KANTON AARGAU

REGIERUNGSRAT

Regierungsgebäude, 5001 Aarau
Telefon 062 835 12 40, Fax 062 835 12 50
regierungsrat@ag.ch
www.ag.ch/regierungsrat

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)
Haus der Kantone
Speichergasse 6
Postfach
3001 Bern

21. Februar 2024

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme; Stellungnahme

Sehr geehrte Damen und Herren

Der Regierungsrat der Kantons Aargau bezieht sich auf Ihr Schreiben vom 23. November 2023, mit welchem Sie den Entwurf der Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme zur Stellungnahme zugestellt haben. Er bedankt sich für diese Möglichkeit.

Der Abschluss einer entsprechenden Vereinbarung ist aus Sicht des Regierungsrats zwingend erforderlich. Als fraglich erweist sich allerdings, ob die Bestimmungen des Vereinbarungsentwurfs vollständig sachgerecht sind und den datenschutzrechtlichen Vorgaben entsprechen. Der Regierungsrat bittet die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) deshalb, sich noch einmal vertieft mit den datenschutzrechtlichen Aspekten dieser Vereinbarung zu befassen und den vorliegenden Entwurf nötigenfalls entsprechend zu überarbeiten. Zu prüfen sind insbesondere die folgenden Fragen:

- Entsprechen Gegenstand und Zweck gemäss Art. 1 des Vereinbarungsentwurfs den verfassungsrechtlichen Anforderungen?
- Genügt die Zweckdefinition gemäss Art. 1 des Vereinbarungsentwurfs oder müsste nicht der Zweck für jede einzelne Abfrageplattform beziehungsweise für jedes einzelne Datenbanksystem separat in der Vereinbarung definiert sein?
- Muss Art. 3 des Vereinbarungsentwurfs dahingehend angepasst werden, dass Bagatellvorkommnisse nicht vom Anwendungsbereich des gemeinsamen Polizeidatenraums erfasst werden?
- Bedarf es ergänzender Bestimmungen in der Vereinbarung, um Zweckänderungen verhindern zu können?
- Bedarf es ergänzender Bestimmungen betreffend übergeordnete Aufsicht beziehungsweise Kontrolle der Datenbearbeitung im Rahmen der gemeinsam betriebenen Ablageplattform und der gemeinsam betriebenen Datenbanksysteme, insbesondere wenn der Bund nicht an diesen beteiligt ist?

- Entsprechen die im Vereinbarungsentwurf vorgesehenen Verweise auf Regelungen in Betriebsverordnungen den verfassungsrechtlichen Anforderungen?

Aus Sicht des Regierungsrats besteht ein erhebliches Risiko, dass die Vereinbarung in der aktuellen Ausgestaltung einem Normenkontrollverfahren nicht standhalten würde.

Die KKJPD wird zudem gebeten, im Hinblick auf die Bereinigung der Vereinbarung und das darauffolgende Beitrittsverfahren möglichst konkret aufzuzeigen, mit welchen Kosten die Kantone im Zusammenhang mit dem Betrieb der gemeinsamen Abfrageplattform und den gemeinsamen Datenbanksystemen zu rechnen haben.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Im Namen des Regierungsrats

Dr. Markus Dieth
Landammann

Joana Filippi
Staatsschreiberin

Kopie
- info@kkjpd.ch

KANTON
APPENZELL INNERRHODEN

Landammann und Standeskommission

Sekretariat Ratskanzlei
Marktgasse 2
9050 Appenzell
Telefon +41 71 788 93 11
info@rk.ai.ch
www.ai.ch

Ratskanzlei, Marktgasse 2, 9050 Appenzell

Per E-Mail an
info@kkjpd.ch

Appenzell, 22. Februar 2024

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme
Stellungnahme Kanton Appenzell I.Rh.

Sehr geehrte Damen und Herren

Mit Schreiben vom 23. November 2023 haben Sie uns die Vernehmlassungsunterlagen zum Entwurf einer Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme zukommen lassen.

Die Standeskommission hat die Vereinbarung geprüft. Sie begrüsst grundsätzlich Bestrebungen, welche den Polizeibehörden erlauben, auf Daten in kantonalen, nationalen und internationalen Polizei-Informationssystemen zuzugreifen. Dies ist für eine effiziente, kantonsübergreifende oder internationale Polizeiarbeit unabdingbar.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Im Auftrage von Landammann und Standeskommission
Der Ratschreiber:

Markus Dörig

Zur Kenntnis an:
- Justiz-, Polizei- und Militärdepartement Appenzell I.Rh., Marktgasse 10d, 9050 Appenzell
- Ständerat Daniel Fässler, Weissbadstrasse 3a, 9050 Appenzell
- Nationalrat Thomas Rechsteiner (thomas.rechsteiner@parl.ch)

Landeskanzlei
Kasernenstrasse 31
4410 Liestal
T 061 552 50 06
landeskanzlei@bl.ch
www.bl.ch

BASEL LANDSCHAFT
REGIERUNGSRAT

Regierungsrat, Kasernenstrasse 31, 4410 Liestal

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
info@kkjpd.ch

Liestal, 6. Februar 2024

Vernehmlassung betreffend die interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme

Sehr geehrte Frau Präsidentin
Sehr geehrter Herr Präsident

Besten Dank für die Gelegenheit zur Stellungnahme.

Wir begrüssen das Vorhaben, polizeiliche Daten zwischen den Kantonen untereinander und mit dem Bund austauschen zu können. Die Strafverfolgung muss über die Kantonsgrenzen hinweg auf Informationen zugreifen und Tatzusammenhänge herstellen können.

Zu den einzelnen Bestimmungen haben wir folgende Bemerkungen:

Art. 1 Abs. 1 Gegenstand und Zweck
Bst. a: Zu prüfen ist, ob der weit gefasste Begriff «öffentliche Ordnung», der viele Gefahren von geringer Intensität umfasst, aus verfassungsrechtlicher Sicht dem umfassenden Datenaustausch unterworfen werden darf.

Bst. b: Gilt der Datenaustausch im Bereich der präventiven Polizeitätigkeit für sämtliche Delikte? Wir bitten Sie, die Zulässigkeit der umfassenden Umschreibung rechtlich zu prüfen im Hinblick auf die Verfassungskonformität.

Artikel 2: Gemeinsame Abfrageplattformen und Datenbanksysteme
Laut den Erläuterungen handelt es sich bei Art. 2 Abs. 1 um den Kern der Vorlage, welcher den Kantonen die formelle Rechtsgrundlage bietet, Polizeidaten mit anderen Kantonen und gegenüber dem Bund auszutauschen. Darin wird einzig das Zugänglichmachen von Daten aufgeführt. Wäre es hier nicht sinnvoll, auch das Abrufen von Daten bzw. das Beschaffen, Verwenden etc. von Daten entsprechend der «Datenbearbeitung» gemäss Art. 5 Bst. d DSG zu nennen?

Artikel 3: Anwendungsbereich
Im Bericht wird auf Art. 3 lit. i verwiesen, obwohl im Vereinbarungstext keine lit. i aufgeführt wird.

Artikel 4: Anwendbares Recht
Aufgrund dieser Formulierung ist nicht klar, ob in den Bereichen Haftung, Kostentragung und Verfahrensrecht auf die PTI-Vereinbarung verwiesen wird oder ob gerade für diese Bereiche in der vorliegenden Vereinbarung ein «abweichender Rechtsrahmen» geschaffen wird. Da sich im Folgenden Regelungen zur Haftung und Kostentragung finden, gehen wir davon aus, dass für diese Punkte die PTI-Vereinbarung nicht anwendbar sein soll. (Unklar ist uns, wo das Verfahrensrecht geregelt ist?)

Wir schlagen deshalb die folgende Formulierung vor:
«Es gilt das in der PTI-Vereinbarung für anwendbar erklärte Recht, soweit diese Vereinbarung keine abweichenden Bestimmungen vorsieht. Abweichende Bestimmungen bestehen insbesondere für die Haftung, Kostentragung und das Verfahrensrecht.»

Weitere Bestimmungen zum anwendbaren Recht in Artikel 7 Ziffer 2, Artikel 21 und Artikel 22:
Die Regelungen des anwendbaren Rechts sind kompliziert, verstreut über die Artikel 4, 7 Ziffer 2, 21 und 22, uneinheitlich und zudem teils davon abhängig, ob der Bund beteiligt ist oder nicht (vgl. Art. 10 Abs. 4). Wir empfehlen, hierzu eine klarere Regelung zu finden.

Artikel 5 Absatz 9: Begriffe
Die Regelung der Verantwortlichkeiten und die damit verbundenen Pflichten sind nicht genügend klar normiert. Für jede Abfrageplattform oder eine gemeinsame Datenbank ist ein Gesamtverantwortlicher zu definieren und wir schlagen vor, zu normieren, welche Aufgaben er in seiner Rolle zu erfüllen hat. Gleichfalls erscheint die Rolle des Leistungserbringers nicht vollständig geklärt. Die kantonalen Datenschutzgesetze wie auch das Bundesdatenschutzgesetz verwenden typischerweise die Unterscheidung zwischen dem verantwortlichen öffentlichen Organ («Der/die Verantwortliche») und einer Auftragsdatenbearbeiterin. Die Verantwortlichen entscheiden über den Umfang, die Zwecke und die Mittel und somit auch über die Angemessenheit der Sicherheitsmassnahmen der Datenbearbeitung und die Auftragsdatenbearbeiterinnen setzen diese um.

Artikel 6: Bearbeitungsgrundsätze
Wir schlagen vor, auf rein deklaratorische Bestimmungen zu verzichten wie insbesondere Artikel 6 Ziff. 1 und Ziff. 3.

Art. 7 Abs. 3 Umfang der Datenbearbeitung und Datenschutz
Der Begriff «insbesondere» bedeutet, dass die Auflistung nicht abschliessend ist. Aus den Erläuterungen sehen wir nicht, welche weitere Punkte, die nicht in Absatz 3 aufgeführt sind, hier hinzukommen könnten. Im Hinblick auf das Bestimmtheitsgebot laden wir Sie ein, zu prüfen, ob eine nicht abschliessende Formulierung verfassungskonform ist.

Artikel 8: Haftung
Art. 25 Abs. 5 PTI-Vereinbarung lautet:
Für Staatshaftungsansprüche nach bernischem Recht haftet PTI Schweiz mit ihrem Vermögen. Die Ausfallhaftung des Kantons Bern (Art. 101 Abs. 2 des bernischen Personalgesetzes vom 16. Sept. 2004) gilt nicht; an ihre Stelle treten die Beitragsverpflichtungen nach dieser Vereinbarung.

Art. 101 Personalgesetz Kt. Bern lautet:
[1]Öffentliche Organisationen des kantonalen Rechts und private Organisationen oder Personen, die unmittelbar mit kantonalen öffentlichen Aufgaben betraut sind, haften für den Schaden, den ihre Organe oder Angestellten in Erfüllung ihrer Aufgabe Dritten widerrechtlich zugefügt haben.
[2] Wird ein Schaden, für den eine Organisation oder eine Person gemäss Absatz 1 haftet, nicht gedeckt, steht der Kanton für den Ausfall ein. In diesem Umfang geht die Forderung der Geschädigten auf den Kanton über.

Im Bericht steht: «Handelt es sich beim Leistungserbringer um eine Bundesstelle, so gilt das Bundesgesetz über die Verantwortlichkeit des Bundes sowie seiner Mitglieder und Beamten (Verantwortlichkeitsgesetz) (…).» Wir verstehen diese Ausführung so, dass für die Frage der Haftung die PTI-Vereinbarung nicht anwendbar sein soll, sondern die «für sie anwendbaren Rechtsgrundlagen» gemäss Art. 8 Ziffer 1. Dies würde bedeuten, dass wie im Bericht erwähnt, für den Bund das Verantwortlichkeitsgesetz gilt. Da Leistungserbringer auch Dritte und damit Private sein können, wären für sie privatrechtliche Haftungsnormen und für die Kantone ihr jeweiliges Staatshaftungsgesetz anwendbar. Wir bitten um entsprechende Ergänzung und Konkretisierung im Bericht.

Im Bericht wird zu Art. 8 Ziffer 2 auf Art. 25 Abs. 5 der PTI-Vereinbarung verwiesen. Im Fall einer analogen Regelung zu Art. 25 Abs. 5 der PTI-Vereinbarung würden die Ausführungen im Bericht zur Verantwortlichkeit des Bundes keinen Sinn ergeben, da gemäss Art. 25 Abs. 5 der PTI-Vereinbarung für die Staatshaftung das bernische Recht anwendbar ist. Da der Bund PTI-Vereinbarungspartei ist, gilt dies auch für den Bund.

Wir verstehen es so, dass einzig für die Frage des Ausfalls, d.h. wenn die haftbare Person oder Organisation den Schaden nicht decken will oder kann, Art. 25 Abs. 5 der PTI-Vereinbarung analog angewendet werden soll, nicht aber für die Frage, ob eine Haftbarkeit gegeben ist.

Wir schlagen die folgende Formulierung vor, wobei der Leistungserbringer definitionsgemäss (vgl. Art. 5 Ziffer 9) PTI Schweiz oder ein bezeichneter Dritter, mithin auch ein Privater, sein kann. Ziffer 1 ist mit dem Begriff «Leistungserbringer» zu ergänzen.

«1. Teilnehmende, Leistungserbringer, ihre Mitarbeitenden und Auftragnehmer, soweit ihnen eine öffentliche Aufgabe übertragen ist, haften nach den für sie anwendbaren Rechtsgrundlagen für den Schaden, den sie durch widerrechtliches Bearbeiten von Daten einem anderen Teilnehmenden oder Dritten zufügen.
2. Soweit eine Haftung des Leistungserbringers besteht, haftet dieser mit seinem Vermögen. Wird ein Schaden, für den ein Leistungserbringer haftet, nicht gedeckt, steht die PTI Schweiz mit den Beitragsverpflichtungen nach der PTI-Vereinbarung dafür ein.»
(Ziffer 3 wie vorgesehen)

Art. 10 Verantwortlichkeiten und Recht der Betroffenen Personen
Abs. 1: Wo ist die Gesamtverantwortung für POLAP im Konkordat ausdrücklich geregelt? Gemäss Bemerkung zu Art. 10 Abs. 4 liegt diese beim fedpol. Die Gesamtverantwortung für die Austauschplattform umfasst u.a. technische Vorgaben für den Anschluss der Quellsysteme, die Verantwortung für das Benutzermanagement (IAM), die Verantwortung für die sichere Datenübermittlung sowie Vorgaben zur Protokollierung sowie Kontrolle der Einhaltung der Vorgaben. Wir bitten Sie, diesen Aspekt im Konkordatstext und nicht nur in den Erläuterungen klar zu regeln.
Abs. 4: Gemäss den Erläuterungen zu Art. 10 Abs. 4 ist vorgesehen, dass das fedpol verantwortlich für POLAP sein wird. Dies widerspricht der Aussage auf Seite 12, 2. Abschnitt, wonach die Verantwortlichkeiten für POLAP bei den Verantwortlichen der Quellsysteme belassen wird. Wir bitten um Klarstellung.

Artikel 16: Gemeinsame Datenbanksysteme, Artikel 17: Betriebsverordnung und Artikel 18: Inhalt der Betriebsverordnung
Laut Art. 18 der Vereinbarung ist vorgesehen, dass grundlegende und wichtige Regelungen wie der Name und der Zweck des gemeinsamen Datenbanksystems, die mögliche Datenbearbeitung, usw. in den Bst. a bis m in einer Betriebsverordnung geregelt werden sollen, welche dann durch den jeweils zuständigen Verordnungsgeber der Kantone erlassen wird.
Insbesondere mit Blick darauf, dass die noch zu schaffenden gemeinsamen Datenbanksysteme in Grundrechte von Privaten eingreifen können (insbesondere in den Schutz der Privatsphäre, Art. 13 BV), sind unseres Erachtens diese in Art. 18 aufgeführten Punkte zwingend durch den Gesetzgeber zu regeln und nicht in einer Betriebsverordnung. Es handelt sich um wichtige und grundlegende Bestimmungen. Für den Fall der Schaffung eines gemeinsamen Datenbanksystems ist deshalb eine neuerliche interkantonale Vereinbarung (nach dem gleichen Verfahren, das für die Gesetzgebung gilt) abzuschliessen, welche diese grundlegenden Punkte regelt.
Gleichzeitig sind wir der Ansicht, dass auch geringfügige Änderungen der Betriebsverordnung, sobald diese auch nur untergeordneten Rechtswirkungen haben, nicht ohne Beschluss durch den Verordnungsgeber erfolgen dürfen (vgl. Art. 17 Ziffer 3 und 4).

Artikel 25 Ziffer 1: Protokollierung
Die Protokolldaten sollten unseres Erachtens gleich lang wie die Daten aufbewahrt bzw. erst mit den Daten gelöscht werden.

Artikel 26: Datenlöschung
Wie unter Artikel 16 ausgeführt, reicht es unseres Erachtens nicht, für die Schaffung eines konkreten Datenbanksystems eine Betriebsverordnung zu erlassen. Erforderlich ist, zumindest nach basellandschaftlichem Verfassungsrecht, eine interkantonale Vereinbarung, welche durch die Kantone im formellen Gesetzgebungsverfahren – gleich wie die vorliegende Vereinbarung – erlassen wird. Die Löschfristen sollten in der jeweiligen Vereinbarung geregelt werden und sich am jeweiligen Verwendungszweck orientieren.

Eine starre zeitliche Frist von 10 Jahren erscheint als nicht adäquat, bei einer Vollstreckungsverjährung von bis zu 30 Jahren gemäss Art. 97 StGB.

Artikel 27: Betroffenenrechte
Ziffer 3 nennt eine zentrale Auskunftsstelle. Worum handelt es sich dabei bzw. wer übernimmt diese Aufgabe? Diese Auskunftsstelle sollte für jede Datenbank explizit benannt werden. Vorzugsweise sollte dies im vorliegenden Konkordat geschehen.

Art. 28 Abs. 2 Auftragsbearbeitung
Polizeidaten sind regelmässig besonders sensitiv und von erhöhtem Schutzbedarf. Deshalb sollte eine Auslagerung ins Ausland nur ausnahmsweise und aus triftigen Gründen, d.h. wichtigen öffentlichen Interessen, erfolgen. Reine Kosten- und Effizienzgründe reichen dafür nicht aus (rein finanzielle Interessen stellen keine tauglichen öffentlichen Interessen zur Rechtfertigung eines Grundrechtseingriffes nach Art. 36 BV dar).

Artikel 30: Beitritt und Artikel 31: Änderung der Betriebsverordnung
Wir unterstützen die vorgeschlagene Formulierung, wonach sich der Genehmigungsprozess nach dem Recht des jeweiligen Kantons richtet. Nach basellandschaftlichem Verfassungsrecht ist dies das Parlament (Landrat).

Artikel 32: Kündigung und Austritt
Will man einzig von Seiten der Teilnehmenden eine Kündigung ermöglichen oder soll es auch den Leistungserbringern möglich sein, zu kündigen?
Falls ja, sollte diese Kündigungsmöglichkeit jedenfalls auf Stufe interkantonale Vereinbarung, welches das formelle Gesetzgebungsverfahren im Kanton durchläuft, geregelt werden und nicht auf Ebene Betriebsverordnung.

Vorgeschlagene Rechtsgrundlagen in den kantonalen Polizeigesetzen
Im Entwurf werden Musterformulierungen für die Ergänzung der kantonalen Polizeigesetze (Art. X1 und X2) vorgeschlagen:

- Aus den Unterlagen geht nicht hervor, ob diese Ergänzungen alternativ oder zusätzlich zum Konkordat geschaffen werden sollen. Unseres Erachtens sollten diese Bestimmungen im Konkordat enthalten sein. Eine Aufnahme in die kantonalen Polizeigesetze wäre dann überflüssig.
- Was ist in Art. X2 mit dem Verweis «gemäss Art. X» genau gemeint? Ein Verweis auf § 3 und § 44a des Polizeigesetzes/BL?

Verfassungsrechtliche Überprüfung (Datenschutz)
Die kantonsintern konsultierten Fachstellen äussern zu einzelnen Punkten Bedenken, ob diese verfassungskonform sind. Uns ist es ein Anliegen, dass das Konkordat einer gerichtlichen Überprüfung standhalten wird. Die Polizei, die Staatsanwaltschaft und die Gerichte sind darauf angewiesen, dass die gestützt auf das Konkordat gewonnenen Beweise (via Datenaustausch) verwertbar sind. Kommt ein Gericht zum Schluss, dass Normstufe oder die Bestimmtheit nicht dem verfassungsrechtlichen Datenschutz entspricht, können Strafverfahren mangels verwertbarer Beweise teilweise oder ganz die Grundlage verlieren. Daher regen wir an, die folgenden Fragestellungen zu klären:

- Normstufe: Laut unserem kantonalen Datenschutzgesetz (vgl. § 19 IDG/BL; SGS 162) dürfen besondere Personendaten (Profiling usw.) nur dann bekannt gegeben werden, wenn ein Gesetz dazu ausdrücklich ermächtigt oder dies zur Erfüllung einer im Gesetz ausdrücklich umschriebenen Aufgabe erforderlich ist. Auch im Abrufverfahren dürfen besondere Personendaten nur zugänglich gemacht werden, wenn ein Gesetz im formellen Sinn dies ausdrücklich vorsieht. Sind diese Anforderungen für den Datenaustausch gestützt auf das vorliegende Konkordat eingehalten?
- Normdichte: Kritisiert wird aus in datenschutzrechtlicher Hinsicht, dass die Umschreibung des Umfangs des Datenaustauschs zu vage gefasst und das verfassungsrechtliche Bestimmtheitsgebot nicht eingehalten sei. Wie kann dieses Problem behoben werden?

Hochachtungsvoll

Monica Gschwind
Regierungspräsidentin

Elisabeth Heer Dietrich
Landschreiberin

Regierungsrat des Kantons Basel-Stadt

Rathaus, Marktplatz 9
CH-4001 Basel

Tel: +41 61 267 85 62
E-Mail: staatskanzlei@bs.ch
www.regierungsrat.bs.ch

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)

Per E-Mail an:
info@kkjpd.ch

Basel, 27. Februar 2024

P231678

Regierungsratsbeschluss vom 27. Februar 2024
Vernehmlassung der KKJPD zur Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme: Stellungnahme des Kantons Basel-Stadt

Sehr geehrte Damen und Herren

Mit Schreiben vom 23. November 2023 haben Sie uns die Vernehmlassungsunterlagen zu einer Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme zukommen lassen. Wir danken Ihnen für die Gelegenheit zur Stellungnahme.

Der Regierungsrat des Kantons Basel-Stadt würde in formeller Hinsicht zwar den Erlass eines Bundesgesetzes begrüssen, doch unter den gegebenen Umständen – das EJPD erachtet dafür eine verfassungsrechtliche Grundlage als notwendig – erscheint der Abschluss einer Interkantonalen Vereinbarung sinnvoll.

Die Strafverfolgungsbehörden sind bei ihrer strafprozessualen Ermittlungsarbeit immer stärker darauf angewiesen, polizeiliche Daten national, vernetzt, vereinheitlicht und auch rasch austauschen zu können. Die derzeit herrschende Praxis mittels Einzelverbreitung von Erkenntnisanfragen ist veraltet und auch im Hinblick auf die mit den Schengen-Standards einzuhaltenden Antwortfristen zu langsam und zu schwerfällig. Allerdings ist den datenschutzrechtlichen Bedenken Rechnung zu tragen. Wir überlassen Ihnen in der Beilage deshalb die Stellungnahme des Datenschutzbeauftragten des Kantons Basel-Stadt.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse
Im Namen des Regierungsrates des Kantons Basel-Stadt

Lukas Engelberger
Vizepräsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin

Beilage
- Stellungnahme des Datenschutzbeauftragten des Kanton Basel-Stadt vom 8. Februar 2024

Datenschutzbeauftragter des Kantons Basel-Stadt

Beat Rudin, Prof. (em.) Dr. iur., Advokat
Datenschutzbeauftragter
Henric Petri-Strasse 15, Postfach 205
CH-4010 Basel

Tel: +41 61 201 16 40
direkt: +41 61 201 16 42
E-Mail: beat.rudin@dsb.bs.ch
www.dsb.bs.ch

Per E-Mail an: <Politikreferat@jsd.bs.ch>

Politikreferat
Justiz- und Sicherheitsdepartement des
Kantons Basel-Stadt

Basel, 8. Februar 2024

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme / Stellungnahme

Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, zum vorliegenden Geschäft Stellung nehmen zu können. Unsere Stellungnahme stützt sich auf Vorbereitungen im Rahmen der Arbeitsgruppe «Sicherheit» von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, und ist insbesondere mit der Aufsichtsstelle Datenschutz des Kantons Basel-Landschaft abgestimmt.

1 Allgemeines

Die Vorlage der KKPKS wurde durch Mitglieder der Konferenz der Schweizerischen Datenschutzbeauftragten (privatim) ebenfalls einer eingehenden Analyse unterzogen. privatim wird eine detaillierte Vernehmlassungsantwort verfassen und der KKPKS zustellen. Wir beschränken uns an dieser Stelle auf die aus unserer Sicht für unsere Kanton wichtigsten datenschutzrechtlichen Aspekte.

