgericht hat wiederholt festgehalten, die automatisierte Fahrzeugfahndung stelle einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) dar: Im Unterschied zur Kontrollschilderhebung durch eine Polizeistreife ermögliche das System die massenhafte und praktisch unbegrenzte Erhebung und Auswertung von Daten. Erkennungsdienstliche Informationen würden nicht nur erhoben und (mehr oder weniger lang) aufbewahrt, sondern auch mit anderen Datensammlungen zusammengeführt und automatisch abgeglichen. Sowohl die serielle und simultane Verarbeitung grosser und komplexer Datensätze wie auch der Umstand, dass die erkennungsdienstlichen Informationen mit anderweitig erhobenen Daten kombiniert werden, steigerten die Eingriffsintensität. Der Eingriff in das Recht auf Privatsphäre erfolge bei der automatisierten Fahrzeugfahndung weder anlassbezogen noch aufgrund eines konkreten Verdachts. Dies könne eine abschreckende Wirkung zeitigen (sog. «chilling effect»). Schliesslich besteht auch das Risiko, dass Betroffene aufgrund einer dem System immanenten Fehlerquote zu Unrecht in Verdacht gerieten (BGE 146 I 11, E. 3.2 und nicht publ. E. 2.1; Urteil 1C_39/2021 der I. öffentlich-rechtliche Abteilung des Bundesgerichts vom 29. November 2022, E 8.1.1; beides mit Hinweis auf LUKAS BÜRGE, Zulässigkeit und Verwertbarkeit von polizeilichen Aufzeichnungen der automatisierten Fahrzeugfahndung und Verkehrsüberwachung, *forum* 1/2021, S. 58; Beschlüsse des deutschen Bundesverfassungsgerichts zur automatisierten Kraftfahrzeugkennzeichenkontrolle, beide vom 18. Dezember 2018, betr. Bayern [1 BvR 142/15, in: BVerfGE 150, 244] sowie Baden-Württemberg und Hessen [1 BvR 2795/09 und 3187/10, in: BVerfGE 150, 309]).

Wir lehnen die automatisierte Fahrzeugfahndung und Verkehrsüberwachung grundsätzlich ab. Sollte daran jedoch festgehalten werden, so muss der Verwendungszweck in Art. 22b VE-PolG eingeschränkt werden. Das heisst, es muss auf alles, was über eine temporäre (nicht stationäre) Überwachung und den unmittelbaren Abgleich vor Ort hinausgeht, verzichtet werden und Nicht-Treffer sind sofort zu löschen. Zudem braucht es Kontrollmechanismen, die im Gesetz festzuhalten sind. Weiter muss sichergestellt sein, dass bei der automatisierten optischen Erfassung einzig Fahrzeuge und Kontrollschilder erfasst werden und nicht auch die Fahrzeuginsass:innen. Die Erstellung von Bewegungsprofilen ist gänzlich zu streichen.

Art. 27 Abs. 1^{bis} VE-PolG

Die Bestimmung ermöglicht die genannten Datenbearbeitungen zur Erfüllung des gesetzlichen Auftrags der Kantonspolizei. Dies ist nach unserem Erachten viel zu unbestimmt. Es besteht die Gefahr, dass gestützt auf diese Bestimmung beispielsweise eine Bearbeitung von besonders schützenswerten Personendaten getätigt wird, die aufgrund des Zwecks, den sie – die Datenbearbeitung – verfolgt, völlig unverhältnismässig ist.

Wir beantragen, dass in der Bestimmung selbst festgehalten und aus der Botschaft ersichtlich wird, welche Datenbearbeitungen für welche polizeilichen Zwecke getätigt werden können.

Art. 27a VE-PolG

Bei der Bearbeitung von besonders schützenswerten Personendaten handelt es sich grundsätzlich um einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung (Art. 13 Abs. 2 BV). Auf eine solch

generalklauselartige Formulierung – wie hier vorliegend – können Datenbeschaffungen, einschliesslich besonders schützenswerter Personendaten, nicht abgestützt werden.

Wir beantragen, dass in der Bestimmung selbst festgehalten und aus der Botschaft ersichtlich wird, zu welchem polizeilichen Zweck besonders schützenswerte Personendaten beschafft werden können.

Art. 29 Abs. 1 VE-PoIG

Die Digitale Gesellschaft erachtet die Weitergabe, einschliesslich besonders schützenswerter Personendaten, an Dritte als kritisch. Sofern gesetzlich vorgesehen, erachten wir ein solches Vorgehen als akzeptabel. Hingegen scheint es uns als zu generalklauselartig formuliert, dass Daten, einschliesslich besonders schützenswerter Personendaten, an Dritte weitergeleitet werden können, wenn es unerlässlich ist. Daher beantragen wir, dass Art. 29 Abs. 1 VE-PoIG wie folgt geändert wird:

¹ Die Kantonspolizei kann Daten, einschliesslich besonders schützenswerter Personendaten, an Dritte weiterleiten, soweit dies gesetzlich vorgesehen ~~oder unerlässlich~~ ist für:

Art. 29 Abs. 3 VE-PoIG

Es ist unklar, wie eine automatisierte Datenbekanntgabe auf die Daten beschränkt werden kann, die notwendig sind für die Aufgabenerfüllung der Gemeinden bzw. wie eine darüber hinausgehende automatisierte Datenbekanntgabe ausgeschlossen werden kann. Lediglich zur Erleichterung der behördlichen Aufgaben darf nicht eine Schnittstelle zwischen den verschiedenen Einheiten geschaffen und die Bekanntgabe undifferenziert erfolgen; die Interessen der betroffenen Person (Schutz vor Missbrauch der eigenen Daten, Schutz der Privatsphäre) zum Interesse des Staates an effizienteren Abläufen stehen dann in einem Missverhältnis.