1.1 Form der Rechtsetzung

Die gewählte Form des rechtsetzenden Konkordats für die Schaffung eines einheitlichen Polizeidatenraums hat zum Ziel, einheitliche Rechtsgrundlagen für die (teilnehmenden) Kantone für den Austausch von Daten, gemäss dem vorliegenden Entwurf aber auch über die Datenbearbeitung selber in gemeinsamen Datenbanken zu schaffen. Die derzeit bestehenden Rechtsgrundlagen in den kantonalen Polizeigesetzen sind in vieler Hinsicht uneinheitlich, und führen in der Praxis zu Auslegungsproblemen. Insofern begrüsst der Datenschutzbeauftragte grundsätzlich eine Vereinheitlichung, da klare Regeln für die Bearbeitung von Personendaten (inkl. Datenaustausch) eine hohe Bedeutung haben. Aufgrund der erfahrungsgemäss nicht einfach durchzuführenden Anpassung eines Konkordates enthält der vorliegende Entwurf zahlreichreiche erhebliche Rechtsfragen, deren Regelung auf Verordnungsebene erfolgen soll, was zu einer geringeren demokratischen Legitimation führt (unter der Annahme, dass für diese Fragen die Verordnung überhaupt die ausreichende Normstufe ist). Vorgesehen ist, dass die strategische Versammlung der PTI die Verordnungen für die spezifischen gemeinsamen Datenbanken erlassen soll, die dann durch die einzelnen Kantone genehmigt werden müssen (Art. 17 Abs. 2 f.). Den Kantonen wird empfohlen, die Kompetenz zur Genehmigung der Betriebsverordnungen an ihre Vertretung in der strategischen

Versammlung der PTI zu delegieren (Erl. Bericht, S. 15). Dies ist gemäss Art. 6. Abs. 2 PTI-Vereinbarung die kantonale Justiz- und Polizeidirektorin. Damit haben das Volk und die Parlamente nach Inkrafttreten des Konkordats wenig bis keinen Einfluss mehr auf die Regelungsmaterie, die aber in vielen Fällen derart wichtige Regelungen enthält, die eigentlich auf Stufe Gesetz gehörten.

Der Bund kann der vorliegenden Vereinbarung nicht beitreten, allerdings ist einerseits vorgesehen, dass fedpol die gemeinsame Abfrageplattform betreibt, und andererseits, dass sich der Bund einzelnen gemeinsamen Datenbanken durch die Übernahme der Betriebsverordnung bzw. den Abschluss einer Leistungsvereinbarung anschliessen kann. Der Bund ist somit aktiver Teilnehmer beim Austausch von Polizeidaten und dem Betrieb von gemeinsamen Datenbanken, obwohl das Polizeirecht in der Kompetenz der Kantone liegt. Er hat es bisher mit Verweis auf seine fehlende Rechtsetzungskompetent abgelehnt, gesetzgeberisch tätig zu werden. Ende letzten Jahres hat der Nationalrat einer Motion seiner sicherheitspolitischen Kommission zugestimmt, die entsprechenden Verfassungsgrundlagen zu schaffen, um diese Materie regeln zu können.

Eine Regelung in einem Bundesgesetz sowie in vom Bundesrat erlassenen Verordnungen genösse u.E. wesentlich mehr demokratischen Rückhalt als die vorliegende Variante. Wir regen an zu prüfen, ob einer Bundeslösung nicht der Vorzug gegeben werden sollte

1.2 Frage der Bestimmtheit

Zweck und Gegenstand des vorliegenden Konkordatsentwurfs sind äusserst breit gefasst. Trotz wiederholter Bekräftigung des Legalitätsprinzips, des Bestimmtheitsgebots und des Verhältnismässigkeitsgrundsatzes käme das Konkordat einer Blankoermächtigung für den Datenaustausch im Polizeibereich gleich, welche den verfassungsrechtlichen Anforderungen u.E. nicht genügt. Da zudem weder die Kategorien der zu bearbeitenden Daten (Art. 7 Abs. 3) noch die zulässigen Datenbearbeitungsvorgänge (Art. 20) abschliessend aufgeführt sind, können innerhalb des äussert weiten Anwendungsbereichs (Art. 3) grundsätzlich sämtliche Daten auf beinahe jede erdenkliche Weise bearbeitet werden. Wohl müssen pro gemeinsame Datenbank die Datenbearbeitungsvorgänge näher definiert werden, dies geschieht aber wie gezeigt auf Verordnungsstufe, bzw. für die Austauschplattform im von der operativen Versammlung der PTI erlassenen Betriebsreglement, und damit auf einer Normstufe, die u.E. nicht ausreicht.

Die in den gemeinsamen Datenbanken möglichen Datenbearbeitungen können erhebliche Grundrechtseingriffe für die betroffenen Personen darstellen, die erforderliche Normstufe und die Regelungsdichte müssen der Eingriffsschwere angepasst sein. Dies erscheint vorliegend nicht gegeben, da der Entwurf den zulässigen Datenbearbeitungen keine echte Grenze setzt. Eine zulässige Gesetzesdelegation an den Verordnungsgeber setzt voraus, dass sich die Delegation auf eine bestimmte, genau umschriebene Materie beschränkt und dessen Umfang klar begrenzt sein muss. Gerade diesen Anforderungen vermag der aktuelle Konkordatsentwurf aufgrund seiner sehr weiten Zweckausrichtung jedoch nicht zu genügen.

1.3 Regelung der Verantwortung

Die Regelung der Verantwortlichkeiten und die damit verbundenen Pflichten sind u.E. nicht genügen klar normiert. Für jede Abfrageplattform oder eine gemeinsame Datenbank ist zwingend ein Gesamtverantwortlicher zu definieren und es ist zu normieren, welche Aufgaben er in seiner

Rolle zu erfüllen hat. Gleichfalls erscheint die Rolle des Leistungserbringers nicht vollständig geklärt. Die kantonalen Datenschutzgesetze wie auch das Bundesdatenschutzgesetz verwenden typischerweise die Unterscheidung zwischen dem verantwortlichen öffentlichen Organ («Der/die Verantwortliche») und einer Auftragsdatenbearbeiterin. Die Verantwortlichen entscheiden über den Umfang, die Zwecke und die Mittel und somit auch über die Angemessenheit der Sicherheitsmassnahmen der Datenbearbeitung, die Auftragsdatenbearbeiterinnen setzen dies um. Wir gehen davon aus, dass die Leistungserbringerin eine Auftragsdatenbearbeiterin ist, allerdings passt diese Rolle nicht vollständig auf die im Entwurf vorgesehene Rolle.

2 Bemerkungen zu einzelnen Bestimmungen

Die folgende Liste erhebt nicht den Anspruch auf Vollständigkeit, wir haben eine Auswahl der uns am wichtigsten erscheinenden Punkte vorgenommen. Einige der nachfolgenden Anregungen haben einen Bezug zu den allgemeinen Bemerkungen.

2.1 Art. 1 Abs. 2

Die Zwecke nach Art. 1 Abs. 1 sind u.E. einzuschränken:

lit. a: sollte auf die Gewährleistung der öffentlichen Sicherheit beschränkt werden. Die «öffentliche Ordnung» umfasst viele Gefahren von geringer Intensität, die einen solch weitläufigen Datenaustausch nicht rechtfertigen.

lit. b: Ist u.E. einzuschränken. Grundsätzlich sollte sich das Konkordat auf die repressive Polizeitätigkeit beschränken. Die präventive Polizeitätigkeit ist nur im Rahmen eines abschliessenden Kataloges von besonders schwerwiegenden Verbrechen zu erfassen. Als Orientierung kann etwa der Katalog in Art. 260bis StGB dienen.

2.2 Art. 3 lit. h

lit. h: könnte ersatzlos gestrichen werden. Bei Sach- und Personenfahndungen greift lit. d.

2.3 Art. 4

Allgemein: Die Regelungen des anwendbaren Rechts sind kompliziert, uneinheitlich und zudem teils davon abhängig, ob der Bund beteiligt ist oder nicht (vgl. Art. 10 Abs. 4). Wir empfehlen, hierzu eine klarere Regelung zu finden.

2.4 Art. 5 Abs. 9

Es ist unklar, ob der Leistungserbringer ein «Verantwortlicher» im Sinne des Datenschutzrechts ist oder ein «Auftragsbearbeiter». Die Definition ist zudem unvollständig, weil sie «Leistungen» nennt, die ihrerseits nicht definiert sind (welche Leistungen, in wessen Auftrag etc.). Wir empfehlen eine Präzisierung der Definition (vgl. Ziff. 1.3).

2.5 Art. 7 Abs. 3

Aufgrund der Offenheit des Regelungsgehalts des Konkordats und der Tragweite der Regelungen erscheint uns die Delegation des Erlasses weiterer Datenkategorien auf die Ebene der Betriebsverordnungen nicht statthaft. Auf den Begriff «insbesondere» ist deshalb zu verzichten (vgl. Ziff. 1.2).

2.6 Art. 9 Abs. 3 und 4

Während Abs. 3 für die Nutzung der Abfrageplattform im Sinne einer Gegenrechtsklausel den Anschluss von «eigenen entsprechenden» Informationssystemen voraussetzt, überlässt Abs. 4 die Auswahl der Systeme den Teilnehmenden. Damit der Aspekt des Gegenrechts korrekt umgesetzt wird, ist im Betriebsreglement zu beschreiben, welche Mindestanforderungen die Teilnehmenden beim Anschluss ihrer Systeme zu erfüllen haben.

2.7 Art. 10 Abs. 1

Die *Gesamtverantwortung* für POLAP ist im Konkordat ausdrücklich zu regeln. Gemäss Bemerkung zu Art. 10 Abs. 4 liegt diese beim Fedpol. Die Gesamtverantwortung für die Austauschplattform umfasst u.a. technische Vorgaben für den Anschluss der Quellsysteme, die Verantwortung für das Benutzermanagement (IAM), die Verantwortung für die sichere Datenübermittlung sowie Vorgaben zur Protokollierung sowie Kontrolle der Einhaltung der Vorgaben.

2.8 Art. 10 Abs. 3

Diese Regelung trägt den Interessen der betroffenen Personen ungenügend Rechnung: Sinn und Zweck von POLAP ist die Informationskumulierung (durch Austausch) aus verschiedenen Quellsystemen – mit den entsprechenden Folgen für die betroffenen Personen (Täter, Opfer etc.). Es ist fraglich, wie diesem Umstand im Rahmen des Auskunftsrechts Rechnung getragen wird. Die Auskunft nur beim Verantwortlichen für ein einzelnes Quell- bzw. Informationssystem gibt nur eine Teilauskunft. Wie erhalten die betroffenen Personen die Gesamtübersicht über die sie betreffenden Abfragen bzw. «Einsichten» über POLAP? Bei wem und nach welchem anwendbaren Datenschutzrecht?

2.9 Art. 10 Abs. 5

Die Protokollierung von Datenbekanntgaben über die Abfrageplattform sollte einheitlich geregelt sein (auch mit Blick auf Art. 11 und die Rechte der betroffenen Personen). Die Regelung muss vorsehen, dass Suchanfragen protokolliert und deren Rechtmässigkeit mittels periodischer Stichproben überprüft werden können. Zudem ist festzulegen, welche Angaben die abfragende Stelle mitliefern muss, damit eine eindeutige Identifikation der abfragenden Person möglich ist. Zu prüfen ist sodann die Normierung der Konsequenzen bei der Feststellung von unrechtmässigen Zugriffen.

2.10 Art. 13 Abs. 1

Die Rolle des Leistungserbringers ist nicht vollständig geklärt. Wenn er die Rolle eines Auftragsdatenbearbeiters hat, sollte es nicht an ihm liegen, ein Betriebsreglement zu erlassen. Nach Art. 5 Abs. 9 ist er (lediglich) «verantwortlich» für die Umsetzung. Das Betriebsreglement muss u.E. vom Gesamtverantwortlichen – d.h. Fedpol – erlassen werden (vgl. Ziff. 1.3).

Art. 16 Abs. 1: Die Formulierung « (...) Können Datenbanksysteme durch einen Leistungserbringer schaffen» ist bezüglich den damit verbundenen Verantwortlichkeiten unklar.

2.11 Art. 17 Abs. 3

Da der Anwendungsbereich des Konkordats sowie die dadurch ermöglichten Bearbeitungsvorgänge ausserordentlich weit ist, ist zu erwarten, dass in den konkreten Datenbanken Datenbearbeitungen vorgesehen werden, die einer formellgesetzlichen Grundlage bedürfen. Diese Bestimmung erweckt den Anschein, dass das Konkordat diese formellgesetzliche Grundlage für alle Arten von Datenbearbeitungen selber darstelle, und nicht nur die Teilnahme am Austausch, was u.E. wegen der mangelnden Bestimmtheit nicht zutrifft (vgl. Ziff. 1.1/1.2).

2.12 Art. 18 lit. d und e

Auch für gemeinsame Datenbanksysteme ist die Gesamtverantwortung zu regeln (vgl. Bemerkungen zu Art. 10 Abs. 1) und der Gesamtsicht (vgl. Bemerkungen zu Art. 10 Abs. 3) Rechnung zu tragen. Dies ist in den Erläuterungen festzuhalten.

2.13 Art. 20 Abs. 1

Für die Formen der Datenbearbeitungen, die hier benannt sind, kann diese Beschreibung resp. Begründung kaum genügen. Alle Buchstaben umfassen die am weitesten in die Grundrechte eingreifenden Datenbearbeitungen (bspw. Profiling) und erfordern je sehr spezifische regulatorische Auseinandersetzungen mit den Techniken bezogen auf die jeweiligen Anwendungszwecke, andernfalls wird hier ein Blankocheck für jede Polizeiarbeit in sämtlichen polizeilichen Tätigkeiten ausgestellt.

2.14 Art. 21 Abs. b und c

Gemäss Art. 30 Abs. 1 stehen alle gemeinsamen Datenbanksysteme allen Teilnehmern offen, so dass sich das anwendbare Recht immer nach der PTI-Vereinbarung richten würde (lit. b). Was ist mit «regionalem Betrieb» gemeint und wann kommt lit. c demnach zur Anwendung?

2.15 Art. 22

Die Bestimmung ist unklar: Die verwendeten Begriffe sind unbestimmt und die PTI-Vereinbarung enthält keine Vorschriften über die «Organisation», den «Betrieb» und die «Abwicklung» von gemeinsamen Datenbanken.

2.16 Art. 23

Abs. 1 und 2: Hier wird (erneut) nicht klar, wer der Verantwortliche ist. Laut Erläuterungen zu Abs. 1 wird mit dem Leistungserbringer (als «Verantwortlichem»?) die zentrale Stelle des jeweiligen Informationssystems informiert. Abs. 2 unterscheidet dann wieder zwischen Verantwortlichem und Leistungserbringer.

2.17 Art. 28 Abs. 2

Polizeidaten sind regelmässig besonders sensitiv und von erhöhtem Schutzbedarf. Deshalb sollte eine Auslagerung ins Ausland nur ausnahmsweise und aus triftigen Gründen, d.h. wichtigen öffentlichen Interessen, erfolgen. Reine Kosten- und Effizienzgründe reichen dafür nicht aus (rein finanzielle Interessen stellen u.E. keine tauglichen öffentlichen Interessen zur Rechtfertigung eines Grundrechtseingriffes nach Art. 36 BV dar).

2.18 Art. 34

Abs. 2: Die Erläuterungen sprechen von einer Ermächtigung der strategischen Versammlung zum Erlass rechtsetzender Bestimmungen. Dies geht weit über den Begriff der «einfachen Berichtigung, die keine materielle Rechtswirkung haben» hinaus. Die Tragweite der Delegation ist unklar.

In welcher Form können die Kantone eine Nichtanwendbarkeit dieser Bestimmung vorsehen? Und was ist die Folge, wenn einzelne Kantone davon Gebrauch machen?

Wir danken für die Berücksichtigung dieser Anliegen in der kantonsinternen Stellungnahme und stehen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Beat Rudin

Datenschutzbeauftragter des Kantons Basel-Stadt

Beat Rudin, Prof. (em.) Dr. iur., Advokat
Datenschutzbeauftragter
Henric Petri-Strasse 15, Postfach 205
CH-4010 Basel

Tel: +41 61 201 16 40
direkt: +41 61 201 16 42
E-Mail: beat.rudin@dsb.bs.ch
www.dsb.bs.ch

Per E-Mail an: <Politikreferat@jsd.bs.ch>

Politikreferat
Justiz- und Sicherheitsdepartement des
Kantons Basel-Stadt

Basel, 8. Februar 2024

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme / Stellungnahme

Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, zum vorliegenden Geschäft Stellung nehmen zu können. Unsere Stellungnahme stützt sich auf Vorbereitungen im Rahmen der Arbeitsgruppe «Sicherheit» von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, und ist insbesondere mit der Aufsichtsstelle Datenschutz des Kantons Basel-Landschaft abgestimmt.

1 Allgemeines

Die Vorlage der KKPKS wurde durch Mitglieder der Konferenz der Schweizerischen Datenschutzbeauftragten (privatim) ebenfalls einer eingehenden Analyse unterzogen. privatim wird eine detaillierte Vernehmlassungsantwort verfassen und der KKPKS zustellen. Wir beschränken uns an dieser Stelle auf die aus unserer Sicht für unsere Kanton wichtigsten datenschutzrechtlichen Aspekte.

1.1 Form der Rechtsetzung

Die gewählte Form des rechtsetzenden Konkordats für die Schaffung eines einheitlichen Polizeidatenraums hat zum Ziel, einheitliche Rechtsgrundlagen für die (teilnehmenden) Kantone für den Austausch von Daten, gemäss dem vorliegenden Entwurf aber auch über die Datenbearbeitung selber in gemeinsamen Datenbanken zu schaffen. Die derzeit bestehenden Rechtsgrundlagen in den kantonalen Polizeigesetzen sind in vieler Hinsicht uneinheitlich, und führen in der Praxis zu Auslegungsproblemen. Insofern begrüsst der Datenschutzbeauftragte grundsätzlich eine Vereinheitlichung, da klare Regeln für die Bearbeitung von Personendaten (inkl. Datenaustausch) eine hohe Bedeutung haben. Aufgrund der erfahrungsgemäss nicht einfach durchzuführenden Anpassung eines Konkordates enthält der vorliegende Entwurf zahlreichreiche erhebliche Rechtsfragen, deren Regelung auf Verordnungsebene erfolgen soll, was zu einer geringeren demokratischen Legitimation führt (unter der Annahme, dass für diese Fragen die Verordnung überhaupt die ausreichende Normstufe ist). Vorgesehen ist, dass die strategische Versammlung der PTI die Verordnungen für die spezifischen gemeinsamen Datenbanken erlassen soll, die dann durch die einzelnen Kantone genehmigt werden müssen (Art. 17 Abs. 2 f.). Den Kantonen wird empfohlen, die Kompetenz zur Genehmigung der Betriebsverordnungen an ihre Vertretung in der strategischen

Versammlung der PTI zu delegieren (Erl. Bericht, S. 15). Dies ist gemäss Art. 6. Abs. 2 PTI-Vereinbarung die kantonale Justiz- und Polizeidirektorin. Damit haben das Volk und die Parlamente nach Inkrafttreten des Konkordats wenig bis keinen Einfluss mehr auf die Regelungsmaterie, die aber in vielen Fällen derart wichtige Regelungen enthält, die eigentlich auf Stufe Gesetz gehörten.

Der Bund kann der vorliegenden Vereinbarung nicht beitreten, allerdings ist einerseits vorgesehen, dass fedpol die gemeinsame Abfrageplattform betreibt, und andererseits, dass sich der Bund einzelnen gemeinsamen Datenbanken durch die Übernahme der Betriebsverordnung bzw. den Abschluss einer Leistungsvereinbarung anschliessen kann. Der Bund ist somit aktiver Teilnehmer beim Austausch von Polizeidaten und dem Betrieb von gemeinsamen Datenbanken, obwohl das Polizeirecht in der Kompetenz der Kantone liegt. Er hat es bisher mit Verweis auf seine fehlende Rechtsetzungskompetent abgelehnt, gesetzgeberisch tätig zu werden. Ende letzten Jahres hat der Nationalrat einer Motion seiner sicherheitspolitischen Kommission zugestimmt, die entsprechenden Verfassungsgrundlagen zu schaffen, um diese Materie regeln zu können.

Eine Regelung in einem Bundesgesetz sowie in vom Bundesrat erlassenen Verordnungen genösse u.E. wesentlich mehr demokratischen Rückhalt als die vorliegende Variante. Wir regen an zu prüfen, ob einer Bundeslösung nicht der Vorzug gegeben werden sollte

1.2 Frage der Bestimmtheit

Zweck und Gegenstand des vorliegenden Konkordatsentwurfs sind äusserst breit gefasst. Trotz wiederholter Bekräftigung des Legalitätsprinzips, des Bestimmtheitsgebots und des Verhältnismässigkeitsgrundsatzes käme das Konkordat einer Blankoermächtigung für den Datenaustausch im Polizeibereich gleich, welche den verfassungsrechtlichen Anforderungen u.E. nicht genügt. Da zudem weder die Kategorien der zu bearbeitenden Daten (Art. 7 Abs. 3) noch die zulässigen Datenbearbeitungsvorgänge (Art. 20) abschliessend aufgeführt sind, können innerhalb des äussert weiten Anwendungsbereichs (Art. 3) grundsätzlich sämtliche Daten auf beinahe jede erdenkliche Weise bearbeitet werden. Wohl müssen pro gemeinsame Datenbank die Datenbearbeitungsvorgänge näher definiert werden, dies geschieht aber wie gezeigt auf Verordnungsstufe, bzw. für die Austauschplattform im von der operativen Versammlung der PTI erlassenen Betriebsreglement, und damit auf einer Normstufe, die u.E. nicht ausreicht.

Die in den gemeinsamen Datenbanken möglichen Datenbearbeitungen können erhebliche Grundrechtseingriffe für die betroffenen Personen darstellen, die erforderliche Normstufe und die Regelungsdichte müssen der Eingriffsschwere angepasst sein. Dies erscheint vorliegend nicht gegeben, da der Entwurf den zulässigen Datenbearbeitungen keine echte Grenze setzt. Eine zulässige Gesetzesdelegation an den Verordnungsgeber setzt voraus, dass sich die Delegation auf eine bestimmte, genau umschriebene Materie beschränkt und dessen Umfang klar begrenzt sein muss. Gerade diesen Anforderungen vermag der aktuelle Konkordatsentwurf aufgrund seiner sehr weiten Zweckausrichtung jedoch nicht zu genügen.

1.3 Regelung der Verantwortung

Die Regelung der Verantwortlichkeiten und die damit verbundenen Pflichten sind u.E. nicht genügen klar normiert. Für jede Abfrageplattform oder eine gemeinsame Datenbank ist zwingend ein Gesamtverantwortlicher zu definieren und es ist zu normieren, welche Aufgaben er in seiner

Rolle zu erfüllen hat. Gleichfalls erscheint die Rolle des Leistungserbringers nicht vollständig geklärt. Die kantonalen Datenschutzgesetze wie auch das Bundesdatenschutzgesetz verwenden typischerweise die Unterscheidung zwischen dem verantwortlichen öffentlichen Organ («Der/die Verantwortliche») und einer Auftragsdatenbearbeiterin. Die Verantwortlichen entscheiden über den Umfang, die Zwecke und die Mittel und somit auch über die Angemessenheit der Sicherheitsmassnahmen der Datenbearbeitung, die Auftragsdatenbearbeiterinnen setzen dies um. Wir gehen davon aus, dass die Leistungserbringerin eine Auftragsdatenbearbeiterin ist, allerdings passt diese Rolle nicht vollständig auf die im Entwurf vorgesehene Rolle.

2 Bemerkungen zu einzelnen Bestimmungen

Die folgende Liste erhebt nicht den Anspruch auf Vollständigkeit, wir haben eine Auswahl der uns am wichtigsten erscheinenden Punkte vorgenommen. Einige der nachfolgenden Anregungen haben einen Bezug zu den allgemeinen Bemerkungen.

2.1 Art. 1 Abs. 2

Die Zwecke nach Art. 1 Abs. 1 sind u.E. einzuschränken:

lit. a: sollte auf die Gewährleistung der öffentlichen Sicherheit beschränkt werden. Die «öffentliche Ordnung» umfasst viele Gefahren von geringer Intensität, die einen solch weitläufigen Datenaustausch nicht rechtfertigen.

lit. b: Ist u.E. einzuschränken. Grundsätzlich sollte sich das Konkordat auf die repressive Polizeitätigkeit beschränken. Die präventive Polizeitätigkeit ist nur im Rahmen eines abschliessenden Kataloges von besonders schwerwiegenden Verbrechen zu erfassen. Als Orientierung kann etwa der Katalog in Art. 260bis StGB dienen.

2.2 Art. 3 lit. h

lit. h: könnte ersatzlos gestrichen werden. Bei Sach- und Personenfahndungen greift lit. d.

2.3 Art. 4

Allgemein: Die Regelungen des anwendbaren Rechts sind kompliziert, uneinheitlich und zudem teils davon abhängig, ob der Bund beteiligt ist oder nicht (vgl. Art. 10 Abs. 4). Wir empfehlen, hierzu eine klarere Regelung zu finden.

2.4 Art. 5 Abs. 9

Es ist unklar, ob der Leistungserbringer ein «Verantwortlicher» im Sinne des Datenschutzrechts ist oder ein «Auftragsbearbeiter». Die Definition ist zudem unvollständig, weil sie «Leistungen» nennt, die ihrerseits nicht definiert sind (welche Leistungen, in wessen Auftrag etc.). Wir empfehlen eine Präzisierung der Definition (vgl. Ziff. 1.3).

2.5 Art. 7 Abs. 3

Aufgrund der Offenheit des Regelungsgehalts des Konkordats und der Tragweite der Regelungen erscheint uns die Delegation des Erlasses weiterer Datenkategorien auf die Ebene der Betriebsverordnungen nicht statthaft. Auf den Begriff «insbesondere» ist deshalb zu verzichten (vgl. Ziff. 1.2).

2.6 Art. 9 Abs. 3 und 4

Während Abs. 3 für die Nutzung der Abfrageplattform im Sinne einer Gegenrechtsklausel den Anschluss von «eigenen entsprechenden» Informationssystemen voraussetzt, überlässt Abs. 4 die Auswahl der Systeme den Teilnehmenden. Damit der Aspekt des Gegenrechts korrekt umgesetzt wird, ist im Betriebsreglement zu beschreiben, welche Mindestanforderungen die Teilnehmenden beim Anschluss ihrer Systeme zu erfüllen haben.

2.7 Art. 10 Abs. 1

Die *Gesamtverantwortung* für POLAP ist im Konkordat ausdrücklich zu regeln. Gemäss Bemerkung zu Art. 10 Abs. 4 liegt diese beim Fedpol. Die Gesamtverantwortung für die Austauschplattform umfasst u.a. technische Vorgaben für den Anschluss der Quellsysteme, die Verantwortung für das Benutzermanagement (IAM), die Verantwortung für die sichere Datenübermittlung sowie Vorgaben zur Protokollierung sowie Kontrolle der Einhaltung der Vorgaben.

2.8 Art. 10 Abs. 3

Diese Regelung trägt den Interessen der betroffenen Personen ungenügend Rechnung: Sinn und Zweck von POLAP ist die Informationskumulierung (durch Austausch) aus verschiedenen Quellsystemen – mit den entsprechenden Folgen für die betroffenen Personen (Täter, Opfer etc.). Es ist fraglich, wie diesem Umstand im Rahmen des Auskunftsrechts Rechnung getragen wird. Die Auskunft nur beim Verantwortlichen für ein einzelnes Quell- bzw. Informationssystem gibt nur eine Teilauskunft. Wie erhalten die betroffenen Personen die Gesamtübersicht über die sie betreffenden Abfragen bzw. «Einsichten» über POLAP? Bei wem und nach welchem anwendbaren Datenschutzrecht?

2.9 Art. 10 Abs. 5

Die Protokollierung von Datenbekanntgaben über die Abfrageplattform sollte einheitlich geregelt sein (auch mit Blick auf Art. 11 und die Rechte der betroffenen Personen). Die Regelung muss vorsehen, dass Suchanfragen protokolliert und deren Rechtmässigkeit mittels periodischer Stichproben überprüft werden können. Zudem ist festzulegen, welche Angaben die abfragende Stelle mitliefern muss, damit eine eindeutige Identifikation der abfragenden Person möglich ist. Zu prüfen ist sodann die Normierung der Konsequenzen bei der Feststellung von unrechtmässigen Zugriffen.

2.10 Art. 13 Abs. 1

Die Rolle des Leistungserbringers ist nicht vollständig geklärt. Wenn er die Rolle eines Auftragsdatenbearbeiters hat, sollte es nicht an ihm liegen, ein Betriebsreglement zu erlassen. Nach Art. 5 Abs. 9 ist er (lediglich) «verantwortlich» für die Umsetzung. Das Betriebsreglement muss u.E. vom Gesamtverantwortlichen – d.h. Fedpol – erlassen werden (vgl. Ziff. 1.3).

Art. 16 Abs. 1: Die Formulierung « (…) Können Datenbanksysteme durch einen Leistungserbringer schaffen» ist bezüglich den damit verbundenen Verantwortlichkeiten unklar.

2.11 Art. 17 Abs. 3

Da der Anwendungsbereich des Konkordats sowie die dadurch ermöglichten Bearbeitungsvorgänge ausserordentlich weit ist, ist zu erwarten, dass in den konkreten Datenbanken Datenbearbeitungen vorgesehen werden, die einer formellgesetzlichen Grundlage bedürfen. Diese Bestimmung erweckt den Anschein, dass das Konkordat diese formellgesetzliche Grundlage für alle Arten von Datenbearbeitungen selber darstelle, und nicht nur die Teilnahme am Austausch, was u.E. wegen der mangelnden Bestimmtheit nicht zutrifft (vgl. Ziff. 1.1/1.2).

2.12 Art. 18 lit. d und e

Auch für gemeinsame Datenbanksysteme ist die Gesamtverantwortung zu regeln (vgl. Bemerkungen zu Art. 10 Abs. 1) und der Gesamtsicht (vgl. Bemerkungen zu Art. 10 Abs. 3) Rechnung zu tragen. Dies ist in den Erläuterungen festzuhalten.

2.13 Art. 20 Abs. 1

Für die Formen der Datenbearbeitungen, die hier benannt sind, kann diese Beschreibung resp. Begründung kaum genügen. Alle Buchstaben umfassen die am weitesten in die Grundrechte eingreifenden Datenbearbeitungen (bspw. Profiling) und erfordern je sehr spezifische regulatorische Auseinandersetzungen mit den Techniken bezogen auf die jeweiligen Anwendungszwecke, andernfalls wird hier ein Blankocheck für jede Polizeiarbeit in sämtlichen polizeilichen Tätigkeiten ausgestellt.

2.14 Art. 21 Abs. b und c

Gemäss Art. 30 Abs. 1 stehen alle gemeinsamen Datenbanksysteme allen Teilnehmern offen, so dass sich das anwendbare Recht immer nach der PTI-Vereinbarung richten würde (lit. b). Was ist mit «regionalem Betrieb» gemeint und wann kommt lit. c demnach zur Anwendung?

2.15 Art. 22

Die Bestimmung ist unklar: Die verwendeten Begriffe sind unbestimmt und die PTI-Vereinbarung enthält keine Vorschriften über die «Organisation», den «Betrieb» und die «Abwicklung» von gemeinsamen Datenbanken.

2.16 Art. 23

Abs. 1 und 2: Hier wird (erneut) nicht klar, wer der Verantwortliche ist. Laut Erläuterungen zu Abs. 1 wird mit dem Leistungserbringer (als «Verantwortlichem»?) die zentrale Stelle des jeweiligen Informationssystems informiert. Abs. 2 unterscheidet dann wieder zwischen Verantwortlichem und Leistungserbringer.

2.17 Art. 28 Abs. 2

Polizeidaten sind regelmässig besonders sensitiv und von erhöhtem Schutzbedarf. Deshalb sollte eine Auslagerung ins Ausland nur ausnahmsweise und aus triftigen Gründen, d.h. wichtigen öffentlichen Interessen, erfolgen. Reine Kosten- und Effizienzgründe reichen dafür nicht aus (rein finanzielle Interessen stellen u.E. keine tauglichen öffentlichen Interessen zur Rechtfertigung eines Grundrechtseingriffes nach Art. 36 BV dar).

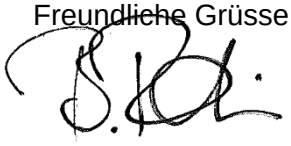
2.18 Art. 34

Abs. 2: Die Erläuterungen sprechen von einer Ermächtigung der strategischen Versammlung zum Erlass rechtsetzender Bestimmungen. Dies geht weit über den Begriff der «einfachen Berichtigung, die keine materielle Rechtswirkung haben» hinaus. Die Tragweite der Delegation ist unklar.

In welcher Form können die Kantone eine Nichtanwendbarkeit dieser Bestimmung vorsehen? Und was ist die Folge, wenn einzelne Kantone davon Gebrauch machen?

Wir danken für die Berücksichtigung dieser Anliegen in der kantonsinternen Stellungnahme und stehen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse



Beat Rudin

Kanton Bern
Canton de Berne

Regierungsrat

Postgasse 68
Postfach
3000 Bern 8
info.regierungsrat@be.ch
www.be.ch/rr

Staatskanzlei, Postfach, 3000 Bern 8

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und – direktoren (KKJPD)

Per E-Mail (in Word und PDF) an:
info@kkjpd.ch

RRB Nr.:	97/2024	14. Februar 2024
Direktion:	Sicherheitsdirektion	
Klassifizierung:	Nicht klassifiziert	

Vernehmlassung der KKJPD: Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme
Stellungnahme des Kantons Bern

Sehr geehrte Frau Co-Präsidentin
Sehr geehrter Herr Co-Präsident
Sehr geehrte Damen und Herren

Der Regierungsrat des Kantons Bern dankt Ihnen für die Gelegenheit zur Stellungnahme.

1. Grundsätzliches

Der Regierungsrat begrüsst die Stossrichtung des Konkordats. Es ist in der Tat an der Zeit, eine Rechtsgrundlage für den interkantonalen Datenaustausch zu schaffen. Die Kriminalität hört nicht an den Kantonsgrenzen auf und ist mitunter interkantonal und international organisiert. Bei der hohen Mobilität der Täterschaft sind für eine moderne Polizeiarbeit Informationen und der gesicherte Austausch dieser Informationen unerlässlich. Auch die angestrebte Vereinfachung der Schaffung gemeinsamer Datenbanksysteme wird im Grundsatz begrüsst.

Die positiven Entwicklungen auf Bundesebene (Motionen 18.3592 und 23.4311) sollten nach Auffassung des Regierungsrates nicht dazu führen, dass das vorliegende interkantonale Vorhaben zurückgestellt wird. Es sollte unabhängig von der Entwicklung auf Bundesebene vorangetrieben werden.

2. Anträge

2.1 Vorgehen

Der Vereinbarungsentwurf und insbesondere Kapitel 3 sind gutachterlich auf ihre Verfassungsmässigkeit hin zu untersuchen.

Begründung

Der Vereinbarungsentwurf widmet sich zwei Teilbereichen. Neben dem interkantonalen Datenaustausch über eine gemeinsame Abfrageplattform sieht er auch Rahmenbestimmungen für gemeinsame Datenbanksysteme vor. Mit Kapitel 3 des Vereinbarungsentwurfs (Gemeinsame Datenbanksysteme) betreten die Kantone nach Einschätzung des Regierungsrats in rechtlicher Hinsicht noch wenig ausgetretene Pfade. Entsprechend erachtet es der Regierungsrat als unerlässlich, dass die KKJPD und die KKPKS den Regelungsvorschlag gutachterlich auf seine Verfassungsmässigkeit hin beurteilen lassen. Insbesondere sind dabei die Vereinbarkeit der Vereinbarung mit der verfassungsrechtlichen Kompetenzordnung und die hinreichende Bestimmtheit der (gesetzesvertretenden) Rechtsgrundlagen für schwere Grundrechtseingriffe von Interesse. Ohne ein solches Gutachten erblickt der Regierungsrat Risiken im Ratifizierungsprozess in den 26 Kantonsparlamenten.

2.2 Antrag zu Artikel 7

Artikel 7 Absatz 3 Buchstabe i sei zu ergänzen, damit auch relevante Daten zu Informationsquellen bearbeitet werden dürfen.

Begründung

Nicht nur die Angaben von, sondern auch die relevanten Daten zu Informationsquellen müssen von der Polizei bearbeitet werden dürfen.

2.3 Antrag zu Artikel 9

Artikel 9 Absatz 1 zweiter Satz sei zu streichen.

Begründung

Dass für die Abfrageplattform durch die operative Versammlung PTI ein Betriebsreglement erlassen wird, ergibt sich (sinnvollerweise) aus Artikel 13 Absatz 1 und muss entsprechend nicht bereits in Artikel 9 Absatz 1 aufgeführt werden.

2.4 Antrag zu Artikel 10

Es sei die Verankerung der Zuständigkeit für die datenschutzrechtliche Gesamtverantwortung und die Aufsicht sowie das anwendbare Datenschutzrecht für die Abfrageplattform zu regeln im Fall, wenn der Bund sich nicht an der Abfrageplattform beteiligt oder diese betreibt.

Begründung

Artikel 10 Absatz 4 regelt lediglich den Fall, wenn der Bund sich an der Abfrageplattform beteiligt oder diese betreibt. Der Regierungsrat nimmt zur Kenntnis, dass angestrebt wird, dass der Bund (fedpol) die Abfrageplattform errichten und betreiben soll. Theoretisch ist jedoch auch der

Fall denkbar, dass der Bund sich nicht beteiligt und die Errichtung und den Betrieb der Abfrageplattform den Kantonen überlässt. Bei der Gesamtverantwortung, der Aufsicht und beim anwendbaren Datenschutzrecht handelt es sich um zentrale Rechtsfragen, die das Konkordat auch für diesen Fall klären müsste.

2.5 Antrag zu Artikel 10

Es ist in der Vereinbarung zu klären, ob beim Abruf die Daten nur «gesichtet» oder auch direkt anderweitig bearbeitet werden können (z.B. Speicherung). Zudem sei zu klären, ob es nicht einer periodischen Kontrolle der Zugriffe bedürfte.

Begründung

Im erläuternden Bericht zu Art. 10 Abs. 1 des Entwurfs steht, dass die Daten aus den Quellsystemen nur zwecks «Sichtung» angezeigt werden können. Aus dem Vereinbarungsentwurf selbst geht diese Einschränkung jedoch nicht hervor.

2.6 Antrag zu Artikel 27

Die Erläuterungen zu Artikel 27 Absatz 3 seien insofern zu ergänzen, als dass jene Stelle definiert wird, welche die Auskunftsstelle festlegt.

Begründung

Weder Artikel 18 noch Artikel 19 halten fest, dass die Auskunftsstelle in der Betriebsverordnung und damit durch den strategischen Ausschuss PTI oder im Betriebsreglement, also die operative Versammlung PTI, definiert wird.

2.7 Antrag zum erläuternden Bericht zu Artikel 8 Absatz 2 und 3

Der erläuternde Bericht zu Artikel 8 Absatz 2 und 3 sei anzupassen.

Begründung

Soweit eine Haftung des Leistungserbringers besteht, soll gemäss Artikel 8 Absatz 2 anstelle der Staatshaftung die Beitragsverpflichtung nach der PTI-Vereinbarung treten. Die PTI-Vereinbarung sieht in Artikel 25 Absatz 7 vor, dass betreffend Haftung und Arbeitsverhältnisse das Verfahrensrecht des Kantons Bern gilt. In Artikel 8 Absatz 2 der «Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme» wird jedoch festgehalten, dass wenn eine Haftung des Leistungserbringers besteht, diese nach dem Prozessrecht des Sitzkantons des Leistungserbringers geltend zu machen ist. Gemäss Artikel 5 Ziffer 9 der «Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme» kann Leistungserbringer sowohl die PTI als auch ein bezeichneter Dritter sein. Hat der bezeichnete Dritte seinen Sitz nicht im Kanton Bern, sondern beispielsweise im Kanton Zürich, wäre das Prozessrecht des Kantons Zürichs anwendbar. Wir regen an, den erläuternden Bericht von Artikel 8 Absatz 2 zu ergänzen,

damit klar wird, ob nun Artikel 25 Absatz 7 der PTI-Vereinbarung oder Artikel 8 Absatz 2 Vorrang geniesst.

Artikel 8 Absatz 3 sieht vor, dass das Klagerecht des haftbaren Teilnehmenden gegen Mitarbeitende eines anderen Teilnehmenden ausgeschlossen ist. Der Regierungsrat geht davon aus, dass es sich dabei um Fälle handelt, bei den Teilnehmende gegenüber Dritten haftbar werden, weil diese in ihren Rechten verletzt worden sind. Dies könnte im erläuternden Bericht noch etwas ausführlicher dargestellt werden. Zu prüfen wäre auch, ob allenfalls auf jene Konstellationen einzugehen ist, in welchen Teilnehmende selbst durch Mitarbeitende von anderen Teilnehmenden geschädigt werden. In diesem Fall müsste auch der Absatz 3 noch ergänzt werden (z.B. «Das Klagerecht des haftbaren bzw. geschädigten Teilnehmenden [...].»).

2.8 Antrag zum erläuternden Bericht S. 25

Der erläuternde Bericht zu Artikel 12 Absatz 1 und 2 sei anzupassen.

Begründung

Artikel 12 Absatz 1 sieht vor, dass sich die Finanzierung, und damit die möglichen Kostenschlüssel, nach der VPTI richten, konkret demnach nach Artikel 22 Absatz 2 VPTI. Die möglichen Kostenschlüssel sind somit abschliessend definiert und in der separaten Vereinbarung kann von diesem Grundsatz nicht mehr abgewichen werden, wie es der erläuternde Bericht zu Artikel 12 Absatz 1 fälschlicherweise darstellt. Wir bitten Sie, den Bericht insofern zu korrigieren.

2.9 Antrag zum erläuternden Bericht zu Artikel 17 Absatz 4 und 34 Absatz 2

Der Bericht sei im Sinne der nachfolgenden Hinweise zu präzisieren.

Begründung

Die Artikel 17 Absatz 4 und 34 Absatz 2 sehen je eine Kompetenzdelegation vor für Änderungen mit untergeordneter materieller Rechtswirkung. Aus Sicht des Regierungsrats sollte hierzu eine Präzisierung im erläuternden Bericht vorgenommen werden, was unter diesen offenen Begriff fallen kann. Insbesondere ist unklar, ob damit auch Auswirkungen ohne direkte Rechtswirkungen – wie beispielsweise Änderungen mit finanziellen bzw. personellen Auswirkungen – gemeint sind.

2.10 Weiteres

Der Regierungsrat begrüsst die vorgeschlagenen Regelungen in Artikel 17 Absatz 3 und 4 sowie in Artikel 34 Absatz 2. Sie vereinfachen zum einen das Verwaltungshandeln (Satz 1) und respektieren gleichzeitig die unterschiedlichen rechtlichen Ausgangslagen in den Kantonen (Satz 2). Die bernische Einführungsgesetzgebung zur vorliegenden Vereinbarung könnte vorsehen, dass der Regierungsrat einfache Berichtigungen ohne materielle Rechtswirkungen im Sinne von Artikel 34 Absatz 2 vornehmen darf (vgl. Art. 69 Absatz 2 der Verfassung des Kan-

tons Bern [KV-BE; BSG 101.1]). Artikel 17 Absatz 4 müsste im Kanton Bern hingegen aller Voraussicht nach für nicht anwendbar erklärt werden, um der Aufgabenzuteilung gemäss Artikel 88 Absatz 2 KV-BE gerecht zu werden.

Zuletzt möchte der Regierungsrat eine allgemeine Bemerkung zu den Kosten anbringen. Das Finanzierungssystem ist zwingend ausgewogen und fair auszugestalten, damit nicht einzelne Kantone den Hauptteil der Kosten tragen müssen, wenn z.B. nur wenige Kantone dem Konkordat beitreten.

Der Regierungsrat dankt Ihnen für die Berücksichtigung seiner Anliegen.

Freundliche Grüsse

Im Namen des Regierungsrates

Philippe Müller
Regierungspräsident

Christoph Auer
Staatsschreiber

Verteiler
- Alle Direktionen
- Staatskanzlei
- Sicherheitskommission des Grossen Rates
- Kommission für Staatspolitik und Aussenbeziehungen des Grossen Rates
- Datenschutzaufsichtsstelle des Kantons Bern

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Zoll und Grenzsicherheit BAZG

CH-3003 Bern, BAZG

Per E-Mail
Konferenz der Kantonalen Justiz- und
Polizeidirektorinnen und -direktoren KKJPD
Haus der Kantone
Speichergasse 6
3001 Bern

Bern, 23. Februar 2024

Vernehmlassung zur Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme

Sehr geehrte Damen und Herren

Die KKJPD hat am 23. November 2023 dazu eingeladen, Stellung zur Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme zu nehmen. Das Bundesamt für Zoll und Grenzsicherheit (BAZG) bedankt sich, im Rahmen der Vernehmlassung angehört zu werden und nimmt dazu wie folgt Stellung:

Das BAZG begrüsst die Bestrebungen für eine interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme. Nach unserer Sicht ist für eine moderne Schweizer Polizeiarbeit neben der operativen Zusammenarbeit auch ein effizienter Austausch polizeilicher Daten wichtig. Eine dazu nötige Vernetzung der Polizeidatenbanken zwischen den Kantonen untereinander sowie – wo sinnvoll bzw. zweckmässig auch mit dem Bund – ist anzustreben. Ein engerer Informationsaustausch unter den Polizeibehörden wirkt sich aus unserer Sicht auch positiv auf die Möglichkeiten der Bekämpfung der grenzüberschreitenden Kriminalität und der Gewährleistung der inneren Sicherheit der Schweiz aus.

Das BAZG versteht die Vorlage dahingehend, dass ein Datenaustausch mit dem Bund gestützt auf diese Vereinbarung zum heutigen Zeitpunkt nicht vorgesehen ist. In diesem Zusammenhang ist die in der Vorlage formulierte Absicht zur Schaffung der notwendigen rechtlichen Grundlagen, damit die Kantone zu einem späteren Zeitpunkt in gleicher Weise mit dem Bund zusammenarbeiten können und der Bund an Informationssystemen teilnehmen kann, zu begrüssen. Ein entsprechendes Interesse an einer künftigen Teilnahme Seitens des Bundes wäre positiv zu werten.

Bundesamt für Zoll und Grenzsicherheit BAZG
Pascal Lüthi
Direktor
Taubenstrasse 16, 3003 Bern
www.bazg.admin.ch

Des Weiteren verweisen wir auf die nachstehenden Anmerkungen und Fragestellungen:

- Das BAZG hat Stand heute keine rechtliche Grundlage, Daten aus Zollstrafverfahren anderen Strafverfolgungsbehörden im Abrufverfahren zur Verfügung zu stellen. Aus unserer Sicht lässt sich aus der Vereinbarung nicht abschliessend ableiten, ob für die geplante gemeinsame Abfrageplattform auch der Austausch von Daten aus Strafverfahren gestützt auf das Bundesgesetz über das Verwaltungsstrafrecht (VStrR; *SR 313.0*) beabsichtigt ist.

- Entsprechen die in Artikel 3 lit. b (auch lit. c, d, oder e) aufgeführten Aufgaben auch jenen Analyseaufgaben des BAZG zur gezielten Ansprache verdächtiger Reisender an der Grenze (frz.: *tâches d'analyse pour le ciblage des voyageurs suspects à la frontière*)? Falls ja, würden wir eine präzisere Formulierung begrüssen.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Bundesamt für Zoll und Grenzsicherheit BAZG

Pascal Lüthi
Direktor

DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
Conférence des directrices et directeurs des départements cantonaux de justice et police
Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia

Per E-Mail an: info@kkjpd.ch

21. Februar 2024

Stellungnahme zur interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme

Sehr geehrte Frau Co-Präsidentin Kayser-Frutschi, sehr geehrter Herr Co-Präsident Ribaux

Am 23. November 2023 eröffnete die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) die Vernehmlassung zur interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme. 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

Die Vereinbarung will eine effiziente Zusammenarbeit der polizeilichen Behörden der

Kantone und Gemeinden und dem Bund. Zu diesem Zweck soll der interkantonale Austausch polizeilicher Daten und der Betrieb gemeinsamer Datenbanksysteme ermöglicht werden. Das Ziel der Vereinbarung ist die Schaffung eines schweizweiten Polizeidatenraums (vgl. erläuternder Bericht, S. 7).

Die schweizweite Datenbearbeitung und der Datenaustausch unter Polizeikorps bergen grosse datenschutzrechtliche Risiken und schwere Grundrechtseingriffe. Wir stehen der Schaffung von einer gemeinsamem Abfrageplattform und gemeinsamen Datenbanksystemen grundsätzlich sehr kritisch gegenüber und lehnen einen schweizweiten Polizeidatenraum ab.

Bund und Kantone verfügen über eine Vielzahl von Datenbanken mit polizeilichen Informationen, die unterschiedlichen Bearbeitungszwecken dienen. Die Möglichkeiten der kantonalen Polizeikorps untereinander auf diese Daten zuzugreifen, sind jedoch zu Recht begrenzt. Öffentliche Organe dürfen Personendaten grundsätzlich nur zu dem Zweck bearbeiten, zu dem sie erhoben wurden. Der automatisierte Informationsaustausch und das Abrufverfahren ohne Einschränkungen und ohne Anforderungen im Einzelfall erachten wir als sehr problematisch. Der uneingeschränkte Zugriff auf zahlreiche bundesweite Datenbanken, ohne dass angegeben werden muss, warum und zu welchem Zweck eine bestimmte Information benötigt wird, birgt ein erhebliches Missbrauchspotenzial. Der erläuternde Bericht erkennt zwar richtigerweise, dass das Bestimmtheitsgebot verlangt, «dass der Datenaustausch in vorhersehbarerweise eingeschränkt wird. Ein pauschaler Datenaustausch, bei welchem die Polizeibehörden sämtliche ihrer Daten in eine Datenbank eingeben oder via Abrufverfahren bekannt geben können, steht dem entgegen» (S. 18). Genau das soll aber mit der polizeilichen Abfrageplattform POLAP mit kantonalen, nationalen und internationalen Polizeidaten eingeführt werden: «Mit einer einzigen online Abfrage können Informationen aus allen angeschlossenen Systemen der Kantone, des Bundes und auch auf internationaler Ebene standardisiert und parallel abgerufen werden» (erläuternder Bericht, S. 11).

Das Erfassen, die Bearbeitung und die Weitergabe besonderer Personendaten stellen einen Eingriff in das in Art. 13 Abs. 1 BV sowie Art. 8 Ziff. 1 EMRK verankerte Recht auf Privatsphäre dar. Es ist zentral, dass dabei die Verhältnismässigkeit des jeweiligen Eingriffs gewahrt wird und konkrete gesetzliche Schranken und Kontrollmechanismen bestehen, um den Schutz vor Missbrauch persönlicher Daten gemäss Art. 13 Abs. 2 BV zu gewährleisten. Diese Grundsätze dürfen dem Bestreben nach einem

umfassenderen Datenaustausch und der Einführung neuer Datenbanksysteme nicht untergeordnet werden. Es liegt aber in der Natur von grossen Datenbanken und Abfrageplattformen, dass darin grosse Mengen an Daten gespeichert werden und viele Personen darauf Zugriff haben (vgl. auch erläuternder Bericht, S. 8). Das erhöht das Missbrauchspotenzial wesentlich. Dafür sind keine genügenden Kontrollmechanismen vorgesehen. Zur Gewährleistung des Grundrechts- und Datenschutzes braucht es aber klare gesetzliche Schranken und Kontrollmechanismen. Die Reichweite des Datenabgleichs muss «im Gesetz sachbezogen eingegrenzt» werden (Urteil des BGer 6B_908/2018 vom 7. Oktober 2019 E.3.3.2). Die Anforderungen an Grundrechtseingriffe und den Umgang mit Personendaten dürfen nicht heruntergesetzt werden.