Wir beantragen, dass in der Bestimmung selbst festgehalten und aus der Botschaft ersichtlich wird, welche Datenbestände zur Erfüllung welcher polizeilichen Aufgabe, d.h. zu welchem Zweck, automatisiert an die Gemeinden bekanntgegeben werden können.

Art. 29a^{bis} VE-PoIG

Beim Bund und in den Kantonen gibt es eine Vielzahl von Datenbanken mit polizeilichen Informationen, die unterschiedlichen Bearbeitungszwecken dienen. Die Möglichkeiten der kantonalen Polizeikorps untereinander auf diese Daten zugreifen zu können, sind jedoch zu Recht begrenzt. Öffentliche Organe dürfen Personendaten grundsätzlich nur zu dem Zweck bearbeiten, zu dem sie erhoben worden sind. Den automatisierten Informationsaustausch und das Abrufverfahren ohne Einschränkungen und Anforderungen für den Einzelfall beurteilen wir als sehr problematisch. Der uneingeschränkte Zugriff auf zahlreiche bundesweite Datenbanken ohne die Voraussetzung zur Angabe, weshalb und zu welchem Zweck eine bestimmte Information benötigt wird, birgt erhebliches Missbrauchspotenzial.

Wir lehnen Art. 29a^{bis} VE-PoIG in dieser Form ab.

Art. 29a^{bis} Abs. 1 VE-PoIG

«Zur Erfüllung ihrer Aufgaben» ist zu unspezifisch. Die Zwecke zu denen eine elektronische Zusammenarbeit möglich ist, müssen genauer definiert werden.

Art. 29a^{bis} Abs. 2 VE-PoIG

Eine durch «insbesondere» nicht abschliessende Aufzählung der Schnittstellen und Informationssysteme genügt nicht. Die Schnittstellen und Informationssysteme für die elektronische Zusammenarbeit müssen abschliessend geregelt werden.

Zudem ist die Notwendigkeit eines Abrufverfahrens zu begründen bzw. ist vorab zu klären, ob das Abrufverfahren überhaupt notwendig ist. Es muss eingegrenzt werden, zu welchem Zweck auf welche Daten von welchen Behörden zugegriffen werden kann. Kontrollmechanismen sind vorzusehen.

Art. 29a^{bis} Abs. 3 VE-PolG

Beteiligt sich die Kantonspolizei an Informationssystemen im Sinne von Abs. 2 lit. b oder lit. c, ist die Regierung berechtigt, die Datenbearbeitung einem anderen Recht zu unterstellen und die Aufsichtsbehörde zu bezeichnen.

Es ist überhaupt nicht nachvollziehbar, was mit dieser Bestimmung bezweckt werden soll. Fraglich ist insbesondere, was es heissen soll, dass der Regierungsrat die Datenbearbeitung einem anderen Recht (als dem Recht des Kantons Graubünden?) zu unterstellen. Geht es hier darum, dass die Kantonspolizei des Kanton Graubünden beispielsweise Daten aus dem Kanton Solothurn bearbeitet und dass diese Datenbearbeitung deswegen dem Recht des Kantons Solothurn unterstellt wird? So zumindest verstehen wir diese Bestimmung (am ehesten). Sofern diese Auffassung zutrifft, ist anzumerken, dass das Handeln der Kantonspolizei eines Kantons immer nur dem Recht dieses Kantons unterstellt sein kann. Zudem ist es Aufgabe des Gesetzgebers und nicht der Regierung, das Recht, nach welchem sich das polizeiliche Handeln richtet zu bestimmen bzw. zu erlassen.

Art. 29a^{bis} Abs. 4 VE-PolG

Der Gesetzesentwurf sieht vor, dass die Kantonspolizei die Einzelheiten der Zusammenarbeit, namentlich betreffend Organisation, Verantwortung für den Betrieb und die Datenbearbeitung, Massnahmen zur Gewährleistung der Datensicherheit, Modalitäten der Gewährleistung von Auskunft und Einsicht sowie die Kostentragung in einer Vereinbarung regelt. Angesichts der Grundrechtsrelevanz und Sensibilität der erfassten Personendaten halten wir es nicht für vertretbar, dass diese höchst relevanten Aspekte der Datenbearbeitung in einer Vereinbarung der beteiligten Polizeikorps geregelt werden. Stattdessen braucht es dafür jeweils konkret ausformulierte Bestimmungen in einer formell-gesetzlichen Grundlage.

Wir beantragen, dass diese Rahmenbedingungen zur elektronischen Zusammenarbeit ausdrücklich auf Gesetzesstufe geregelt werden.

Art. 30 Abs. 1 und 2 VE-PolG

Wir beantragen, dass diese Rahmenbedingungen der Datenbearbeitung ausdrücklich auf Gesetzesstufe geregelt werden.

Schlussbemerkung

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Der Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln bedeutet keine Zustimmung der Digitalen Gesellschaft.

Freundliche Grüsse

Erik Schönenberger
Geschäftsleiter