Der erläuternde Bericht spricht irreführend von der Bekämpfung des Terrorismus und der Schwerstkriminalität, für welche die Vernetzung der polizeilichen Datenbanken unabdingbar sei (erläuternder Bericht, S. 4). Solche Schlagwörter sind symptomatisch für die schlecht oder gar nicht begründete Einführung von immer mehr und ausufernden Überwachungsmöglichkeiten. Während also vermeintlich Terrorismus und Schwerstkriminalität bekämpft werden sollen, bezweckt die Vereinbarung eine effiziente Zusammenarbeit zur Erkennung und Verhinderung von Straftaten (Art. 1 Ziff. 1 lit. b) und sieht keine Beschränkung auf schwere Verbrechen vor. So können im schweizweiten Polizeidatenraum Daten bereits allein für Verkehrskontrollen im Abrufverfahren ausgetauscht werden (Art. 2 lit. h). Der Anwendungsbereich und die Zwecke zur Datenbearbeitung bleiben viel zu offen und unbestimmt. Auch der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) kritisierte in einem Interview der NZZ, dass es jeder Verhältnismässigkeit widerspreche, Daten über Bagatelldelikte auf Vorrat zentral zu bearbeiten. Er spricht von «rechtsstaatlicher Ignoranz», wobei unsere Staatsidee mit Prinzipien wie der Gewaltenteilung oder dem Föderalismus auf Kosten eines «zentralen Datensilos» geopfert werden. Laut dem EDÖB braucht es keine weitere Zentralisierung oder Verknüpfung von Polizeidatenbanken. Stattdessen sei eine Digitalisierung der Amtshilfe nötig, sodass Polizeibehörden ihre Gesuche online stellen können und diese in Standardsituationen automatisiert genehmigt werden können. Wir befürworten die Position des EDÖB. Der geplante Ausbau des automatisierten Informationsaustausches sowie das Abrufverfahren, durch welche Polizist:innen nahezu uneingeschränkt Zugriff auf schweizweite und sogar internationale Datenbanken erhalten, ist sowohl aus grundrechtlicher als auch aus datenschutzrechtlicher Perspektive kritisch zu

beurteilen. Insbesondere eine Anbindung an internationale Informationssysteme (vgl. Art. 9 Ziff. 2) lehnen wir vehement ab.

Parallel zu dieser interkantonalen Vereinbarungen ändern aktuell bereits einige Kantone ihre Polizeigesetze und schaffen darin eine gesetzliche Grundlage, um den Datenaustausch und gemeinsame Datenbanksysteme mit dem Bund, den Kantonen und Gemeinden zu ermöglichen und die Zusammenarbeit mit anderen Polizeikorps und Sicherheitspartnern zu stärken. So z.B. das Polizeigesetz des Kantons Zürich oder Freiburg. Die aktuellen Revisionen der kantonalen Polizeigesetze kranken allesamt an einer Unbestimmtheit und Unverhältnismässigkeit. Es bleibt viel zu unbestimmt, wer unter welchen Voraussetzungen auf welche Daten zugreifen darf, während ausreichende Kontrollmechanismen und Schranken fehlen. Da sich die aktuellen Revisionen der kantonalen Polizeigesetze bereits auf diese Vereinbarung stützen, kommt ihr eine grossen Verantwortung zu. Die Vereinbarung schafft mit ihrer eigenen Unbestimmtheit und Unverhältnismässigkeit aber keinen regulierenden Rahmen für die kantonale Gesetzgebung.

Profiling

Die Vereinbarung sieht zudem die Möglichkeit vor, in gemeinsamen Datenbanken Profiling und Profiling mit hohem Risiko zur Verhinderung und Aufklärung von Straftaten zu betreiben (Art. 20 Ziff. 1 lit. a). Wir lehnen Profiling generell ab. Insgesamt ist nicht zu überblicken, welche Daten davon betroffen sein können und was für Überwachungsmöglichkeiten sich hieraus ergeben. Eine Spezifizierung in der Betriebsverordnung (vgl. erläuternder Bericht, S. 28) ist daher nicht ausreichend. Zudem braucht Profiling durch ein Bundesorgan gemäss Art. 6 Abs. 7 DSG eine ausdrückliche Einwilligung. Auch wenn das DSG für kantonale Behörden nicht anwendbar ist, stützt sich die Vereinbarung mehrfach auf das DSG (vgl. Art. 9 Ziff. 4). Die Anforderungen des DSG an Profiling dürfen nicht herabgesetzt werden.

Schlussbemerkung

Abschliessend ist nochmals zu betonen, dass das Ziel einer effizienteren Zusammenarbeit der Polizeibehörden und weiterer Behörden nicht zulasten der Grundrechte und des Datenschutzes erfolgen darf. Wir lehnen die interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme ab.

DIGITALE | GESELLSCHAFT

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 Anna Walter

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Der Beauftragte

CH-3003 Bern

POST CH AG
EDÖB; EDÖB-A-5ED73401/2

Versand als Anhang
Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
Haus der Kantone
Speichergasse 6
3001 Bern

Ihr Zeichen:
Unser Zeichen: EDÖB-A-5ED73401/2
Sachbearbeiter/in: Frédéric Schoenbett
Bern, 22. Februar 2024

Entwurf für eine interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit zur Stellungnahme zum oben genannten Entwurf. Unsere Anmerkungen finden Sie untenstehend:

Vorbemerkungen

Der Bund kann nicht Partei der interkantonalen Vereinbarung sein; sie betrifft in erster Linie die kantonalen Organe. Die Bestimmungen der Vereinbarung sind keine ausreichende Rechtsgrundlage für Personendatenbearbeitungen durch Bundesorgane. Die Stellungnahme des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) beschränkt sich somit auf allgemeine Überlegungen zur Schaffung eines «nationalen Schweizer Polizeidatenraums». Wir überlassen es den in der Konferenz der schweizerischen Datenschutzbeauftragten (Privatim) zusammengeschlossenen kantonalen Datenschutzbehörden, die Artikel der Vereinbarung ausführlich zu kommentieren.

Wir erlauben uns dennoch, generell darauf hinzuweisen, dass die Bestimmungen zum Geltungsbereich der interkantonalen Vereinbarung sehr weit und unbestimmt gefasst sind, indem alle Daten erfasst werden sollen, die im Rahmen der kriminalpolizeilichen Strafverfolgung über die sicherheitspolizeiliche Gefahrenabwehr bis hin zu verwaltungspolizeilichen Aufgaben bearbeitet werden. Ein solch uferloser Geltungsbereich verwischt die Konturen der polizeilichen Datenbearbeitung zu den unterschiedlichen Zwecken der polizeilichen Prävention und Repression und läuft auf eine unzulässige Blankettermächtigung hinaus. Hinzu kommt, dass der Entwurf damit auch die Differenzierungen verwischt, welche die Bundesverfassung bei der Aufgabenteilung zwischen Bund und Kantonen bezüglich der strafverfolgenden und übrigen Aufgaben der Polizeibehörden statuiert.

Feldeggweg 1
3003 Bern
Tel. +41 58 463 74 84, Fax +41 58 465 99 96
www.edoeb.admin.ch

1. Verfassungsrechtliche Aspekte

Gemäss der Bundesverfassung liegt die Gesetzgebungskompetenz im Bereich der Polizei bei den Kantonen. Der Vollzug polizeirechtlicher Bestimmungen ist ebenfalls Sache der Kantone. Der Bund hat begrenzte und subsidiäre Kompetenzen, zum Beispiel in den Bereichen Sicherheit des Bundes, Zusammenarbeit von Bund und Kantonen und internationale Zusammenarbeit. Zu Recht weist der erläuternde Bericht darauf hin, dass der Vereinbarungsentwurf mit der Kompetenzverteilung zwischen Bund und Kantonen gemäss der Bundesverfassung in Konflikt gerät. Im Gegensatz zur Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS) schliesst der EDÖB daraus, dass das Ziel, nämlich die Schaffung eines «nationalen Schweizer Polizeidatenraums», nicht rechtmässig umgesetzt werden kann; weder mit den derzeit laufenden Anpassungen der kantonalen Polizeigesetze noch mit der vorgeschlagenen interkantonalen Vereinbarung. Kantonale Gesetze und interkantonale Vereinbarungen dürfen der verfassungsrechtlichen Kompetenzverteilung zwischen Bund und Kantonen nicht widersprechen, weder endgültig noch im Sinne einer Übergangslösung. Der erläuternde Bericht weist richtigerweise auf die Gefahr hin, dass die Vereinbarung im Fall einer abstrakten Normenkontrolle durch das Bundesgericht für ungültig erklärt werden müsste. Dies stellt ein hohes Risiko dar, welches im Projekt mit einer Ausführlichkeit auszuweisen ist, welche dessen Bedeutung gerecht wird (s. Ziff. 4.2).

2. Aktuelle Situation: Amtshilfe über den Nationalen Polizeiindex und zahlreiche zentral betriebene Spezialapplikationen, aber keine Zusammenlegung aller Polizeidaten

Im Rahmen der Strafverfolgung haben die Kantonspolizeien nicht nur Zugang zum Nationalen Polizeiindex, sondern auch zu weiteren Informationssystemen des Bundes, die unter anderem die Verbreitung von Daten aus den kantonalen Polizeikorps ermöglichen. Es sind dies insbesondere:

- das System Bundesdelikte (teilweise);
- das System internationale und interkantonale Polizeikooperation;
- das System zur Unterstützung der Ermittlungen der Kantone im Bereich ihrer Strafverfolgungskompetenzen;
- das automatisierte Polizeifahnungssystem (RIPOL) und der nationale Teil des Schengener Informationssystems.

Es ist erstaunlich, dass diese vielen Systeme, die in den letzten fünfzig Jahren mittels zahlreicher Gesetzesrevisionen eingeführt, angepasst und perfektioniert wurden, im erläuternden Bericht nicht erwähnt wurden. Dieser rechtfertigt eine radikale Änderung des Systems zur Bearbeitung von Personendaten durch die Polizeien, ohne den Status Quo darzustellen.

Die Rechtsgrundlagen für die erwähnten Systeme finden sich in vielen miteinander verwobenen Bestimmungen einzelner Bundesgesetze, zum Beispiel im Strafgesetzbuch, im Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI), im Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten, im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit, im Waffengesetz (WG) oder im zukünftigen BAZG-Vollzugsaufgabengesetz. Die Nutzerinnen und Nutzer dieser Systeme verschaffen sich online Zugang zu den Personendaten, ohne im Einzelfall vorgängig bei der für das System verantwortlichen Behörde ein summarisch begründetes Amtshilfegesuch einzureichen.

Die Kantons- und Gemeindepolizeien und die Sicherheitsbehörden des Bundes (Bundesamt für Polizei [fedpol], Bundesamt für Zoll und Grenzsicherheit und Nachrichtendienst des Bundes) bearbeiten in ihren eigenen Systemen Personendaten, die sie für die Erfüllung ihrer gesetzlichen Aufgaben beschafft haben. Diese Behörden leisten sich gegenseitig Amtshilfe; sie können auf der Grundlage eines summarisch begründeten Gesuchs die im Einzelfall erforderlichen Personendaten austauschen. Um diese Amtshilfe zu vereinfachen, betreibt fedpol für die Kantone gemäss Artikel 17 BPI den Nationalen Polizeiindex. Dank diesem können Kantons- und Gemeindepolizeien ihre Amtshilfegesuche gezielt an die Verantwortlichen derjenigen Systeme richten, für die der Index die Registrierung einer konkreten Person anzeigt.

3. «Alter» Wunsch, alle polizeilichen Datenbanken in einem «nationalen Schweizer Polizeidatenraum» zu vereinen

Aufgrund der verfassungsrechtlichen Kompetenzverteilung haben die Gesetzgeber von Bund und Kantonen bisher darauf verzichtet, alle von den Polizeikorps beschafften Personendaten in einem einzigen System zu vereinen und damit allen Polizeibehörden in der Schweiz zugänglich zu machen.

Neben den zahlreichen polizeilichen Informationssystemen wie dem RIPOL, die der Bund für sich selbst und für die Kantone betreibt, und den Informationssystemen, die eine Kantonspolizei für sich selbst und für andere Kantons- oder Gemeindepolizeien betreibt, verfügt jedes Polizeikorps über ein eigenes System, in dem es die Personendaten bearbeitet, die es in der Bevölkerung ihres Zuständigkeitsbereiches beschafft. Während Informationen über Schwerstkriminalität und schwerwiegende Verstösse gegen die öffentliche Ordnung in nationalen Datenbanken wie dem RIPOL bearbeitet werden, erfassen die Berichtssysteme der einzelnen Kantonspolizeien kleinere Vorfälle wie nächtliche Ruhestörungen.

Mit der Vorlage verfolgt die KKPKS den «alten» Wunsch, alle Personendaten, die im Kontakt mit der Bevölkerung eines Zuständigkeitsbereiches (Kantone und Gemeinden) beschafft werden, ohne Amtshilfe uneingeschränkt online zugänglich zu machen. So reichen entsprechende Bestrebungen zur Zusammenlegung dieser Bürgerdaten bis zum Projekt für ein nationales Kriminalinformationssystem der 1970er-Jahre zurück, das die politischen Organe von Bund und Kantonen im Jahre 1984 abbrachen.

Gleichzeitig zur Vereinbarung wird das Ziel der Zusammenlegung auch mit der Erweiterung der Bearbeitungskompetenzen in den kantonalen Polizeigesetzen und mit dem Projekt der Polizeiabfrageplattform (POLAP) von fedpol verfolgt. Mit der Plattform soll so eine standardisierte Suche nach Polizeidaten der Kantone und der Polizeibehörden des Bundes möglich werden.

Die Vorlage ist aus datenschutzrechtlicher Sicht besonders heikel. Die KKPKS legt richtigerweise dar, dass die Rechte der betroffenen Personen durch das Vorhaben, alle von den Polizeibehörden in der Schweiz bearbeiteten Personendaten online zur Verfügung zu stellen, schwer beeinträchtigt werden. Zu Recht zeigen die Erläuterungen denn auch, dass eine Anpassung von dem Referendum unterstellter Rechtsgrundlagen nötig ist, wenn Daten neu ohne Amtshilfe direkt online zugänglich gemacht werden sollen. Dies aufgrund der damit verbundenen Intensivierung des Eingriffs in die Privatsphäre und informationelle Selbstbestimmung der Betroffenen.

4. Mängel der Vorlage

Wie nachfolgend dargelegt wird, weist die Vorlage schwere Mängel auf, sodass sie sich sowohl in staatsrechtlicher wie auch datenschutzrechtlicher Hinsicht insgesamt als unzulässig erweist.

4.1 Unzureichende Begründung der Erforderlichkeit und Dringlichkeit

a) Fehlende Darstellung des Status Quo

Der EDÖB masst sich nicht an, die mit der Vorlage verbundenen Anliegen der KKPKS fachlich zu beurteilen. Seine nachfolgende Kritik richtet sich vielmehr gegen die Begründung der Vorlage: So müssen die nach dem Grundsatz der Verhältnismässigkeit zu erfüllenden Kriterien der Erforderlichkeit und Geeignetheit der polizeilichen Bearbeitung von Personendaten unter gesteigerter Inanspruchnahme der Grundrechte der betroffenen Personen unmittelbar – mit der von der Rechtsprechung erforderlichen Begründungsdichte – aus der Vereinbarung und dem erläuternden Bericht hervorgehen.

In den Erläuterungen weist die KKPKS wiederholt darauf hin, dass die durch den Nationalen Polizeiindex geschaffenen Erleichterungen und der heutige Austausch von Personendaten zwischen den Korps unzureichend seien. Die vorgeschlagene Anpassung sei deshalb unabdingbar und dringlich. Zur äusserst knappen Begründung der Erforderlichkeit verweist die KKPKS auf Seite 4 ihres erläuternden Berichts auf schwerstkriminelle Phänomene:

«Jedes Polizeikorps muss einzeln abgefragt werden. Bei der Bekämpfung von Terrorismus oder transkantonalen und internationalen Schwerstkriminalität ist ein derart schwerfälliger und mit Zeitverlust verbundener Prozess nicht mehr zielführend und mit erheblichen Sicherheitsrisiken behaftet.»

Diese Begründung ist wenig belastbar, da für die Bearbeitung von Personendaten zur Aufdeckung und Verfolgung der schweren und schwersten Kriminalität bereits ein «gemeinsamer Polizeidatenraum» besteht, indem fedpol und das Bundesamt für Zoll und Grenzsicherheit (BAZG) für diese Bearbeitungszwecke seit Jahren für alle Korps online zugängliche Applikationen einschliesslich der internationalen Polizeikanäle zur Verfügung stellen. Wenn die KKPKS zur Begründung des Vereinbarungsentwurfs die Schwerstkriminalität anruft, sollte sie gegenüber der Bevölkerung zumindest ausweisen, weshalb die erwähnten, bestehenden Applikationen von fedpol und BAZG sich in der Praxis als ungenügend oder ungenügend entwicklungsfähig erweisen.

Entsprechende Begründungen sowie eine zur Begründung der Erforderlichkeit notwendige Gegenüberstellung des Ist- und Sollzustandes sucht man in den Erläuterungen indessen vergeblich.

b) Fehlende Angaben zur kriminologischen Erforderlichkeit

Auch fehlen Hinweise, inwieweit die heutige Bearbeitung sich als ungenügend erweist. Hat sich die Kriminalitätslage gemäss der Kriminalstatistik in der Schweiz allgemein oder im Bereich der in den Vernehmlassungsunterlagen genannten Serieneinbrüche auf längere Frist zurück betrachtet signifikant verschlimmert? Der EDÖB ist keine Fachbehörde für Kriminologie, stellt aufgrund seiner Zuständigkeiten im Zusammenhang mit Datenschutzverletzungen jedoch fest, dass die Kriminalitätslage vor allem im Bereich der Cyberkriminalität ausser Kontrolle zu geraten droht. Eine kriminologische Entwicklung also, die sich durch eine landesweite Bearbeitung von Bagatelldaten, die im Kontakt mit der lokalen Bevölkerung anfallen, schwerlich durchbrechen lassen dürfte. Zu all diesen Entwicklungen fehlen – abgesehen von den wiederholten Dringlichkeitshinweisen – jegliche Erläuterungen.

c) Fehlende Hinweise zur Digitalisierung der Amtshilfe

In den Vernehmlassungsunterlagen beruft sich die KKPKS indessen auf die vom Bundesrat am 15. August 2018 angenommene Motion Eichenberger (18.3592), die zur Begründung keineswegs die Schwerstkriminalität, sondern die Verfolgung von flüchtigen Serieneinbrechern anführt. Leider führt die KKPKS in den Erläuterungen erneut nicht aus, warum sich die bestehenden landesweiten Instrumente

wie zum Beispiel das RIPOL für die Verfolgung solcher Serientäter als ungenügend erweisen. Kaum nachzuvollziehen ist, dass die KKPKS in Anlehnung an eine Motion, die in ihrem Wortlaut den Serieneinbruch als einziges Beispiel nennt, einen Auftrag zur Zugänglichmachung sämtlicher Kategorien von Daten herleitet, welche die Korps bearbeiten (inklusive verwaltungspolizeilicher Personendaten).

Grund zur Besorgnis geben in diesem Zusammenhang insbesondere folgende Aussagen auf Seite 4 der Erläuterungen, welche nahelegen, dass die kantonalen Korps die amtshilfeweisen Rückfragen, welche sich aufgrund von Treffern im nationalen Polizeiindex aufdrängen, mit nicht mehr zeitgemässen Arbeitsmethoden abwickeln:

«Informationen über verdächtige Personen aus anderen Kantonen können Polizeibehörden nur indirekt über den Polizeiindex und mit erheblichem Aufwand mittels Anfragen per Telefon oder E-Mail erhalten.»

Diese Aussage der KKPKS gibt Anlass zur Befürchtung, dass es die Kantone versäumt haben könnten, die über ihre Einsatzzentralen verbreiteten Amtshilfegesuche durch zeitgemäss informatisierte Abläufe oder durch zeitgerecht beantwortbare Ring-Abfragen über digitale Anfrageportale zu bearbeiten. Zudem lassen Medienberichte über Fahndungspannen und pauschale Klagen der Polizei über das angebliche Ungenügen der heutigen Mechanismen der Amtshilfe meist die Frage unbeantwortet, ob und inwieweit die heute zur Verfügung stehenden Mittel der Amtshilfe im konkreten Fall tatsächlich genutzt und ausgeschöpft wurden.

Vor dem Hintergrund des erläuternden Berichts empfiehlt der EDÖB der KKPS somit bezüglich berechtigter Anliegen, statt zur Abschaffung der polizeilichen Amtshilfe zu deren zeitgemässen Digitalisierung zu schreiten. So wäre es denkbar, Onlinezugriffe mit einer Standardisierung und Automatisierung der Amtshilfe zu koppeln, indem die online zugreifenden Stellen vor dem eigentlichen Zugriff auf einem vorbereiteten Textfeld den Grund ihres Zugriffs und nähere Bezeichnungen zum Geschäft eingeben und ihre Informationsbedürfnisse je nach Routinecharakter des Gesuchs mittels Multiple-Choice oder Freitext begründen würden. Je nach Eindeutigkeit, Komplexität und Relevanz des Anliegens würden die im Einzelfall benötigten Informationen dann von den ersuchten Behörden zeitlich mehr oder weniger unmittelbar freigeschaltet.

Auch wenn eine Freischaltung in statistisch häufigen Standardsituationen und in Fällen zeitlicher Dringlichkeit automatisiert erfolgte, würde der Eingriff in die grundrechtlich geschützte Sphäre der Betroffenen milder ausfallen, als bei einem direkten Online-Zugriff ohne vorgeschaltete Amtshilfe. Dies, u.a., weil die Begründung der Amtshilfe dokumentiert und somit auch einer nachträglichen Kontrolle im Einzelfall zugänglich würde.

4.2 Schengen

a) Unzureichende Ausweisung der Risiken

Als assoziiertes Schengen-Mitglied hat die Schweiz die EU-Richtlinie 2016/680 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates zu übernehmen und zu beachten. Gemäss Artikel 27 dieser Richtlinie, welcher die vorgängige Erstellung einer Datenschutz-Folgenabschätzung (DSFA) regelt, und den daran angepassten Datenschutzgesetzgebungen von Bund und Kantonen haben die Einwohnerinnen und Einwohner der Schweiz einen rechtlichen Anspruch darauf, dass die Verantwortlichen von Projekten zur Bearbeitung von Personendaten im Anwendungsbereich der Richtlinie die damit einhergehenden Risiken vor der Inbetriebnahme angemessen prüfen und ausweisen. Gleichzeitig sind in der DSFA

auch die notwendigen Abhilfemassnahmen sicherzustellen, und es ist der Nachweis zu erbringen, dass die anwendbaren Rechtsgrundlagen eingehalten werden.

Mit dem Vereinbarungsentwurf soll eine in jedem Kanton dem Referendum unterstellte Rechtsgrundlage geschaffen werden, um unter Abschaffung der polizeilichen Amtshilfe einen polizeibehördlichen Direktzugriff auf alle Polizeidaten zu ermöglichen, die im Kontakt mit Personen in der Schweiz anfallen. Die Befassung der Parlamente und der referendumsberechtigten Bevölkerungen in den Kantonen setzt voraus, dass diese sowohl über die staatspolitischen Risiken (Machtzuwachs der Polizei und Intensivierung der Bearbeitung von Bürgerdaten) als auch die informationstechnischen Risiken und Schadenspotentiale (Cyberangriffe und Datenverluste usw.) informiert werden.

Weder zu diesen wesentlichen Risiken noch zur Einhaltung der staats- und verfassungsrechtlichen Rahmenbedingungen (s. vorne Ziff. 1) finden sich Angaben im erläuternden Bericht, der mit seinen spärlich begründeten Aussagen weder der rechtspolitischen noch der datenschutzrechtlichen Tragweite der Vorlage gerecht wird, die wesentliche Aspekte der grundrechtsrelevanten Personendatenbearbeitung offenlässt und in unzulässiger Weise an kantonale Exekutivorgane delegiert.

b) Irreführende Angaben zum Informationsaustausch

Im erläuternden Bericht wird festgehalten, dass nach Abschluss der Arbeiten zur Interoperabilität im Schengenraum die Schweiz paradoxerweise mit Europa mehr Polizeidaten um ein Vielfaches schneller und einfacher werde austauschen können, als dies im Binnenverhältnis zwischen Bund und Kantonen und zwischen den Kantonen möglich sei. Dieser Vergleich mit dem Schengenbereich und die daraus abgeleitete Behauptung sind aus folgenden Gründen irreführend:

So betrifft der Direktzugriff im Schengenbereich fast ausschliesslich das Schengener Informationssystem (SIS) und ist dementsprechend auf die im SIS enthaltenen Ausschreibungen oder Delikte beschränkt. Auf das SIS haben sowohl fedpol als auch die verschiedenen Kantonspolizeien bereits heute einen direkten (Online-)Zugriff. Die Interoperabilität wird diese Zugriffsrechte nicht ändern, sondern erleichtern und verbessern. Mit anderen Worten werden die Schweizer Strafverfolgungsbehörden auch nach Einführung der Interoperabilität einen direkten Zugriff auf dieselben Daten im SIS haben wie bis anhin. Zudem sind die von Schweizer Behörden getätigten Einträge im SIS auch im RIPOL enthalten, auf welches sowohl fedpol als auch die Kantonspolizeien bereits heute bis auf Stufe Streifenpolizei einen direkten und mobilen Online-Zugriff haben.

Davon zu unterscheiden sind die Informationen, die zusätzlich zu den im SIS selbst enthaltenen Daten im Rahmen der Amtshilfe ausgetauscht werden. Ein solcher Austausch erfolgt – wie bei jeder Amtshilfe – auch im Rahmen von Schengen im Einzelfall und unter Einhaltung der jeweiligen Vorschriften. In der Schweiz regelt das Schengen-Informationsaustausch-Gesetz (SIaG) diesen Informationsaustausch zwischen den Strafverfolgungsbehörden des Bundes und der anderen Schengen-Staaten. Gestützt auf das SIaG erfolgt dieser Informationsaustausch, sowohl das Ersuchen um Information als auch die Weiterleitung der angefragten Informationen, mittels Formularen. Folglich müssen die Daten im Einzelfall verlangt werden, und es besteht in diesen Fällen kein direkter (Online-)Zugriff auf diese Daten.

Daraus folgt, dass die im erläuternden Bericht auf Seite 5 gemachte Aussage, dass im Schengenraum paradoxerweise mit Europa mehr Polizeidaten um ein Vielfaches schneller und einfacher ausgetauscht werden können als im Binnenverhältnis, irreführend ist.

5. Fazit

Der EDÖB lehnt den Vereinbarungsentwurf der KKPKS ab, da er ihn für zu wenig begründet und aus rechtsstaatlicher und datenschutzrechtlicher Sicht für unzulässig hält.

Der in der Vorlage vorgesehene Systemwechsel und die damit verbundene Kompetenzerweiterung der Polizeikorps bei der Bearbeitung von Personendaten könnten rechtmässig und glaubwürdig nur mit der Schaffung einer neuen Bestimmung in der Bundesverfassung erreicht werden, wie es die Motion 23.4311 der Sicherheitspolitischen Kommission des Nationalrats verlangt. Diese wäre dem obligatorischen Referendum unterstellt und würde dem Schweizer Volk zur Abstimmung vorgelegt. Das Ergebnis eines solchen Plebiszits darf auch nicht durch eine bloss übergangsrechtliche Geltung der vorgeschlagenen Vereinbarung vorweggenommen werden.

Mit Blick auf die teilweise berechtigten Anliegen der KKPKS empfiehlt der EDÖB der KKJPD, im Sinne der obenstehenden Ausführungen eine zeitgemässe digitale Lösung für die landesweite Bearbeitung von Personendaten im Rahmen der polizeilichen Amtshilfe entwickeln und einer erneuten Analyse der Rechtsgrundlagen unterziehen zu lassen.

Freundliche Grüsse

Adrian Lobsiger
Der Beauftragte

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

Le préposé

POST CH AG
CH-3003 Berne | PFPDT; EDÖB-A-5ED73401/1

Envoi en annexe
Conférence des directrices et directeurs des départements cantonaux de justice et police
Haus der Kantone
Speichergasse 6
3001 Bern

Votre référence :
Notre référence : EDÖB-A-5ED73401/1
Dossier traité par : Frédéric Schönbett
Berne, le 22 février 2024

Projet de convention intercantonale sur l'échange de données à des fins d'exploitation de plateformes de recherche et de systèmes de bases de données communs

Mesdames, Messieurs,

Nous vous remercions de nous avoir consultés au sujet de l'objet cité en titre et vous faisons part des remarques suivantes :

Remarques liminaires

La Confédération ne peut pas être partie à la convention intercantonale qui concerne avant tout les organes cantonaux. Ses dispositions ne peuvent servir de base légale suffisante pour le traitement de données personnelles par les organes fédéraux. Pour ces raisons, la prise de position du Préposé fédéral à la protection des données et à la transparence (PFPDT) se limite à des considérations générales sur la création d'un « espace national suisse de données de police ». Nous laissons les autorités cantonales de protection des données regroupées au sein de la Conférence des Préposé(e)s suisses à la protection des données (privatim) commenter de manière détaillée les articles de la convention.

Nous nous permettons cependant de signaler que les dispositions portant sur le champ d'application de la convention sont formulées de manière très ouverte et très vague, puisqu'elles prévoient de saisir toutes les données traitées par la police lors d'enquêtes criminelles, qu'elles servent à écarter un danger pour la sécurité ou à accomplir des tâches de police administrative. Donner un champ d'application aussi large revient à supprimer le cadre dans lequel doit s'insérer le traitement des données par la police, à savoir atteindre ses objectifs de prévention et de répression, et à lui donner un blanc-seing inadmissible. Le projet brouille au surplus la répartition des tâches entre la Confédération et les cantons qu'impose la Constitution en matière d'autorités de poursuite pénale et des autres tâches de police.

Feldeggweg 1
3003 Berne
Tél. +41 58 463 74 84, Fax +41 58 465 99 96
www.edoeb.admin.ch

1. Aspects constitutionnels

La Constitution attribue aux cantons la compétence de légiférer dans le domaine de la police. L'exécution des dispositions légales en matière de police est également de leur compétence. La Confédération dispose de compétences limitées et subsidiaires, par exemple la sécurité de la Confédération, la coopération entre les cantons et la Confédération et la collaboration internationale. Le rapport explicatif souligne à juste titre que le projet de convention entre en conflit avec la répartition des compétences entre la Confédération et les cantons inscrite dans la Constitution. Contrairement à la CCPCS, le PFPDT conclut de cette situation que la finalité poursuivie, à savoir la création d'un « espace national suisse de données de police » ne peut être légalement mis en œuvre ni par les adaptations des lois cantonales sur la police qui sont en cours, ni par la convention intercantonale proposée. Les lois cantonales et les conventions intercantonales ne peuvent pas déroger à la répartition des compétences entre les cantons et la Confédération telle qu'elle est définie par la Constitution, que ce soit de manière définitive ou transitoire. Comme l'indique à juste titre le rapport explicatif, la convention risque donc d'être annulée en cas de contrôle abstrait des normes par le Tribunal fédéral. Ce risque élevé sur un point central du projet requiert d'entrer d'autant plus dans les détails (cf. ch. 4.2).

2. Situation actuelle : assistance administrative au moyen de l'index national de police et de multiples autres applications spéciales exploitées de manière centralisée, mais pas de regroupement de toutes les données policières

Dans le cadre de la poursuite pénale, les polices cantonales ont accès non seulement à l'index national de police mais à plusieurs autres systèmes d'information fédéraux, qui permettent entre autres fonctionnalités la diffusion de données émanant des corps de police cantonaux, notamment :

- le système de traitement des données relatives aux infractions fédérales (en partie),
- le système de traitement des données relatives à la coopération policière internationale et intercantonale,
- le système d'appui aux enquêtes menées par les cantons dans leur domaine de compétence en matière de poursuite pénale,
- le système de recherches informatisées de personnes RIPOL et la partie nationale du système d'information Schengen N-SIS.

Il est étonnant que ces nombreux systèmes, mis en place, adaptés et perfectionnés par de nombreuses révisions de lois depuis une cinquantaine d'années, n'aient pas été mentionnés dans le rapport explicatif, lequel justifie un changement radical du système de traitement des données personnelles par les polices sans présenter la situation actuelle.

Les bases juridiques de ces systèmes se trouvent dans une multitude de dispositions légales spéciales du droit fédéral, comme le code pénal, la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP), la loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États, la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, la loi sur les armes ou la future loi fédérale définissant les tâches d'exécution de l'Office fédéral de la douane et de la sécurité des frontières (OFDF). Les utilisateurs de ces systèmes accèdent en ligne aux données personnelles sans avoir à déposer au préalable auprès de l'autorité responsable du système une demande d'assistance administrative sommairement motivée pour un cas particulier.

Les polices cantonales et communales et les autorités fédérales de sécurité (Office fédéral de la police [fedpol], OFDF et Service de renseignement de la Confédération) traitent dans leurs propres systèmes

les données personnelles collectées lors de l'accomplissement de leurs tâches légales. Ces mêmes autorités se prêtent mutuellement assistance, ce qui les autorise à échanger les données personnelles nécessaires dans un cas particulier et sur la base d'une demande sommairement motivée. Afin de faciliter cette assistance administrative, fedpol gère pour les cantons, conformément à l'art. 17 LSIP, l'index national de police, qui permet aux polices cantonales et communales d'adresser leurs demandes d'assistance administrative de manière ciblée aux responsables des systèmes sources pour lesquels l'index indique l'enregistrement d'une personne concrète.

3. « Ancien » souhait de regrouper toutes les bases de données policières dans un « espace national suisse de données de police »

En raison de la répartition des compétences inscrite dans la Constitution, les législateurs de la Confédération et des cantons ont renoncé jusqu'à présent à regrouper dans un système unique toutes les données personnelles collectées par les corps de police et à les rendre ainsi accessibles à toutes les autorités de police en Suisse.

En plus des nombreux systèmes d'information de la police (RIPOL, que la Confédération exploite pour elle-même et pour les cantons, et systèmes d'information exploités par une police cantonale pour elle-même et pour d'autres polices cantonales ou communales), chaque corps de police dispose de son propre système dans lequel il traite les données personnelles qu'il recueille au contact de la population. Alors que les informations relatives à la criminalité grave et aux atteintes sérieuses à l'ordre public sont traitées dans des banques de données nationales telles que RIPOL, les systèmes de rapport des différentes polices cantonales enregistrent les incidents mineurs tels que les tapages nocturnes.

Avec le présent projet, la Conférence des commandantes et des commandants des polices cantonales (CCPCS) poursuit son « ancien » souhait de rendre accessibles en ligne, sans réserve, toutes les données personnelles générées dans le cadre des contacts avec la population (cantons et communes), ce qui va bien au-delà de l'assistance administrative. Les tentatives de regroupement de ces données remontent ainsi aux années 1970, avec le projet de système national d'information criminelle, avorté en 1984 après l'intervention des organes politiques de la Confédération et des cantons.

Outre le présent projet de convention, cet objectif est poursuivi parallèlement par l'extension des compétences de traitement dans les lois cantonales sur la police et par le projet de plate-forme de recherche policière (POLAP) de fedpol, qui doit permettre de rechercher de manière standardisée les données policières des cantons et celles des autorités fédérales de police.

Ce projet est particulièrement sensible du point de vue de la protection des données. Comme la CCPCS l'explique à juste titre, le projet de mise à disposition en ligne de toutes les données personnelles traitées par les autorités policières en Suisse porte gravement atteinte aux droits des personnes concernées. Comme les explications le montrent également à juste titre, l'abandon de l'exigence de l'assistance administrative pour l'accessibilité dircect en ligne nécessite, en raison de la gravité des atteintes à la vie privée et à l'autodétermination informationnelle des personnes concernées, une adaptation des bases juridiques sujettes au référendum.

4. Défauts du projet

Le projet présente de graves défauts qui le rendent inadmissible tant du point de vue de l'État de droit que sous l'angle de la protection des données.

4.1 Justification insuffisante de la nécessité et de l'urgence du changement

a) Absence de présentation de la situation actuelle

Le PFPDT s'abstient de juger les objectifs poursuivis par le projet au fond. Ses critiques portent sur sa justification. Lorsque le traitement par la police de données personnelles porte une atteinte accrue aux droits fondamentaux des personnes concernées, le principe de proportionnalité demande en effet que les critères de nécessité et d'adéquation ressortent directement de la convention et du rapport explicatif et soient suffisamment motivés conformément à la jurisprudence sur le sujet.

Dans le rapport explicatif, la CCPCS relève à plusieurs reprises que l'accès facilité aux données que permet l'index national de police est insuffisant, tout comme l'échange de données personnelles entre les corps de police. C'est, selon elle, ce qui rend le projet indispensable et urgent. Elle n'en justifie la nécessité que de manière extrêmement brève, à la page 4 du rapport explicatif, en évoquant les crimes les plus graves :

« Chaque corps de police doit être approché séparément. Pour la lutte contre le terrorisme et la grande criminalité transcantonale ou internationale, un processus aussi lourd et générateur de pertes de temps est aujourd'hui inapproprié et à l'origine d'importants risques pour la sécurité. »

Cette justification est peu convaincante, étant donné qu'il existe déjà un « espace commun de données policières » pour le traitement des données personnelles nécessaires aux enquêtes ou aux poursuites sur les crimes graves. Depuis des années, en effet, fedpol et l'OFDF mettent à ces fins des applications accessibles en ligne, reliées aux canaux policiers internationaux, à la disposition de tous les corps de police. Si la CCPCS invoque la lutte contre les crimes les plus graves pour justifier la convention, elle devrait au moins expliquer pourquoi ces applications ne suffisent pas ou ne peuvent être suffisamment développées. On cherche en vain ces explications dans le rapport explicatif, de même qu'une comparaison entre la situation actuelle et celle qui s'appliquerait après l'entrée en vigueur de la convention, pour en justifier la nécessité.

b) Absence de justification du point de vue criminologique

Il manque également des indications sur les insuffisances qu'entraîne le traitement actuel des données. Selon la statistique policière de la criminalité et sur le temps long, la criminalité a-t-elle augmenté de manière significative en Suisse de manière générale ou dans le domaine des cambriolages en série évoqués dans les documents mis en consultation ? Le PFPDT n'est pas spécialisé en criminologie, mais il constate sur la base de ses compétences en matière de violations de la protection des données que c'est principalement la cybercriminalité qui risque d'échapper à tout contrôle. Or, le traitement dans l'ensemble de la Suisse de données relatives à des infractions mineures qui ont été récoltées au contact avec la population pourra difficilement y remédier. On cherche en vain dans le rapport explicatif la moindre information sur l'ensemble de ces questions, alors que l'urgence d'agir y est soulignée à plusieurs reprises.

c) Absence d'informations sur la numérisation de l'assistance administrative

Dans les documents mis en consultation, la CCPCS se fonde sur la motion Eichenberger n° 18.3592, que le Conseil fédéral a proposé d'adopter le 15 août 2018. Le développement de cette intervention parlementaire ne porte nullement sur la grande criminalité mais sur les cambrioleurs en série qui échappent aux poursuites. À nouveau, la CCPCS ne dit pas dans le rapport explicatif pourquoi les instruments existants à l'échelle suisse, tels que le système de recherche national RIPOL, seraient insuffisants pour poursuivre de tels auteurs de délits en série. Il est difficile de comprendre pourquoi elle tire

d'une motion qui a pour seul exemple les cambriolages en série l'idée qu'elle donne pour mandat de rendre accessibles toutes les catégories de données traitées par les corps de police (y compris les données personnelles qui lui servent pour accomplir des tâches de police administrative).

Il est par ailleurs inquiétant de lire en particulier le passage suivant dans le rapport explicatif (p. 4), puisqu'il indique que les corps de police cantonaux ne recourent pas à des méthodes modernes de travail pour traiter les demandes d'assistance administrative qui découlent des résultats positifs des recherches effectuées dans l'index national de police :

« Les informations relatives à des personnes suspectes disponibles dans d'autres cantons ne sont accessibles aux autorités de police qu'indirectement via l'index national de police, ou de manière complexe par téléphone ou par courriel ».

On peut craindre, à lire cette phrase, que les cantons n'aient négligé de développer des processus informatiques modernes ou des réseaux en anneau sur un portail numérique afin d'assurer le traitement en temps utile des demandes d'assistance administrative diffusées par leurs centrales d'engagement. Lorsque les médias rapportent les échecs des enquêtes de police ou les plaintes qu'elle formule sur l'insuffisance des mécanismes actuels de l'assistance administrative, ils n'expliquent pas le plus souvent si les moyens actuels ont bel et bien été utilisés et si toutes les possibilités qu'ils offrent ont été épuisées.

Au vu du rapport explicatif et des préoccupations légitimes qui en ressortent, le PFPDT recommande donc à la CCPCS de lancer les travaux nécessaires à un traitement numérique standardisé moderne de l'assistance administrative entre les corps de police au lieu de la supprimer. On pourrait ainsi imaginer une automatisation de l'assistance administrative avec l'accès en ligne : les services qui font une demande d'accès devraient indiquer au préalable dans un champ prédéfini la raison pour laquelle ils demandent un accès au système, en donnant des précisions sur l'affaire qu'ils traitent et en justifiant leur besoin de disposer des informations ; selon le caractère plus ou moins routinier de la demande, ils devraient simplement cocher une case ou motiver leur demande dans un champ ; l'autorité compétente donnerait ensuite accès aux données nécessaires au cas d'espèce plus ou moins rapidement par un accès au système, en fonction de la clarté, de la complexité et de la pertinence de la demande.

Même si l'accès au système était automatisé dans des situations standard statistiquement fréquentes et dans des cas d'urgence temporelle, l'atteinte à la sphère protégée par les droits fondamentaux des personnes concernées serait moins importante que dans le cas d'un accès direct en ligne sans assistance administrative préalable. Ceci, entre autres, parce que la justification de l'assistance administrative serait documentée et donc accessible à un contrôle ultérieur au cas par cas.

4.2 Schengen

a) Présentation insuffisante des risques

En tant que membre associé de l'accord de Schengen, la Suisse est tenue de reprendre et de respecter la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil. En vertu de son art. 27, qui prévoit la réalisation d'une analyse d'impact sous l'angle de la protection des données « préalablement au traitement », et des législations fédérales et cantonales modifiées en conséquence, les habitants de la Suisse ont droit, dans le champ d'application de la directive, à ce que les responsables de projets de traitement de données personnelles examinent et démontrent de manière appropriée avant la mise en

service les risques qui découlent du traitement. L'analyse d'impact doit aussi garantir les mesures correctives nécessaires et apporter la preuve que les bases juridiques applicables sont respectées.

Le projet de convention prévoit la création, dans chaque canton, d'une base légale sujette au référendum qui permette aux autorités de police, après la suppression de l'assistance administrative, d'accéder directement aux données policières générées lors des contacts avec des personnes en Suisse. Pour que les députés dans les parlements cantonaux et le peuple de chaque canton puissent se prononcer en connaissance de cause, il faut qu'ils soient informés tant des risques pour l'État de droit (davantage de pouvoir conféré à la police, intensification du traitement des données des citoyens) que des risques informatiques et des dommages potentiels (cyberattaques, pertes de données, etc.).

Or, on ne trouve dans le rapport explicatif aucune information sur ces risques essentiels ni sur le respect des principes de l'État de droit et de la Constitution (cf. ch. 1). Les déclarations peu motivées qu'il contient ne sont à pas à la hauteur des enjeux politico-juridiques du projet, notamment sous l'angle de la protection des données. Des aspects essentiels du traitement des données personnelles touchant aux droits fondamentaux sont laissés en suspens et délégués de manière illicite aux organes exécutifs cantonaux.

b) Indications trompeuses sur l'échange d'informations

On lit dans le rapport explicatif que « une fois les travaux concernant l'interopérabilité dans l'espace Schengen terminés, la Suisse pourra échanger avec l'Europe des données de police en plus grande quantité et beaucoup plus simplement et rapidement qu'à l'intérieur du pays, entre les cantons et entre ces derniers et la Confédération, ce qui est paradoxal ». Cette comparaison et la conclusion qui en est tirée sont trompeuses.

L'accès direct dans le domaine Schengen concerne en effet presque exclusivement le système d'information SIS et se limite par conséquent aux signalements et aux infractions qui y sont enregistrés. Tant fedpol que les polices cantonales ont déjà un accès direct (en ligne) au système. L'interopérabilité ne changera rien à ces droits d'accès, mais elle les facilitera et les améliorera. En d'autres termes, les autorités de poursuite pénale suisses continueront de disposer d'un accès direct aux mêmes données après l'introduction de l'interopérabilité. En outre, les données enregistrées dans le SIS par des autorités suisses sont également contenues dans RIPOL, système auquel tant fedpol que les polices cantonales, jusqu'aux policiers qui font des patrouilles, ont déjà un accès direct mobile en ligne.

L'échange d'informations relevant de l'assistance administrative, en plus de celles contenues dans le SIS, est soumis à d'autres règles. Il a lieu, dans le cadre de l'accord de Schengen comme pour toute assistance administrative, pour un cas particulier et dans le respect des prescriptions. En Suisse, cet échange entre les autorités de poursuite pénale de la Confédération et les autres États Schengen est régi par la loi du 12 juin 2009 sur l'échange d'informations Schengen (RS *362.2*). Tant la demande d'informations que leur transmission se font par formulaire, aussi les données doivent-elles être demandées pour chaque cas, sans accès direct (en ligne) aux données.

Le passage précité de la page 5 du rapport explicatif est donc trompeur.

5. Conclusion

Le PFPDT rejette le projet de convention de la CCPCS, car il le juge insuffisamment motivé et inadmissible du point de vue de l'État de droit et de la protection des données.

Le changement de système prévu par le projet et l'extension des compétences des corps de police en

matière de traitement de données personnelles qui en découle ne pourrait être obtenu de manière légale et crédible que par la création d'une disposition dans la Constitution, prévue par la motion 23.4311 du 10 octobre 2023 de la Commission de la politique de sécurité du Conseil national, et par un vote obligatoire du peuple. Le résultat d'une telle votation ne saurait être anticipé en introduisant la présente convention à titre transitoire.

Au vu des demandes partiellement légitimes de la CCPCS, le PFPDT recommande à la CCDJP de développer une solution numérique moderne pour le traitement de données personnelles à l'échelle nationale dans le cadre de l'assistance administrative en matière de police et de la soumettre à une nouvelle analyse des bases légales, dans le sens des explications ci-dessus.

Nous vous prions d'agréer, Mesdames et Messieurs, nos salutations distinguées.

Adrian Lobsiger
Le préposé

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Polizei fedpol
Direktion

POST CH AG

CH-3003 Bern fedpol; bap-jeke

Aktenzeichen: 053.0-380/6/1
Ihr Zeichen:

Konferenz der Kantonalen Justiz- und
Polizeidirektorinnen und -direktoren KKJPD
Per Mail an: info@kkjpd.ch

Bern, 15. Februar 2024

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme – Stellungnahme fedpol

Sehr geehrte Frau Präsidentin, sehr geehrter Herr Präsident

Ich nehme Bezug auf Ihr Schreiben vom 23. November 2023 zur Vernehmlassung über die interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme. Der Vorsteher des Eidgenössischen Justiz- und Polizeidepartements, Bundesrat Beat Jans, hat fedpol damit beauftragt, zur titelerwähnten Vereinbarung Stellung zu nehmen. Für die Möglichkeit zur Stellungnahme danken wir Ihnen bestens.

fedpol hat sowohl das SEM als auch das BJ konsultiert und begrüsst die Bestrebungen der KKJPD mittels der vorliegenden interkantonalen Vereinbarung (Konkordat) die gesetzlichen Grundlagen für einen sehr wichtigen Teilbereich des polizeilichen Datenaustauschs zu schaffen und zudem den Betrieb von gemeinsamen Datenbanksystemen zu regeln.

Einleitende Bemerkungen

Da eine Teilnahme des Bundes am Konkordat nicht vorgesehen ist, beschränken wir uns auf einige Hinweise, welche die Polizeiliche Abfrageplattform (POLAP) und die gemeinsamen Datenbanksysteme betreffen.

Für den Bund steht **die Umsetzung der Motion 18.3591 Eichenberger-Walther «Nationaler polizeilicher Datenaustausch» mit dem Programm POLAP (Polizeiliche Abfrageplattform)** im Vordergrund. Der Bund und die Kantone, unterstützt durch Polizeitechnik und -informatik Schweiz (PTI Schweiz), treiben die technische Umsetzung der Motion Eichenberger mit dem Programm POLAP voran. Das Programm POLAP besteht aus drei Projekten. In den Projekten 1 und 2 werden der Aufbau der eigentlichen Abfrageplattform,

Bundesamt für Polizei fedpol
Nicoletta della Valle
Guisanplatz 1
3003 Bern
Tel. +41 58 463 11 23
marco.jeker@fedpol.admin.ch
https://www.fedpol.admin.ch/

der Anschluss der bestehenden polizeilichen Informationssysteme des Bundes und der EU (Projekt 1) und der Anschluss der neuen Systeme der EU zur Umsetzung der Interoperabilität (Projekt 2) umgesetzt. Das Projekt 3 beinhaltet den Anschluss der kantonalen polizeilichen Informationssysteme (Vorgangsdatenbearbeitungssysteme). Wenn die kantonalen polizeilichen Informationssysteme an POLAP angeschlossen werden, ist ein Austausch von polizeilichen Informationen unter den Kantonen und mit dem Bund möglich. Für den Informationsaustausch ausserhalb von gerichtspolizeilichen Verfahren gemäss Schweizerischer Strafprozessordnung (StPO, SR 312.0) fehlen bei vielen Kantonen die notwendigen gesetzlichen Grundlagen. Diese Lücke soll mit dem Konkordat geschlossen werden.

Die Projekte 1 und 2 betreffen primär den Bund, da die davon betroffenen Personendaten und Datenbekanntgaben in der Verantwortung von Behörden des Bundes liegen (fedpol, SEM, BAZG). fedpol wird die POLAP-Plattform für die Behörden der Kantone und des Bundes betreiben. Das ISC-EJPD wird den technischen Betrieb übernehmen. Nach heutigem Kenntnisstand wird sich daran auch mit dem Projekt 3 und dem Anschluss der kantonalen Informationssysteme nichts ändern. Im Konkordat wird der Betrieb der Abfrageplattform (im Sinne von POLAP) aber als eine Aufgabe der Konkordatsmitglieder beschrieben. POLAP ist zwar ein Projekt von Bund und Kantonen, aber die Verantwortung für den Betrieb von POLAP liegt beim Bund (fedpol).

Zu den Bestimmungen betreffend «Gemeinsame Datenbanksysteme»

Artikel 5 Ziffer 6 des Konkordats definiert gemeinsame Datenbanksysteme als Informationssysteme mit einer zentralen Datenbank, welche von mehreren Teilnehmenden betrieben werden, um ihre polizeilichen Aufgaben zu erfüllen. Diese Formulierung ist unklar und könnte deshalb auch missverstanden werden. Nach dem Wortlaut ist entscheidend, dass eine zentrale Datenbank betrieben wird. Damit wäre eine distribuierte Datenhaltung, zum Beispiel bei Stellen des Bundes und/oder den Kantonen, ausgeschlossen. Es kann sein, dass eine zentrale Datenhaltung als gute Lösung in einem konkreten Fall erscheint, sollte aber nicht zwingend vorgegeben sein. Die durch das Konkordat vorgegebene Definition von gemeinsamen Datenbanksystemen sollte nochmals geprüft werden, da sie uns als unnötig einschränkend erscheint.

Artikel 16 Absatz 3 hält fest, dass der Bund unter Vorbehalt des Bundesrechts an den gemeinsamen Datenbanksystemen durch Abschluss einer Leistungsvereinbarung oder durch Übernahme der Betriebsverordnung teilnehmen kann. Aus den Bestimmungen und den Erläuterungen zu diesen Bestimmungen geht aber nicht hervor, wie dies geschehen könnte. Vielmehr wird darauf verwiesen, dass der Bund Mitglied von PTI Schweiz ist und damit auch mitbestimmen könnte. Gleichzeitig wird darauf hingewiesen, dass die Beteiligung des Bundes, sei es in Form einer Leistungsvereinbarung oder durch die Übernahme der Betriebsverordnung, bundesrechtskonform sein müsse. Eine Leistungsvereinbarung oder die Übernahme der Betriebsverordnung alleine reichen für Behörden des Bundes aber als gesetzliche Grundlagen für eine Datenbearbeitung in einem gemeinsamen polizeilichen Datenbanksystem nicht aus. Wenn eine oder mehrere Behörden des Bundes zusammen mit den Kantonen polizeiliche Daten in einem geteilten Informationssystem bearbeiten wollen, benötigen sie eine ausdrückliche gesetzliche Grundlage in einem Bundesgesetz im formellen Sinn. Dies ist insbesondere dann der Fall, wenn die Bundesbehörden dadurch polizeiliche Informationen an Behörden der Kantone oder des Bundes im Abrufverfahren bekanntgeben würden. Deshalb muss zwischen der möglichen organisatorischen und finanziellen Beteiligung des Bundes an gemeinsamen Datenbanksystemen und der Regelung dieser Aspekte mittels einer Leistungsvereinbarung und den Bestimmungen bezüglich der Datenbearbeitungen klar differenziert werden. Für die Datenbearbeitungen der Bundesbehörde in einem gemeinsamen

polizeilichen Datenbanksystem müssten trotz einer Leistungsvereinbarung oder der Übernahme der Betriebsverordnung die geeigneten formell-gesetzlichen Bestimmungen vorhanden sein. Wir regen an, dass dieser Sachverhalt in den Erläuterungen noch klarer dargestellt wird.

Zudem geben wir zu bedenken, dass die Bestimmungen bezüglich Datenbearbeitungen in Artikel 20 des Konkordats nur für von den Teilnehmenden gemeinsam betriebenen Datenbanksystemen Gültigkeit hätten. Dies hätte zur Konsequenz, dass das Konkordat keine gesetzlichen Grundlagen für den Datenaustausch unter den Kantonen mittels vom Bund betriebener Informationssysteme schaffen würde. Dieses Manko könnte auch mittels einer Vereinbarung zwischen den Teilnehmenden des Konkordats und dem Bund nicht beseitigt werden. Insofern müsste das 3. Kapitel des Konkordats nochmals überdacht werden, wenn es auch die gesetzlichen Grundlagen für den polizeilichen Datenaustausch ausserhalb von Verfahren gemäss StPO schaffen soll, der nicht in einem von den Teilnehmenden betriebenen gemeinsamen Datenbanksystem stattfindet. Dieser Punkt ist von grosser Wichtigkeit, da der Bund (fedpol) schon heute Informationssysteme betreibt, die einen Austausch von Informationen unter den Kantonen und mit dem Bund ermöglichen würden, aber mangels geeigneter kantonaler gesetzlicher Grundlagen dafür nicht vollständig genutzt werden können.

Zu den Bestimmungen betreffend POLAP (2. Kapitel: Gemeinsame Abfrageplattform)

Artikel 9: Betrieb und Nutzung

Gemäss den Ausführungen im erläuternden Bericht handelt es sich bei der Abfrageplattform in Artikel 9 primär um POLAP, doch könnte es sich auch um andere Abfrageplattformen handeln (Ausführungen zu Art. 9 Abs. 1, S. 22.). Nun wird aber fedpol POLAP zusammen mit dem technischen Leistungserbringer ISC-EJPD für den Bund und die Kantone betreiben. Insofern ist die Formulierung von Artikel 9 Absatz 1 des Konkordats nicht passend, da sie gerade POLAP nicht betrifft. Für andere Abfrageplattformen kann die vorgeschlagene Bestimmung durchaus als gesetzliche Grundlage angesehen werden. Für POLAP ist dies aber nicht der Fall. In diesem Sinne regen wir eine dahingehende Ergänzung des Titels von Kapitel 2 an, dass es sich um POLAP und weitere von den Teilnehmenden betriebene Abfrageplattformen handeln kann. Zudem erlauben wir uns den Hinweis, dass die Bestimmungen betr. Abfrageplattform(en) so ergänzt und präzisiert werden sollten, dass sie die vom Bund betriebene POLAP und weitere von den Teilnehmenden betriebene Abfrageplattformen regeln. Artikel 9 sollte entsprechend um eine Bestimmung ergänzt werden, welche auch eine Grundlage für die Nutzung von POLAP bzw. generell vom Bund betriebene Abfrageplattformen durch die Teilnehmenden schafft.

Weiter sollten die Bestimmungen so formuliert sein, dass sie mehr als eine von den Teilnehmenden betriebene Abfrageplattform ermöglichen. So sollte zum Beispiel in Artikel 9 Absatz 1 die Pluralform verwendet werden, da ansonsten der Eindruck entstehen könnte, dass es sich nur um eine Abfrageplattform handeln darf. In der ganzen Vereinbarung ist darauf zu achten, dass die Formulierungen nicht nur eine Abfrageplattform zulassen würden.

Artikel 10: Verantwortlichkeit und Rechte der betroffenen Personen

Zu Artikel 10 Absatz 4 ist festzuhalten, dass auf die in POLAP stattfindenden Datenbearbeitungen klarerweise das Bundesgesetz über den Datenschutz (DSG, SR 235.1) zur Anwendung gelangen wird, da hier der Bund (fedpol) als Verantwortlicher gemäss Artikel 5 Buchstabe j DSG handeln wird. Entsprechend wird auch der EDÖB seine gesetzliche Aufsichtsfunktion bezüglich der in POLAP stattfindenden Datenbearbeitung wahrnehmen müssen. Das ergibt sich aus dem DSG und müsste für POLAP nicht ausdrücklich geregelt werden.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme bei den weiteren Arbeiten an der interkantonalen Vereinbarung. Für Rückfragen oder Bemerkungen können Sie sich gerne an kpr-ks@fedpol.admin.ch wenden.

Freundliche Grüsse

Nicoletta della Valle
Direktorin

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Vorsteher des Eidgenössischen Justiz- und Polizeidepartements EJPD

P.P. CH-3003 Bern GS-EJPD POST CH AG

Konferenz der Kantonalen Justiz- und
Polizeidirektorinnen und -direktoren KKJPD
Per Mail an: info@kkjpd.ch

Bern, 22. Februar 2024

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme

Sehr geehrte Frau Präsidentin, sehr geehrter Herr Präsident

Ich nehme Bezug auf Ihr Schreiben vom 23. November 2023 und danke Ihnen für die Möglichkeit zur Stellungnahme. Fedpol hat in meinem Auftrag eine detaillierte Stellungnahme erarbeitet, die ich Ihnen gerne in der Beilage zukommen lasse.

Für den Bund bleibt das Schaffen von konkreten gesetzlichen Grundlagen für die polizeiliche Abfrageplattform POLAP ausserhalb von gerichtspolizeilichen Verfahren gemäss Strafprozessordnung das zentrale Anliegen an die interkantonale Vereinbarung. Diese gesetzlichen Grundlagen sind für die Umsetzung von Projekt 3 (Vorgangsdatenbearbeitungssysteme) des Programms POLAP entscheidend. Das Eidgenössische Justiz- und Polizeidepartement (EJPD) unterstützt entsprechend die Stellungnahme von fedpol.

Ich danke Ihnen für die Berücksichtigung der Stellungnahme bei den weiteren Arbeiten und die sehr gute Zusammenarbeit.

Freundliche Grüsse

Beat Jans
Bundesrat

Beilage:

Stellungnahme fedpol 15. Februar 2024 zur interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme

ETAT DE FRIBOURG
STAAT FREIBURG

Kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation – Chorherrengasse 2, 1700 Freiburg

Autorité cantonale de la transparence, de la protection des données et de la médiation ATPrDM
Kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation ÖDSMB

Die Kommission

Chorherrengasse 2, 1700 Freiburg

T +41 26 322 50 08
www.fr.ch/atprdm

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren

Per Mail :
info@kkjpd.ch

Réf: LS/yo 2024-PrD-38/2024-Trans-17/2024-Méd-2
Courriel: secretariatatprdm@fr.ch

Freiburg, 23. Februar 2024

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen

Sehr geehrte Damen und Herren

Gerne nehmen wir zur erwähnten Vorlage Stellung. Aus verfassungs- und datenschutzrechtlicher Sicht ergeben sich einerseits grundsätzliche Vorbehalte und andererseits Hinweise zu einzelnen Bestimmungen des Vereinbarungsentwurfs. Letztere finden Sie in der Tabelle als Beilage zu diesem Schreiben.

Auf grundsätzlicher Ebene stellt sich zunächst die Frage, ob ein Konkordat, das unabhängig von der Höhe der zu schützenden Rechtsgüter bzw. der Schwere der Straftaten, die es zu verhindern oder verfolgen gilt, einen «Polizeidatenraum Schweiz» schaffen will, mit der verfassungsrechtlichen Kompetenzordnung vereinbar ist, welche die Polizeikompetenzen primär den Kantonen zuweist (Art. 3 und 57 BV). Zwar kann es für klar begrenzte Aufgaben sinnvoll oder sogar angezeigt sein, dass sich die Kantone zur besseren Aufgabenerfüllung zusammenschliessen, jedoch entzieht ein derart breit angelegtes Konkordat – zumal wenn es weitreichende Konkretisierungen an die ausführenden Organe delegiert – dem kantonalen Gesetzgeber wesentliche Teile seiner Regelungshoheit.

Ob auf der ganzen Breite des Konkordats ein überwiegendes öffentliches Interesse besteht, welches die Grundrechtseingriffe aus dem Datenaustausch rechtfertigt (Art. 36 Abs. 2 BV), kann mangels einer substanziellen Darlegung der Sachlage nicht beurteilt bzw. darf ohne nachvollziehbare Begründung nicht einfach angenommen werden. Pauschale Hinweise auf einen Vertrauensverlust in der Öffentlichkeit oder das Risiko einer Ausbreitung von internationalen/-kantonalen kriminellen Strukturen genügen nicht als Rechtfertigung, um die von den Kantonen verantworteten Polizeiinformationssysteme für den Datenaustausch zur Erfüllung jeglicher polizeilichen Aufgaben zusammenzuschliessen. Auch wird nicht dargelegt, warum sich die geltend gemachten technischen Hürden nicht durch eine Verbesserung (im Sinne einer Digitalisierung) der Instrumente zur bereits heute zulässigen Amtshilfe als mildere Massnahme beseitigen lassen.

Damit ist auch die verlangte Verhältnismässigkeit (Art. 36 Abs. 3 BV) des angestrebten Datenaustauschs nicht nachvollziehbar dargelegt. Zwar hält der Konkordatsentwurf die

Teilnehmenden sehr allgemein dazu an, die vereinbarten Kompetenzen verhältnismässig wahrzunehmen (Art. 6), jedoch bleibt die Zuordnung zwischen den polizeilichen Aufgaben (Art. 3) und den erlaubten Datenbearbeitungen (Art. 7 und 20) so vage, dass das Konkordat selbst die Einhaltung der Verhältnismässigkeit nicht gewährleistet.

Dass zahlreiche Konkretisierungen erst an die ausführenden Organe delegiert werden (Art. 13 sowie Art. 17 und 18), führt dazu, dass aus dem Konkordat nicht ersichtlich ist, unter welchen Voraussetzungen und innerhalb welcher verbindlicher Schranken die betroffenen Personen – angesichts des Anwendungsbereichs von Art. 3 bei weitem nicht nur Täter/innen, Tatverdächtige oder Störer/innen – mit einem Datenaustausch rechnen müssen. Damit wird das Konkordat schliesslich auch dem Legalitätsprinzip und der verlangten hinreichenden Bestimmtheit von Eingriffsnormen (Art. 5 Abs. 1 und Art. 36 Abs. 1 BV) nicht gerecht.

Soweit das Konkordat aufgrund der Natur der Polizeitätigkeit (die sich nicht abschliessend abstrakt umschreiben lässt) auf unbestimmte Normen angewiesen ist, kann dies durch unabhängige Kontrollen inkl. öffentlicher Berichterstattung – welche im Konkordat bislang fehlen – teilweise kompensiert werden. Wo die Unbestimmtheit von Rechtssätzen zu einem Verlust an Rechtssicherheit führt, muss die Verhältnismässigkeit umso strenger geprüft werden (Urteil 1C_39/2021 des BGer vom 22.11.2022, E. 4.3.2).

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Laurent Schneuwly
Präsident

ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d'Etat CE
Staatsrat SR

Route des Arsenaux 41, 1700 Fribourg

T +41 26 305 10 40
www.fr.ch/ce

Conseil d'Etat
Route des Arsenaux 41, 1700 Fribourg

PAR COURRIEL

Conférence des directrices et directeurs des
départements cantonaux de justice et police CCDJP
Secrétariat général
Maison des Cantons
Speichergasse 6
Case postale
3001 Berne

Courriel : info@kkjpd.ch

Fribourg, le 5 février 2024

2024-84
Convention intercantonale sur l'échange de données à des fins d'exploitation de plateformes de recherche et de systèmes de bases de données communs - Consultation

Madame la Co-Présidente,
Monsieur le Co-Président,

Nous nous référons à la consultation mentionnée en titre et vous remercions de nous y avoir associés.

Par la présente, nous avons l'avantage de vous informer, dans le délai imparti, que le canton de Fribourg soutient pleinement le projet de convention et ne formule aucune remarque particulière à son égard.

En vous remerciant une nouvelle fois de nous avoir consultés, nous vous prions d'agréer, Madame la Co-Présidente, Monsieur le Co-Président, l'assurance de notre considération distinguée.

Au nom du Conseil d'Etat :

Jean-Pierre Siggen, Président

Danielle Gagnaux-Morel, Chancelière d'Etat

L'original de ce document est établi en version électronique

Copie

—

à la Direction de la sécurité, de la justice et du sport, pour elle et le Service de la justice ainsi que la Police cantonale ;
à la Chancellerie d'Etat.

RÉPUBLIQUE ET CANTON DE GENÈVE

POST TENEBRAS LUX

Genève, le 14 février 2024

Le Conseil d'Etat

750-2024

Conférence des directrices et directeurs
des départements cantonaux de justice
et police (CCDJP)
Madame Karin Kayser-Frutschi
Co-Présidente
Monsieur Alain Ribaux
Co-Président
Maison des cantons
Speichergasse 6
Case postale
3001 Berne

Concerne : convention intercantonale sur l'échange de données à des fins d'exploitation de plateformes de recherche et de systèmes de bases de données communs : réponse à la procédure de consultation

Madame la Co-Présidente,
Monsieur le Co-Président,

Notre Conseil a bien reçu votre lettre du 23 novembre 2023, par laquelle vous avez invité le gouvernement cantonal à se prononcer dans le cadre de la procédure de consultation citée en marge, et vous en remercie.

Notre Conseil soutient les finalités et l'objectif de cette convention, à savoir créer un espace commun pour l'échange de données policières, créer les bases légales formelles de l'échange intercantonal automatisé de données ainsi que les bases nécessaires pour que les cantons puissent collaborer de la même manière avec la Confédération, ceci afin que cette dernière puisse participer aux systèmes d'information, moyennant des conventions de prestations ou en reprenant les ordonnances d'exploitation.

Il est en effet indispensable de faciliter, de fluidifier et de rendre efficace la collaboration entre polices par l'échange de données. Cette convention, qui respecte les compétences cantonales en matière de police, représente le socle incontournable pour atteindre cet objectif et notamment permettre la réalisation du projet POLAP (Polizeiliche Abfrageplattform).

Notre Conseil relève l'équilibre recherché entre la volonté d'augmenter les capacités en matière de coopération policière et la prise en compte explicite de la protection des données, indispensable dès lors que des informations particulièrement sensibles sont concernées.

En vous remerciant d'ores et déjà de l'attention que vous voudrez bien prêter aux observations de notre Conseil, nous vous prions de croire, Madame la Co-Présidente, Monsieur le Co-Président, à l'assurance de notre parfaite considération.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :

Michèle Righetti-El Zayadi

Le président :

Antonio Hodgers

Annexe : analyse détaillée

Copie à (format Word et pdf) : fo@kkjpd.ch

Convention intercantonale sur l'échange de données à des fins d'exploitation de plateformes de recherche et de systèmes de bases de données communs : réponse à la procédure de consultation

Analyse détaillée

Art. 1 Objet et but

L'alinéa 2 mentionne explicitement l'échange de données sensibles, et ce dans une volonté de transparence sur une problématique délicate.

Art. 5 Notions

L'alinéa 1er fait écho à l'alinéa 2 de l'article 1 en posant les définitions liées aux données personnelles et aux questions de profilage qui renvoient à celles utilisées dans la loi fédérale sur la protection des données du 25 septembre 2020 (LPD; RS 235.1).

Art. 6 Principes de traitement

Art. 7 Etendue du traitement des données et de la protection des données

Ces deux articles posent les principes et les limites, ainsi que les conditions à l'échange des données. Les différentes données pouvant être traitées font l'objet d'une énumération détaillée, mais non exhaustive pour des raisons évidentes d'adaptabilité de la convention.

Art. 11 Annonce d'abus

Dans le droit fil de la transparence susmentionnée, ainsi que des principes et des limites à l'échange de données, cet article pose la procédure d'annonce en cas de traitements abusifs de données.

Chapitre 3 – Systèmes de bases de données communs

Sans entrer dans le détail, il convient de souligner ici que les polices cantonales romandes ont mis en place de longue date une base de données communes pour l'analyse des phénomènes sériels (PICAR), puis récemment une nouvelle base destinée à la criminalité sérielle informatique (PICSEL) qui fait l'objet d'une Convention intercantonale et inter-autorités relative à l'échange de données pour exploiter des systèmes du suivi et d'analyse de la situation de la délinquance sérielle. Ces deux outils ont largement dépassé les frontières romandes.

La présente convention offre ainsi un cadre général à la collaboration et au développement de systèmes de bases de données communs.

kanton glarus

Telefon 055 646 60 11/12/15
E-Mail: staatskanzlei@gl.ch
www.gl.ch

Regierungsrat
Rathaus
8750 Glarus

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren KKJPD
Haus der Kantone
Speichergasse 6
3001 Bern

Glarus, 20. Februar 2024
Unsere Ref: 2023-323

Vernehmlassung zur Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme

Sehr geehrte Damen und Herren

Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren KKJPD gab uns in eingangs genannter Angelegenheit die Möglichkeit zur Stellungnahme. Dafür danken wir und lassen uns gerne wie folgt vernehmen:

Die Schaffung einer gemeinsamen, kantonsübergreifenden Datenabfrageplattform ist essenziell. Entsprechend dem Konkordatstext wird befürwortet, dass einerseits einer solchen Plattform die kantonseigenen Daten zur Verfügung gestellt werden können und andererseits der gemeinsame Betrieb dieser Plattform geregelt wird. Auf Stufe Polizeitechnik und –informatik Schweiz (PTI) besteht seitens der KKPKS ein entsprechendes kantonsübergreifendes Projekt. Im Rahmen der geplanten Totalrevision des kantonalen Polizeigesetzes des Kantons Glarus sollen zudem entsprechende Rechtsgrundlagen zum kantonsübergreifenden Datenaustausch vorgesehen werden. Die Vorlage wird insgesamt befürwortet, wobei jedoch auf eine Stellungnahme zu einzelnen Artikeln verzichtet wird.

Genehmigen Sie, sehr geehrte Damen und Herren, den Ausdruck unserer vorzüglichen Hochachtung.

Freundliche Grüsse

Für den Regierungsrat

Benjamin Mühlemann
Landammann

Arpad Baranyi
Ratsschreiber

E-Mail an (PDF- und Word-Version): info@kkjpd.ch

Die Regierung
des Kantons Graubünden

La Regenza
dal chantun Grischun

Il Governo
del Cantone dei Grigioni

Sitzung vom	Mitgeteilt den	Protokoll Nr.
12. Februar 2024	12. Februar 2024	125/2024

Per E-Mail an: info@kkjpd.ch

Vernehmlassung KKJPD - Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme Stellungnahme

Sehr geehrte Damen und Herren

Mit Schreiben vom 23. November 2023 haben Sie uns die Möglichkeit eingeräumt, zum Entwurf der "Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme" sowie den zugehörigen Erläuterungen Stellung zu nehmen. Besten Dank für diese Möglichkeit.

I. Allgemeines

Um die Sicherheit im Kanton Graubünden gewährleisten und die Kriminalität effektiv und effizient bekämpfen zu können, ist ein vermehrter automatisierter Datenaustausch zwischen den eidgenössischen, kantonalen und kommunalen Polizeiorganen erforderlich. Kriminelle Personen agieren mobil, bestens vernetzt und grossräumig, während die Polizeikorps die für die Bekämpfung der Kriminalität relevanten Informationen häufig nur auf Anfrage hin telefonisch oder per E-Mail austauschen können. Diese Diskrepanz in den Mitteln und Möglichkeiten begünstigt die Ausbreitung von kriminellen Strukturen. Der polizeiliche Datenaustausch muss daher auf interkantonaler Ebene stärker aufeinander abgestimmt und vernetzt werden. Aus diesem Grund begrüsst die Regierung des Kantons Graubünden die Schaffung der von der Konfe-

renz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) ausgearbeitete "Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme". Den berechtigten datenschutzrechtlichen Bedenken, die der kantonale Datenschutzbeauftragte und die Konferenz der schweizerischen Datenschutzbeauftragten (privatim) äussern, ist durch eine sorgfältige Konzeption der gemeinsamen Abfrageplattformen und Datenbanksystemen sowie der Implementierung effektiver Kontrollmechanismen Rechnung zu tragen. Es kann nicht zugewartet werden, bis der Bund die rechtlichen Grundlagen geschaffen hat, um den automatisierten polizeilichen Datenaustausch regeln zu dürfen, zumal hierfür mutmasslich die Bundesverfassung der Schweizerischen Eidgenossenschaft revidiert werden muss. Die betreffenden Regelungen, sollten sie denn geschaffen werden, werden dereinst die "Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme" ablösen. Bis dahin braucht es diese Vereinbarung.

II. Bemerkungen zu einzelnen Bestimmungen

Zu Art. 3

Der kantonale Datenschutzbeauftragte und Privatim fordern, den Anwendungsbereich der "Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abgabeplattformen und Datenbanksysteme" im Grundsatz auf die Strafverfolgung zu beschränken. Dieser Forderung kann nicht entsprochen werden. Für die Kriminalitätsbekämpfung ist insbesondere das Aufgabenfeld "Ermittlung" von grosser Bedeutung. Dieses umfasst sowohl die polizeilichen Vorermittlungen als auch die strafprozessualen Ermittlungen. Für die effektive Kriminalitätsbekämpfung ist es sehr wichtig, dass polizeiliche Daten nicht erst dann ausgetauscht werden können, wenn ein Strafverfahren eröffnet ist, sondern bereits im Vorfeld eines solchen. Oft lässt sich ein konkreter Verdacht auf eine strafbare Handlung – welcher für die Eröffnung eines Strafverfahrens bzw. für das Auslösen von weiteren Massnahmen notwendig ist – nur dann erhärten, wenn Informationen bezüglich weiterer, kantons- oder grenzüberschreitender Aktivitäten einer Person oder Gruppierung vorliegen. Von grosser Relevanz in den Bereichen der Deliktsverhinderung und -bekämpfung sowie der Gefahrenabwehr und des Gewaltschutzes sind jedoch auch die frühzeitigen und jederzeit verfügbaren Informationen über beispielsweise die Aktivität von

grenzüberschreitenden Diebesbanden und Betrügerinnen beziehungsweise Betrügern sowie über das Gewaltpotenzial von Einzelpersonen und Gruppierungen. Der Kanton Graubünden begrüsst es deshalb, dass darauf verzichtet wird, den Anwendungsbereich der "Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme" auf die Strafverfolgung zu beschränken.

Zu Art. 11

Art. 11 Abs. 1 legt nicht fest, wer meldepflichtig ist. Laut den Erläuterungen trifft die Meldepflicht die Kantone. Es erscheint sinnvoll, die Regelung in diesem Punkt gleich abzufassen, wie Art. 11 Abs. 2 und die Teilnehmenden zu verpflichten, der für die Abfrageplattform zuständigen Stelle des Bundes und den anderen betroffenen Teilnehmenden missbräuchliche Datenbearbeitungen zu melden.

Zu Art. 17 und 18

Für jedes gemeinsame Datenbanksystem bedarf es einer Betriebsverordnung. Hierbei handelt es sich um eine Verordnung, mit welcher die "Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abgabeplattformen und Datenbanksysteme" in Bezug auf ein konkretes gemeinsames Datenbanksystem präzisiert wird. Die strategische Versammlung von PTI wird in der "Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abgabeplattformen und Datenbanksysteme" ermächtigt werden, entsprechende Verordnungen zu erlassen. Welches Rechtsetzungsverfahren anwendbar sein wird, wird nicht ausdrücklich festgelegt. Womöglich gilt hier aufgrund von Art. 4 das Berner Recht. Sollte dies nicht der Fall sein, so richtet sich das Verfahren zum Erlass der Betriebsverordnungen nach dem jeweils massgeblichen kantonalen Recht. Für den Kanton Graubünden würde dies bedeuten, dass Betriebsverordnungen in Deutsch, Romanisch und Italienisch zu erlassen und zu publizieren sind. Sollte dies nicht sichergestellt werden können, ersucht die Regierung des Kantons Graubünden, den Erlass und die Publikation von Betriebsverordnungen in der "Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme" besonders zu regeln.

Zu Art. 23

Art. 23 Abs. 1 legt nicht fest, wer meldepflichtig ist. Ausserdem ist unklar, in welchem Verhältnis die Informationspflicht des Verantwortlichen gemäss Art. 23 Abs. 2 und die Meldepflicht gemäss Art. 23 Abs. 1 steht. Art. 23 sollte hinsichtlich dieser beiden Punkte präzisiert werden.

Wir bedanken uns für die Möglichkeit zur Stellungnahme.

Namens der Regierung

Der Präsident: Der Kanzleidirektor:

Dr. Jon Domenic Parolini Daniel Spadin

JURA CH RÉPUBLIQUE ET CANTON DU JURA GOUVERNEMENT

Hôtel du Gouvernement
2, rue de l'Hôpital
CH-2800 Delémont

t +41 32 420 51 11
f +41 32 420 72 01
chancellerie@jura.ch

Hôtel du Gouvernement – 2, rue de l'Hôpital, 2800 Delémont

Secrétariat général de la CCDJP
Maison des cantons
Speichergasse 6
3001 Berne

Par email : info@kkjpd.ch

Delémont, le 13 février 2024

Convention intercantonale sur l'échange de données à des fins d'exploitation de plateformes de recherche et de systèmes de bases de données communs – consultation

Madame la co-Présidente,
Monsieur le co-Président,

Le Gouvernement de la République et Canton du Jura accuse réception de votre courrier du 23 novembre 2023 concernant le projet de Convention intercantonale sur l'échange de données à des fins d'exploitation de plates-formes de recherche et de systèmes de bases de données communs. Il vous remercie de l'avoir consulté et prend position comme il suit.

En préambule, le Gouvernement tient à saluer le projet de Convention intercantonale qui lui est soumis dans la mesure où il vise à améliorer et simplifier l'échange de données entre les différentes autorités de police en permettant le recoupement de leurs informations. Il ne fait aucun doute que le travail policier sera ainsi facilité et plus efficient, ce qui permettra une meilleure lutte contre la criminalité au niveau suisse.

Cela étant, le Gouvernement est d'avis qu'un tel projet intercantonal ne peut se faire à satisfaction sans un respect strict des principes de protection des données en vigueur. Par conséquent, les remarques des autorités de protection des données, ainsi que de leur Conférence suisse, PRIVATIM, doivent être prises en compte et le projet adapté en conséquence. En effet, il semble clair que la Convention intercantonale doit obtenir l'approbation de PRIVATIM pour que les traitements de données qui découleront de celle-ci ne soient pas jugés contraire aux principes de protection des données. Si la Convention n'est pas conforme à ces principes, un des risques majeurs est que des poursuites pénales pourraient alors échouer.

Par ailleurs, le Gouvernement tient encore à préciser que le Canton du Jura n'a pas prévu pour le moment d'intégrer dans sa loi sur la police cantonale la disposition X2 « Collaboration électronique » proposée par la CCDJP et qui figure en page 37 du rapport explicatif. En effet, cette disposition telle que prévue n'emporte pas l'aval du préposé à la protection des données Jura-Neuchâtel, pour la raison notamment que la validité de celle-ci au regard des principes de protection des données est remise en cause par PRIVATIM.

En vous remerciant de l'attention portée à la présente, le Gouvernement de la République et Canton du Jura vous prie de croire, Madame la co-Présidente, Monsieur le co-Président, à l'expression de sa parfaite considération.

AU NOM DU GOUVERNEMENT DE LA
RÉPUBLIQUE ET CANTON DU JURA

GOUVERNEMENT DE LA RÉPUBLIQUE ET CANTON DU JURA

Rosalie Beuret Siess
Présidente

Jean-Baptiste Maître
Chancelier d'État

Konferenz der Städtischen Sicherheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs de la sécurité des villes suisses
Conferenza delle direttrici e dei direttori di sicurezza delle città svizzere

Per E-Mail
KKJPD
Generalsekretariat
info@kkjpd.ch

Zürich, 22. Februar 2024

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme; Vernehmlassung

Sehr geehrte Frau Co-Präsidentin, sehr geehrter Herr Co-Präsident

Im Namen der Konferenz der Städtischen Sicherheitsdirektorinnen und -direktoren KSSD danken wir Ihnen für die Einladung zur Vernehmlassung.

Die KSSD begrüsst den vorliegenden Entwurf ausdrücklich. Der Erlass der Vereinbarung würde einen grossen Fortschritt für die polizeiliche Ermittlungsarbeit bedeuten. Wir teilen die Einschätzung der KKJPD, dass ein solcher namentlich in Bereichen wie der Bekämpfung von Terrorismus oder der transkantonalen und internationalen Schwerstkriminalität dringend notwendig ist. Zugleich regen wir dazu an, den datenschutzrechtlichen Bedenken Rechnung zu tragen. Der Austausch ist auf sicherheitsrelevante Daten zu konzentrieren. Wir raten davon ab, die Vorlage zu überladen, gerade weil sie in vielen Kantonen politisch ohnehin umstritten sein dürfte.

Zum Verordnungstext haben wir folgende Anmerkungen:

Hinweis zu Art. 3 (Anwendungsbereich) lit. f.:
Wir regen zu einer Überprüfung an, ob der Austausch von Daten, die bei der *Durchführung verwaltungspolizeilicher Bewilligungsverfahren und Massnahmen* erhoben werden, tatsächlich nötig ist. Bewilligungsverfahren sind zum Teil kommunalrechtlich geregelt. Nicht immer ist die Polizei die Bewilligungsbehörde (z.B. bei Veranstaltungen).

Änderungsantrag zu Art. 17 (Betriebsverordnung):
…
3. Betriebsverordnungen und ihre Änderungen bedürfen der Genehmigung durch das im teilnehmenden Kanton oder in der teilnehmenden Gemeinde für den Erlass einer Verordnung kompetente Organ (Verordnungsinstanz). …

Begründung: Teilnehmende am Datenaustausch sind nach Art. 1 Abs. 1 *polizeiliche Behörden der Kantone und der Gemeinden*. Die Betriebsverordnungen regeln wesentliche Aspekte, u.a. gemäss

Konferenz der Städtischen Sicherheitsdirektorinnen und -direktoren (KSSD)
c/o Sicherheitsdepartement, Bahnhofquai 3, Postfach, 8021 Zürich
Telefon +41 44 411 70 26
info@kssd.ch, www.kssd.ch

Art. 29 den Verteilschlüssel für die Kosten. Daher ist auch eine Genehmigung durch das zuständige Organ einer teilnehmenden Gemeinde vorzusehen.

Wir danken Ihnen für die Berücksichtigung dieser Stellungnahme.

Freundliche Grüsse

Konferenz der Städtischen Sicherheitsdirektorinnen und -direktoren

Co-Präsidentin

Sonja Lüthi
Direktion Soziales und Sicherheit St. Gallen

Co-Präsident

Martin Merki
Sozial- und Sicherheitsdirektion Luzern

Kopien:
- Justiz- und Sicherheitsdepartement des Kantons Basel-Stadt
- Direktion für Sicherheit, Umwelt und Energie der Stadt Bern
- Direction de la sécurité et de l'économie Lausanne
- Dicastero Sicurezza e Spazi urbani della Città di Lugano
- Sozial- und Sicherheitsdirektion der Stadt Luzern
- Direktion Soziales und Sicherheit der Stadt St. Gallen
- Departement Sicherheit und Umwelt der Stadt Winterthur
- Sicherheitsdepartement der Stadt Zürich
- Schweizerische Vereinigung Städtischer Polizeichefs SVSP
- Städtevereinigung der Schutz- und Rettungsorganisationen
- Schweizerischer Städteverband

KANTON
LUZERN

Justiz- und Sicherheitsdepartement
Bahnhofstrasse 15
Postfach 3768
6002 Luzern
Telefon 041 228 59 17
jsdds@lu.ch
www.lu.ch

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)

per E-Mail
info@kkjpd.ch

Luzern, 23. Januar 2024

Protokoll-Nr.: 77

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme; Vernehmlassung

Sehr geehrte Damen und Herren

Für die Gelegenheit, im Rahmen des oben genannten Vernehmlassungsverfahrens Stellung nehmen zu können, danken wir Ihnen. Im Namen und Auftrag des Regierungsrates erlauben wir uns folgende Bemerkungen:

1. Allgemeine Bemerkungen

Wir begrüssen die Schaffung einer interkantonalen Rechtsgrundlage für den polizeilichen Datenaustausch. Die zu erarbeitende gemeinsame Abfrageplattform POLAP und die entsprechenden Datenbanksysteme werden einen wirksamen polizeilichen Datenaustausch ermöglichen und damit wesentlich zu einer effizienten Strafverfolgung beitragen.

Im Kanton Luzern wurden mit der Änderung vom 24. Oktober 2022 des Gesetzes über die Luzerner Polizei (PolG; SRL Nr. 350) die Grundlagen für den Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme geschaffen (§§ 4^{octies}, 4^{sexies} und 4^{novies} PolG). Deren Legitimierung wird aber deutlich gestärkt, wenn auch im interkantonalen Recht dafür Grundlagen geschaffen werden, zumal es sich um interkantonale Systeme handelt. Weiter erleichtert eine solche Grundlage die Zusammenarbeit mit denjenigen kantonalen Polizeikorps, welchen die entsprechenden eigenständigen gesetzlichen Grundlagen fehlten.

Aus unserer Sicht wäre eine Regelung auf nationaler Ebene wünschenswert und nach wie vor anzustreben. Damit die Plattform und die entsprechenden Datenbanksysteme allerdings

möglichst bald in Betrieb genommen werden können, sehen wir die Notwendigkeit einer interkantonalen Vereinbarung.

Da über die Plattform POLAP Daten aus kantonalen, nationalen und internationalen Datenbanksystemen ausgetauscht werden, sollte die Verantwortung für den Betrieb und die Nutzung der Plattform zentralisiert und einer einzigen Behörde oder Institution (wie z. B. dem Bundesamt für Polizei Fedpol) überbunden werden. Dadurch würde verschiedenen Aspekten Rechnung getragen. Einerseits könnte die betreffende Behörde oder Institution einheitliche technische Vorgaben für den Anschluss der Quellsysteme, für die Protokollierung der Datenbearbeitungen und für die Kontrolle des Einhaltens dieser Vorgaben erlassen. Andererseits würde es Betroffenen ermöglicht, ihre Rechte zentral und nicht nur für die einzelnen Quellsysteme auszuüben. Bei Fehlen einer Behörde oder Institution mit Gesamtverantwortung könnten betroffene Personen beim verantwortlichen Organ jeweils nur eine Teilauskunft verlangen und erhalten. Wir empfehlen daher zentralisiert die Überbindung der Gesamtverantwortung für den Betrieb und die Nutzung der Plattform POLAP an eine einzige Behörde oder Institution (wie z. B. Fedpol).

Aus technischer Sicht ist für den Anschluss der kantonalen Informationssysteme an die Abfrageplattform sinnvollerweise ein Schnittstellen-Standard zu definieren. Nur so kann eine einfache und rasche Anbindung gewährleistet werden. Überdies empfehlen wir, den Bereichen IAM (Identity Access Management), Authentifizierung und Protokollierung besondere Aufmerksamkeit zu schenken. Schliesslich ist zu berücksichtigen, dass sehr wahrscheinlich zusätzliche Kosten für erforderliche Anpassungen gemäss der NSP (Network Security Policy) beziehungsweise dem Zonenkonzept entstehen werden.

2. Bemerkungen zu den einzelnen Bestimmungen

Zu den Artikeln 1 und 3
Der Gegenstand und Zweck (Art. 1) sowie der Anwendungsbereich (Art. 3) des Konkordates sind aus datenschutzrechtlicher Sicht eher breit umschrieben. Sie sollten eingeschränkt werden, weil diejenigen Personendaten, die die Polizei bearbeitet und die in der Abfrageplattform und den Datenbanken ausgetauscht werden sollen, zu einem grossen Teil besonders schützenswert sind. Insbesondere ist die «Verhinderung von Straftaten» (Art. 3 lit. c) genauer zu umschreiben, da nicht alle kantonalen Gesetze gleich weitreichende Präventionsaufgaben haben. Auch der Begriff «verwaltungspolizeiliche Bewilligungsverfahren und Massnahmen» (Art. 3 lit. f) ist sehr unbestimmt. Eine beispielhafte Aufzählung dazu wäre hilfreich.

Zudem würde es die Lesbarkeit der Vereinbarung vereinfachen, wenn statt dem Sammelbegriff «Teilnehmende» die Bezeichnung «Polizeibehörden» verwendet würde.

Zu Artikel 26
Die Vereinbarung sieht eine Löschfrist von zehn Jahren vor. Dies halten wir aus datenschutzrechtlicher Sicht für problematisch. Im Kanton Luzern sind vergleichbare Daten nach fünf Jahren zu löschen. Wir empfehlen auch in der Vereinbarung eine solche Frist festzusetzen.

Zu Artikel 28
Lassen Behörden Personendaten durch Dritte bearbeiten, bleiben sie selbst für das Einhalten der Datenschutzvorschriften verantwortlich. Sie müssen sicherstellen, dass sich die Auftragsbearbeiter ebenso an die Vorschriften zum Schutz der Grundrechte halten, wie sie selbst es tun müssen. Dies erfordert eine entsprechende vertragliche Verpflichtung und geeignete Kontrollen, ob die vereinbarten Pflichten auch tatsächlich eingehalten werden. Ist der Auftragsbearbeiter ein internationaler Anbieter, ist eine wirksame Kontrolle kaum möglich. Die nationalen Ansprechpersonen des Auftragsbearbeiters sind oft nicht in der Lage, verbindliche Angaben (z.B. über den genauen Ort einer Datenbearbeitung) zu machen, und wenn doch, dann handelt es sich meist um eine Momentaufnahme, welche schon morgen wieder überholt sein kann.

Da es sich – wie vorstehend ausgeführt – bei den bearbeiteten Personendaten meist um besonders schützenswerte Daten handelt, sollte von einer Bearbeitung im Ausland (Art. 28 Ziff. 2) abgesehen werden.

Für die Berücksichtigung unserer Stellungnahme danken wir Ihnen.

Freundliche Grüsse

Ylfete Fanaj
Regierungsrätin

LE CONSEIL D'ÉTAT
DE LA RÉPUBLIQUE ET
CANTON DE NEUCHÂTEL

CCDJP
Maison des Cantons
Speichergasse 6
3001 Berne

Par courriel info@kkjpd.ch

Convention intercantonale sur l'échange de données à des fins d'exploitation de plates-formes de recherche et de système de données communs

Madame, Monsieur,

Pour donner suite à votre courriel du 23 novembre 2023 relatif à la procédure de consultation susmentionnée, nous vous prions de bien vouloir prendre connaissance de la prise de position du Canton de Neuchâtel.

De manière générale, le Canton soutient ce nouveau projet et salue l'effort entrepris afin d'en améliorer tant la forme que le contenu. Le caractère modulaire de la structure de la convention est un choix pertinent pour réduire les risques et les obstacles juridiques inhérents à la conduite d'un tel projet. Cette conception permettra d'atteindre de manière plus rapide et plus efficace l'objectif d'harmonisation de l'échange des données de police, qui est incontournable.

Cela étant, d'un point de vue politique, un tel projet n'a de chance d'aboutir que s'il est parfaitement conforme aux règles sur la protection des données. Il conviendra donc encore, avant de la soumettre à ratification dans les cantons, de s'assurer de l'avis formel des préposé-e-s.

Cas échéant, au sein de la police neuchâteloise, Mme Eulalie Malan peut contribuer à l'identification des points potentiellement sensibles et se tient volontiers à disposition.

En vous remerciant de nous avoir associés à cette procédure de consultation, nous vous prions de croire, Madame, Monsieur, à l'assurance de notre haute considération.

Neuchâtel, le 19 février 2024

Au nom du Conseil d'État :

Le président,
A. RIBAUX

La chancelière,
S. DESPLAND

RÉPUBLIQUE ET CANTON DE NEUCHÂTEL * CONSEIL D'ÉTAT *

NE

KANTON NIDWALDEN
LANDAMMANN UND REGIERUNGSRAT
Dorfplatz 2, Postfach 1246, 6371 Stans
Telefon 041 618 79 02, www.nw.ch

CH-6371 Stans, Dorfplatz 2, Postfach 1246, STK

PER E-MAIL
Konferenz der Kantonalen Justiz- und
Polizeidirektorinnen und -direktoren KKJPD
Generalsekretariat
Haus der Kantone
Speichergasse 6
3001 Bern

Telefon 041 618 79 02
staatskanzlei@nw.ch
Stans, 20. Februar 2024

Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksystemen. Stellungnahme

Sehr geehrte Damen und Herren

Mit Schreiben vom 23. November 2023 unterbreitete die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) die Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme unter anderem den Kantonen zur Vernehmlassung. Wir bedanken uns für die Möglichkeit zur Stellungnahme.

Der Kanton Nidwalden befürwortet den vorliegenden Entwurf. Wir verweisen auf unsere nachfolgende Begründung.

1 Begründung

Im Kontext der Kooperation zwischen den Polizeibehörden der Kantone und des Bundes der Schweizerischen Eidgenossenschaft wird festgehalten, dass es aktuell an den erforderlichen gesetzlichen Bestimmungen mangelt, welche einen zügigen und umfassenden Austausch von Daten ermöglichen und dadurch signifikant zur Effektivität und Effizienz polizeilicher Arbeit beitragen würden.

Zur Adressierung dieser legislativen Lücke werden prinzipiell drei Handlungsoptionen identifiziert:

1. die Schaffung einer gesetzlichen Basis auf Bundesebene durch ein Bundesgesetz;
2. die Etablierung einer interkantonalen Vereinbarung im Rahmen eines Konkordats; oder
3. die individuelle Anpassung von Rechtsvorschriften durch jede Behörde auf Kantonsebene, spezifisch durch Modifikationen der kantonalen Polizeigesetze.

Angesichts des Projekts "POLAP" verstärkt sich der politische Druck auf die Bundesbehörden, eine gesetzliche Grundlage zu erarbeiten, die nicht nur für das genannte Projekt adäquat wäre, sondern generell den Datenaustausch zwischen den Kantonen und dem Bund erleichtern würde. Jedoch ist der Weg zur Realisierung einer solchen Grundlage auf Bundesebene als

herausfordernd zu bewerten, da er nicht nur potentiell eine Verfassungsänderung erfordert, sondern aufgrund der Regelung des Datenaustausches auch wahrscheinlich ein Referendum nach sich ziehen würde, was eine Implementierung über viele Jahre verzögern könnte. Eine interkantonale Vereinbarung, obwohl politisch ebenso anspruchsvoll, birgt das Risiko unvollständiger Beteiligung der Kantone, bietet jedoch die schnellste Lösung zur Schaffung einer ausreichenden gesetzlichen Basis für den Datenaustausch zwischen Bund und Kantonen.

Vonseiten des Kantons Nidwalden wird volle Unterstützung für den Entwurf einer Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme zum Ausdruck gebracht. Die Notwendigkeit einer engen Kooperation und eines effizienten Datenaustausches zwischen den kantonalen und bundesstaatlichen Polizeibehörden ist essenziell, um die innere Sicherheit der Schweiz zu gewährleisten. Der vorgeschlagene Weg, eine interkantonale Vereinbarung zu etablieren, die den Zugang zu Daten in kantonalen, nationalen und internationalen Polizei-Informationssystemen gewährt, stellt einen bedeutenden Schritt in diese Richtung dar.

Die gegenwärtige Praxis, Informationen über verdächtige Personen ausschliesslich durch zeitaufwendige Anfragen via Telefon oder E-Mail bei jedem Polizeikorps separat zu erheben, wird als ineffizient und mit erheblichen Sicherheitsrisiken behaftet angesehen, insbesondere in Bezug auf die Bekämpfung von Terrorismus und transnationaler schwerer Kriminalität.

Folglich wird die Einführung einer Gesetzgebung auf interkantonaler Ebene, die den automatisierten Informationsaustausch fördert und beschleunigt, nachdrücklich befürwortet. Die in Aussicht gestellte Vereinbarung leistet einen wesentlichen Beitrag zur Stärkung der Sicherheit und etabliert gleichzeitig den rechtlichen Rahmen für einen effektiven Datenaustausch.

2 Zusammenfassung

Die Umsetzung einer bundesgesetzlichen Lösung würde unbestreitbar die einheitlichste Lösung bieten und sollte aus diesem Grund auch weiterverfolgt werden. Angesichts der politischen und zeitlichen Herausforderungen bei der Umsetzung dieser bundesgesetzlichen Lösung wird die interkantonale Vereinbarung als pragmatische Option begrüsst. Der Kanton Nidwalden bekundet seine Unterstützung für den vorliegenden Entwurf einer interkantonalen Vereinbarung zur Förderung eines schnellen und sicheren Datenaustauschs, um die innere Sicherheit zu stärken und einen rechtlichen Rahmen für den Informationsaustausch zu etablieren.

3 Fazit

Der Regierungsrat Nidwalden bedankt sich für die Möglichkeit zur Stellungnahme und spricht sich für eine interkantonale Vereinbarung aus.

Freundliche Grüsse
NAMENS DES REGIERUNGSRATES

Michèle Blöchliger
Landammann

REGIERUNGSRAT · KANTON NIDWALDEN ·

lic. iur. Armin Eberli
Landschreiber

Geht an:
- info@kkjpd.ch

Kanton
Obwalden

Der Vorsteher des Sicherheits- und Sozialdepartements SSD

CH-6060 Sarnen, Enetriederstrasse 1, SSD

Konferenz der Kantonalen Justiz- und
Polizeidirektorinnen und -direktoren KKJPD

per Mail an:
info@kkjpd.ch

Referenz/Aktenzeichen: OWSTK.4803
Unser Zeichen: ks

Sarnen, 21. Februar 2024

**Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme;
Stellungnahme.**

Sehr geehrte Frau Co-Präsidentin,
sehr geehrter Herr Co-Präsident

Für die Einladung zur Vernehmlassung zur interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme danken wir Ihnen.

Der Kanton Obwalden begrüsst ausdrücklich die Förderung eines interkantonalen polizeilichen Datenaustauschs. In der zunehmend vernetzten Welt verlieren Grenzen für die Strafverfolgung weitgehend ihre Bedeutung und sind primär hinderlich. Selbstverständlich bietet das föderale System der kleinräumigen Schweiz dabei auch Vorteile, namentlich wenn es um die Bekämpfung lokaler Täterschaft geht. Bei mobiler Täterschaft und insbesondere im Bereich der digitalen Kriminalität – bei welcher die Täterschaft vielfach aus dem Ausland agiert – gerät das heutige System jedoch an seine Grenzen. Die bestehenden Probleme könnten mit einem verbesserten und vor allem automatisierten Datenaustausch zwischen den Kantonen, mit der Möglichkeit zur kantonsübergreifenden Recherche und Analyse, zu einem gewissen Teil behoben werden.

Zur Schaffung der entsprechenden gesetzlichen Grundlagen hätten wir eine Lösung über den Bund bevorzugt. Dies hätte unseres Erachtens die schnellste und einfachste Möglichkeit dargestellt. In Ermangelung einer entsprechenden Bereitschaft seitens des Bundes begrüssen wir jedoch die Bemühungen zur Erarbeitung des beabsichtigten Konkordats. Dies im Bewusstsein darüber, dass für die

Sicherheits- und Sozialdepartement SSD
Enetriederstrasse 1, 6060 Sarnen
Tel. +41 41 666 62 19
ssd@ow.ch
www.ow.ch

Umsetzung zahlreiche und komplexe Fragen zur Rechtmässigkeit gemeinsamer Datenräume und Datenbänke geklärt werden müssen.

Im Grundsatz sind wir inhaltlich mit dem Entwurf einverstanden. Zu den einzelnen Artikeln haben wir folgende Anmerkungen:

- Art. 3: Im Bericht wird bei Art. 3 ein Lit. i erwähnt, im Entwurf ist dieser jedoch nicht vorhanden. Der Bericht wäre entsprechend zu korrigieren.
- Art. 6: Dass das Verhältnismässigkeitsprinzip stets zu wahren ist, ist als selbstverständlich anzusehen. Gerade im Bereich der Bagatelldelikte gibt es aber auch Fälle der seriellen Kriminalität, welche hohen volkswirtschaftlichen Schaden verursachen und letztlich auch dem Bereich der organisierten Kriminalität zugeordnet werden können. Dies betrifft bspw. Cyberbetrugsdelikte, welche nur einen geringfügigen Deliktsbetrag generieren, Ladendiebstähle durch mobile Täterschaft, usw. Der Datenaustausch bezüglich solcher Delikte wird zwar mit dem vorliegenden Entwurf nicht ausgeschlossen, in den Erläuterungen wird jedoch darauf hingewiesen, dass der Zugriff auf Personendaten in diesem Bereich zu beschränken ist. Gleiches gilt für die Musterbestimmungen, welche unter dem Titel "Rechtsgrundlage in den kantonalen Polizeigesetzen" im erläuternden Bericht vorgeschlagen werden. Auch hier wird im Mustertext zur elektronischen Zusammenarbeit unter Abs. 1 auf die "Verhinderung oder Erkennung oder Bekämpfung von Verbrechen und Vergehen" abgezielt. Wir schlagen vor, diesen Wortlaut wie folgt zu ergänzen: "Verhinderung oder Erkennung oder Bekämpfung von Verbrechen und Vergehen und weiterer Straftaten von überregionaler Tragweite".

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Christoph Amstad
Regierungsrat

Kopie an:
- Amt für Justiz
- Kantonspolizei
- Kantonaler Datenschutzbeauftragter

Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme; Vernehmlassung

Befunde von PTI / V. 1.0 / 14.2.2024 / Konsolidiert durch D. Hänni, Stv. Direktor

POLAP als Programm
Erläuternder Bericht, Kap. 2 «POLAP», Abs. 2, S. 11: *«Die Arbeiten zur Abfrageplattform sind POLAP zusammengefasst, welches aus drei Projekt-Stufen besteht. Die ersten beiden Projekt-Stufen beinhalten den Anschluss von Bundessystemen und die Anbindung der Schengener Informationssysteme an die POLAP. Die dritte Projekt-Stufe beinhaltet die Anbindung der kantonalen Systeme (Quellsysteme).»*. Bei POLAP handelt es sich um ein Programm, bestehend aus drei Projekten. Dies sind die offiziellen HERMES-Bezeichnungen, HERMES ist die offizielle Projektmethodik von Bund und Kantonen. Daher sind die Begriffe entsprechend anzupassen.

Exportfunktionen bzw. Datenabgleich
Erläuternder Bericht, Kap. 2 «POLAP», Abs.5, S.11: *«POLAP sieht keine Exportfunktion für die abgerufenen Daten vor. Die Daten verbleiben in den Quellsystemen.»* und erläuternder Bericht, Kap. 2 «POLAP», Abs.5, S.11 *«Die Informationen können nur zwecks «Sichtung» aufgerufen werden.»* sowie erläuternder Bericht zu Artikel 10 Abs.1, S.23 *«POLAP zeigt die vorhandenen Daten aus den angeschlossenen Quellsystemen nur zwecks „Sichtung“ an.»*

Diese Aussagen müssen differenziert werden. Der POLAP-Referenzclient sieht keine Exportfunktion vor und so kann hier auch ein «Download» erfolgreich verhindert werden. Mittels Anbindung von Drittanwendungen über die zentrale «POLAP-Core» - Funktionalität kann aber im Einzelfall eine Datenübernahme ermöglicht werden, sofern dazu eine Rechtsgrundlage besteht. Siehe dazu u.a. auch die Ziff. 11, Abschnitt 1 der neuen Webservice Richtlinien des EJPD vom 1. November 2023 – V1.6, auf die der POLAP-Core seine Abfragen legitimiert*: «Die Speicherung von über Webservices bezogenen EJPD Daten auf Systemen und Endgeräten des Servicenutzers ist nur dann zulässig, sofern die anwendbaren Rechtsgrundlagen der EJPD Informatiksysteme dies explizit vorsehen und die explizite Zustimmung des Serviceanbieters vorliegt. Die geplante Speicherung der Daten muss im Lösungskonzept dokumentiert sein.».* Es muss daher sichergestellt werden, dass das über POLAP-Core möglich und zulässig ist, ansonsten wäre es bis auf weiteres nötig, dass Zugriffe auf Bundessysteme mit Exportberechtigungen weiterhin separat angeboten werden müsste, was verhindert werden soll. Bei den relevanten Usecases handelt es sich auch nicht um Massenexport-Funktionen, aber z.B. um den Vergleich der Schreibweise von Namen und bei Bedarf um die Übernahme der richtigen Schreibweise.

POLAP als Plattform von PTI
Erläuternder Bericht, Abschnitt «Artikel 2 Abs. 1», S. 18: *«Damit wird den Kantonen auch die Kompetenz erteilt, ihre Informationssysteme an die „POLAP“ Abfrageplattform des Bundes anzuschliessen.»* - Es gibt keine POLAP Abfrageplattform des Bundes, sondern nur eine von PTI. Hingegen gibt es sehr wohl Quellsysteme des Bundes.

Begriffe: Betrieb von mehreren Teilnehmenden
Konkordat: Art. 5, Abschnitt 6, S.2: *«Gemeinsame Datenbanksysteme sind Informationssysteme mit einer zentralen Datenbank, welche von mehreren Teilnehmenden betrieben werden, um ihre polizeilichen Aufgaben zu erfüllen.»*
Bei gemeinsamen Datenbanksystemen von mehreren Organisationen, werden die System selten von diesen selbst betrieben. Sondern die Nutzerorganisationen beauftragen einen Leistungerbringer damit. Daher schlagen wir folgende Formulierung vor: *«Gemeinsame*

Datenbanksysteme sind Informationssysteme mit einer zentralen Datenbank, welche von mehreren Teilnehmenden genutzt werden, um ihre polizeilichen Aufgaben zu erfüllen. Der Betrieb erfolgt durch einen gemeinsam beauftragten Leistungserbringer».

Drei Arten Systeme – Zuständigkeit Datenschutz
Erläuternder Bericht, Art. 7, Absatz 2 (Nummerierung nicht im Originaltext):

«Somit ergibt sich folgendes Bild:

1. *Für den Bund und bei den Bundessystemen kommen das Datenschutzgesetz und die weiteren Bundesgesetze zur Anwendung.*
2. *Für die Informationssysteme unter diesem Konkordat gelten für die Kantone die anwendbaren Bundesgesetze (insb. BV), die vorliegende Vereinbarung, die Betriebsverordnungen und die PTI-Vereinbarung. Subsidiär kommen auf die Quellsysteme die entsprechenden kantonalen Datenschutzbestimmungen zur Anwendung.*
3. *Für Anwendungen unter der PTI-Vereinbarung findet das kantonale bernische Datenschutzgesetz Anwendung (gemäss PTI-Vereinbarung).»*

Wie ist das konkret anzuwenden? Ist folgende Interpretation korrekt? Falls diese Interpretation falsch sein sollte, ist die Beschreibung zwecks besserer Klarheit anzupassen.

- POLAP: POLAP als Ganzes unterstünde Kategorie «2», wobei für die Anwender des Bundes und die Quellsysteme «1» anwendbar wäre.
- Alle weiteren Systeme von PTI, welche als Rechtsgrundlage das Konkordat brauchen bzw. brauchen werden (z.B. PICAR), beziehen sich auf «2».
- Systeme, wie z.B. AFV, ILB, PolAssist, Onrad, App EP, welche bereits heute ohne Konkordat betrieben werden können, gehören zu «3». Insbesondere zu erwähnen sind aber ILB oder AFV, da sie zwar zentrale Systeme sind mit polizeilichen Daten, aber Dank Mandantentrennung keine gemeinsamen Informationssysteme im rechtlichen Sinn sind, sondern um getrennte Systeme, die technisch auf derselben Infrastruktur betrieben werden.

Datentypen
Konkordat Art. 7, Abschnitt 3: es fehlen Angaben zu Waffen. Waffen können zwar Teil des Ereignisses (Abs. 3 lit. a), Tatmittel (Abs. 3 lit. b) oder Deliktsgut (Abs. 3 lit. e) sein, aber sie sollten allenfalls auch noch separat aufgeführt werden.

Betreiber fedpol und Besteller PTI
Konkordat Artikel 9, Abs. 1 *«Die Teilnehmenden betreiben gemeinsam eine Abfrageplattform.».* Für POLAP ist im Gegensatz dazu im neuen BPI folgende Formulierung vorgesehen: «fedpol betreibt die POLAP für den Bund und die Kantone.» Diese Formulierungen sind aufeinander abzustimmen.

Bei POLAP gilt gemäss Einigung mit fedpol, dass PTI der «Besteller» der Lösung ist und fedpol der «Verantwortliche (gemäss DSG)» und Betreiber ist. Das ISC-EJPD ist wiederum als Sublieferant des fedpol der technische Betreiber. Daher schlagen wir folgende alternative Formulierung für den Konkordatstext vor «*Die Teilnehmenden bestellen gemeinsam Leistungen beim verantwortlichen Betreiber der Abfrageplattform».*

Gegenrechtsklausel
Konkordat Artikel 9, Abs. 3 und Erläuternder Bericht: Nicht in jedem Fall ist ein zwingendes Gegenrecht sinnvoll. Es sind Konstellationen denkbar, bei dem nur eine einseitige Anbindung erfolgen soll. Insbesondere für kantonale Systeme ist die Bestimmung sinnvoll,

hingegen aber problematisch für Benutzergruppen seitens Bund (Militärpolizei, ev. BAZG). Da die Bundesstellen ja nicht Teil des Konkordates sind bzw. sich nur beteiligen können, ist diese Bestimmung sowieso nicht 1:1 anwendbar. Somit schlagen wir die Ergänzung *«…bedingt in der Regel…»* vor.

Log – File oder Protokollierung?
Erläuternder Bericht zu Artikel 10, Absatz 5: *«Das Recht des Teilnehmenden bestimmt, ob ein Log-File gespeichert wird oder nicht.»*. Der Begriff des «Log-Files» ist zu vermeiden, da darunter in der Regel eine technische, temporäre Aufzeichnung von Systeminformationen verstanden wird und nicht die verbindliche Protokollierung der Zugriffe. Vorschlag «Log-File» mit «Protokollierung» ersetzen.

Meldung von missbräuchlichen Datenbearbeitungen an den Bund
Artikel 11, Absatz 1 und erläuternder Bericht *«Missbräuchliche Datenbearbeitungen sind der für die Abfrageplattform zuständigen Stelle des Bundes und den anderen betroffenen Teilnehmenden zu melden.»* Woher leitet sich das ab, dass die Meldung an den Bund muss? Es müsste neutral heissen "an den Verantwortlichen gemeldet…", zumindest wenn man die Terminologie des DSG verwendet. Im Falle von POLAP wäre es das fedpol.

Angeschlossene Systeme kant. Rechts sowie von Bundesrecht
Art. 13, Konkordat, Abs. 3a bzw. Erläuternder Bericht *«Da die angeschlossenen Informationssysteme kantonalem Recht unterliegen [..]».* Was ist mit den Bundessystemen?

Zugriffsberechtigungen
Artikel 24 Konkordat und Erläuternder Bericht: *«Die Verwaltung der Zugriffsberechtigungen erfolgt durch den Leistungserbringer.»* und *«Der Leistungserbringer hat damit sicherzustellen, dass die von den Polizeibehörden bezeichneten Personen in ihrer Organisationseinheit, genügend identifiziert und autorisiert werden, um Abfragen im gemeinsamen Datenbanksystem zu tätigen. Das bedingt, dass die Polizeibehörden die dafür zuständigen Personen den Leistungserbringer im Voraus melden. Der Prozess zur Verteilung der Zugriffsberechtigungen richtet sich nach den anwendbaren Regeln der Polizeibehörde.»* Dazu gibt es zwei Anmerkungen:

- Diese Formulierungen berücksichtigen nicht die Funktionsweise eines modernen IAM Systems (wie PTI IAM NextGen). Dabei werden gemeinsam und systemübergreifend Rollen definiert, denen einerseits der Betreiber/Leistungserbringer entsprechende Zugriffsrechte im System zuweist. Die Teilnehmenden (also die Teilnehmer-organisationen) weisen andrerseits ihren zum Zugriff vorgesehenen Benützenden einer Rolle zu. Der Betreiber/Leistungserbringer protokolliert beim Zugriff, welche Person mit welcher Rolle und welchen Abfrageparameter welche Daten abgefragt hat. Somit werden die Personen **NICHT** im voraus gemeldet. Dafür gibt es keinen Grund.
- Auch hier ist der Begriff "Leistungserbringer" zu überprüfen. Es ist nicht klar, welcher Leistungserbringer hier gemeint ist bzw. zur Anwendung kommt und v.a. wird der Begriff der verteilten Aufgaben in einem föderierten IAM Umfeld nicht gerecht.

Vorschlag für eine passende Formulierung im Konkordatstext: *«Die Verwaltung der Zugriffsberechtigungen erfolgt durch den Betreiber in Zusammenarbeit mit den Teilnehmenden».* In den Erläuterungen ist der Text entsprechend auch anzupassen.

Kostentragung
Artikel 29 Konkordat, 2e und Erläuternder Bericht: *«Anzahl teilnehmende Behörden eines Teilnehmenden.»* Was ist damit gemeint? Dass der Kt. Zürich, wenn er mit drei Organisationen kommt, mehr zahlt als der Kt. Uri mit nur einem Partner? Dies macht in dieser Form keinen Sinn und sollte gestrichen werden.

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren

Per Mail:
info@kkjpd.ch

Bern, 23. Februar 2024

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen; Vernehmlassung

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zur erwähnten Vorlage Stellung nehmen zu können. Aus verfassungs- und datenschutzrechtlicher Sicht ergeben sich einerseits grundsätzliche Vorbehalte und andererseits Hinweise zu einzelnen Bestimmungen des Vereinbarungsentwurfs. Letztere finden Sie in der Tabelle als Beilage zu diesem Schreiben.

Auf grundsätzlicher Ebene stellt sich zunächst die Frage, ob ein Konkordat, das unabhängig von der Höhe der zu schützenden Rechtsgüter bzw. der Schwere der Straftaten, die es zu verhindern oder verfolgen gilt, einen «Polizeidatenraum Schweiz» schaffen will, mit der *verfassungsrechtlichen Kompetenzordnung* vereinbar ist, welche die Polizeikompetenzen primär den Kantonen zuweist (Art. 3 und 57 BV). Zwar kann es für klar begrenzte Aufgaben sinnvoll oder sogar angezeigt sein, dass sich die Kantone zur besseren Aufgabenerfüllung zusammenschliessen, jedoch entzieht ein derart breit angelegtes Konkordat – zumal wenn es weitreichende Konkretisierungen an die ausführenden Organe delegiert – dem kantonalen Gesetzgeber wesentliche Teile seiner Regelungshoheit.

Ob auf der ganzen Breite des Konkordats ein *überwiegendes öffentliches Interesse* besteht, welches die Grundrechtseingriffe aus dem Datenaustausch rechtfertigt (Art. 36 Abs. 2 BV), kann mangels einer substanziellen Darlegung der Sachlage nicht beurteilt bzw. darf ohne nachvollziehbare Begründung nicht einfach angenommen werden. Pauschale Hinweise auf einen Vertrauensverlust in der Öffentlichkeit oder das Risiko einer Ausbreitung von internationalen/-kantonalen kriminellen Strukturen genügen nicht als Rechtfertigung, um die von den Kantonen verantworteten Polizeiinformationssysteme für den Datenaustausch

privatim
c/o Datenschutzbeauftragter des Kantons Bern
Poststrasse 25, CH-3072 Ostermundigen
Tel. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

zur Erfüllung jeglicher polizeilichen Aufgaben zusammenzuschliessen. Auch wird nicht dargelegt, warum sich die geltend gemachten technischen Hürden nicht durch eine Verbesserung (im Sinne einer Digitalisierung) der Instrumente zur bereits heute zulässigen Amtshilfe als mildere Massnahme beseitigen lassen.

Damit ist auch die verlangte *Verhältnismässigkeit* (Art. 36 Abs. 3 BV) des angestrebten Datenaustauschs nicht nachvollziehbar dargelegt. Zwar hält der Konkordatsentwurf die Teilnehmenden sehr allgemein dazu an, die vereinbarten Kompetenzen verhältnismässig wahrzunehmen (Art. 6), jedoch bleibt die Zuordnung zwischen den polizeilichen Aufgaben (Art. 3) und den erlaubten Datenbearbeitungen (Art. 7 und 20) so vage, dass das Konkordat selbst die Einhaltung der Verhältnismässigkeit nicht gewährleistet.

Dass zahlreiche Konkretisierungen erst an die ausführenden Organe delegiert werden (Art. 13 sowie Art. 17 und 18), führt dazu, dass aus dem Konkordat nicht ersichtlich ist, unter welchen Voraussetzungen und innerhalb welcher verbindlicher Schranken die betroffenen Personen – angesichts des Anwendungsbereichs von Art. 3 bei weitem nicht nur Täter/innen, Tatverdächtige oder Störer/innen – mit einem Datenaustausch rechnen müssen. Damit wird das Konkordat schliesslich auch dem *Legalitätsprinzip* und der verlangten hinreichenden Bestimmtheit von Eingriffsnormen (Art. 5 Abs. 1 und Art. 36 Abs. 1 BV) nicht gerecht.

Soweit das Konkordat aufgrund der Natur der Polizeitätigkeit (die sich nicht abschliessend abstrakt umschreiben lässt) auf unbestimmte Normen angewiesen ist, kann dies durch unabhängige Kontrollen inkl. öffentlicher Berichterstattung – welche im Konkordat bislang fehlen – teilweise kompensiert werden. Wo die Unbestimmtheit von Rechtssätzen zu einem Verlust an Rechtssicherheit führt, muss die Verhältnismässigkeit umso strenger geprüft werden (Urteil 1C_39/2021 des BGer vom 22.11.2022, E. 4.3.2).

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Ueli Buri
Präsident privatim

Beilage erwähnt

23.10.2023

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme

Kommentierung privatim vom 23.02.2024

Ingress

gestützt auf

- Art. 2 Abs. 1 i.V.m. Art. 57 und Art. 3 sowie Art. 43a und Art. 48 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101);
- das Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI) vom 13. Juni 2008 (SR 361);
- die Vereinbarung zwischen dem Bund und den Kantonen über die Harmonisierung und die gemeinsame Bereitstellung der Polizeitechnik und -informatik in der Schweiz (PTI-Vereinbarung) vom 2. September 2020 (SR 367.1);

Die Kantone, handelnd durch ihre Justiz- und Polizeidirektorinnen beziehungsweise -direktoren schliessen folgende interkantonale Vereinbarung.

mit dem Ziel, in Bezug auf den polizeilichen Datenaustausch einen gemeinsamen Polizeidatenraum zu schaffen,

mit der Absicht, die formelle Rechtsgrundlage für den interkantonalen automatisierten Informationsaustausch zu schaffen,

mit dem Bestreben, die Zusammenarbeit mittels gemeinsamer Informationssysteme auf der Basis der Kompetenz zum Erlass rechtssetzender Bestimmungen zu ermöglichen,

und mit der Absicht, die notwendigen Grundlagen zu schaffen, damit die Kantone in gleicher Weise mit dem Bund zusammenarbeiten können und der Bund mittels Leistungsvereinbarungen oder durch die Übernahme der Betriebsverordnungen an Informationssystemen teilnehmen kann,

1. Kapitel: Allgemeine Bestimmungen

Artikel 1. Gegenstand und Zweck

1. Die Vereinbarung bezweckt durch eine effiziente Zusammenarbeit der polizeilichen Behörden der Kantone und der Gemeinden (nachfolgend die „Teilnehmenden“) untereinander sowie im Rahmen des Bundesrechts mit dem Bund:
   a. die Gewährleistung der öffentlichen Sicherheit und Ordnung;
   b. die Erkennung und Verhinderung von Straftaten;
   c. Bekämpfung von Kriminalität;
   d. effiziente und koordinierte Ermittlungen.
2. Die Vereinbarung schafft die gesetzlichen Grundlagen für den interkantonalen Austausch von polizeilichen

Die Zwecke nach Art. 1 Abs. 1 sind zwingend einzuschränken:

Bst. a: Muss auf die Gewährleistung der öffentlichen Sicherheit beschränkt werden. Die «öffentliche Ordnung» umfasst viele Gefahren von geringer Intensität, die einen solch weitläufigen Datenaustausch nicht rechtfertigen.

Bst. b: Ist einzuschränken. Grundsätzlich ist das Konkordat auf die repressive Polizeitätigkeit zu beschränken. Die präventive Polizeitätigkeit ist nur im Rahmen eines abschliessenden Kataloges von besonders schwerwiegenden Verbrechen zu erfassen. Als Orientierung kann etwa der Katalog in Art. 260bis StGB dienen.

Daten, inkl. besonders schützenswerter Daten, und den Betrieb gemeinsamer Informationssysteme.

Artikel 2. Gemeinsame Abfrageplattformen und Datenbanksysteme

1. Zu diesem Zweck können die Teilnehmenden:
   a. ihre Informationssysteme an gemeinsame Abfrageplattformen der Kantone und/oder des Bundes anschliessen und polizeiliche Daten im Abrufverfahren zugänglich machen;
   b. gemeinsame Datenbanksysteme schaffen sowie betreiben und zu diesem Zweck im Abrufverfahren polizeiliche Daten zugänglich machen;
   c. mit dem Bund gemeinsame Datenbanksysteme schaffen und betreiben oder die eigenen Informationssysteme im Abrufverfahren zugänglich machen.
2. Das kantonale Recht legt fest, ob und in welchem Umfang die Vereinbarung für die Gemeinden gilt.

Artikel 3. Anwendungsbereich

Im gemeinsamen Polizeidatenraum können für folgende polizeiliche Aufgaben Daten bearbeitet und im Abrufverfahren anderen Teilnehmenden und dem Bund zugänglich gemacht werden:

a. Ermittlung (polizeiliche Vorermittlungen und strafprozessuale Ermittlungen);
b. Personen- und Grenzkontrollen;
c. Verhinderung von Straftaten, insbesondere Gefahrenabwehr und Gewaltschutz;
d. Sach- und Personenfahndung;
e. Lagedarstellung und strategische, operative und taktische Analyse von sicherheits- und gerichtspolizeilichen Daten;
f. Durchführung verwaltungspolizeilicher Bewilligungsverfahren und Massnahmen;
g. Personensicherheitsprüfungen;
h. Verkehrskontrollen.

Indem beinahe jede erdenkliche polizeiliche Aufgabe aufgeführt ist, führt Art. 3 entgegen den Erläuterungen zu keiner Eingrenzung auf bestimmte polizeiliche Aufgabenfelder und genügt gegenwärtig nicht dem Bestimmtheitsgebot. Der Katalog ist folgendermassen einzuschränken:

Bst. c: Gefahrenabwehr und Gewaltschutz gehören zur polizeilichen Präventionstätigkeit und sollen – wenn überhaupt – nur im Rahmen eines abschliessenden Kataloges von besonders schwerwiegenden Verbrechen erfasst werden. Als Orientierung kann etwa der Katalog in Art. 260bis StGB dienen.

Bst. e: Es ist zu spezifizieren, dass im Rahmen dieses Buchstabens nur Sachdaten und keine Personendaten zu bearbeiten sind.

Bst. f: Es ist unklar, was für Bewilligungsverfahren und Massnahmen hier gemeint sind. Der Anwendungsbereich ist auf einen spezifischen und abschliessenden Katalog zu beschränken.

Bst. h: Ist ersatzlos zu streichen. Bei Sach- und Personenfahndungen greift Bst. d.

Artikel 4. Anwendbares Recht

Es gilt die Regelung der PTI-Vereinbarung so weit in dieser Vereinbarung kein abweichender Rechtsrahmen geschaffen wird, insbesondere für die Bereiche Haftung, Kostentragung und Verfahrensrecht.

Allgemein: Die Regelungen des anwendbaren Rechts sind kompliziert, uneinheitlich und zudem teils davon abhängig, ob der Bund beteiligt ist oder nicht (vgl. Art. 10 Abs. 4). Wir empfehlen dringend, hierzu eine klarere Regelung zu finden.

Artikel 5. Begriffe

1. Die Begriffe «Personendaten», «besonders schützenswerte Personendaten», «betroffene Person», «Bearbeiten von Personendaten», «Bekanntgeben», «Profiling» und «Profiling mit hohem Risiko» sowie «Verantwortlicher» richten sich nach dem Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020 (SR 235.1).
2. Abfrageplattformen bezeichnen Systeme und technische Möglichkeiten, um mittels einer Suchfunktion Datenbestände in angeschlossenen Datenbanksystemen abzufragen und darzustellen.

Abs. 1: Es erscheint als sinnvoll, die Begriffe im Anwendungsbereich des Konkordats einheitlich zu definieren. Für einen Vorrang der Begriffsdefinitionen des DSG sehen wir aber keinen Grund, zumal z.B. Art. 5 Bst. c DSG die besonders schützenswerten Personendaten abschliessend definiert, wogegen gewisse kantonale Gesetze eine offene Begriffsdefinition enthalten (z.B. Art. 3 Abs. 4 IDG/BS: «Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht, insbesondere Angaben über: …»). Die Begriffe sind deshalb im Konkordat selbst zu definieren, wobei im staatlichen Kontext auf den Begriff «Profiling mit hohem Risiko» verzichtet werden kann.

Abs. 2: «Bearbeiten» ist jeglicher Umgang mit Daten und nicht abhängig davon, ob die Daten gespeichert

3. Das Abrufverfahren ist eine automatisierte Datenbekanntgabe, bei welcher die Empfängerin oder der Empfänger mit Zustimmung des Verantwortlichen auf der Basis von vordefinierten Bedingungen ohne vorgängige Einzelfallkontrolle entscheidet, wann und welche der Daten abgerufen werden. Es ist eine regelmässige Bekanntgabe in Form einer allgemeinen Zugriffsberechtigung (online).
4. Betriebsverordnungen sind dieser Vereinbarung nachgeordnete rechtsetzende Erlasse, die von der strategischen Versammlung PTI beschlossen oder den Teilnehmenden zur Genehmigung unterbreitet werden.
5. Daten sind Sach- und Personendaten inkl. besonders schützenswerte Personendaten, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von ihrer Darstellungsform und Informationsträger.
6. Gemeinsame Datenbanksysteme sind Informationssysteme mit einer zentralen Datenbank, welche von mehreren Teilnehmenden betrieben werden, um ihre polizeilichen Aufgaben zu erfüllen.
7. Informatikmittel sind Geräte, Einrichtungen und Dienste, wie Computersysteme, -programme, Kommunikationsdienste, die der elektronischen Erfassung, Verarbeitung, Speicherung, Übermittlung, Auswertung, Archivierung oder Vernichtung von Informationen dienen.
8. Informationssystem ist ein Überbegriff für Abfrageplattformen und Datenbanksysteme und bezeichnet ein aus einem oder mehreren Informatikmitteln bestehendes System zur Bearbeitung von Daten.
9. Der Leistungserbringer ist für die Umsetzung der Leistungen verantwortlich. Der Leistungserbringer kann gemäss Art. 10 PTI-Vereinbarung PTI oder ein bezeichneter Dritter sein.
10. Der gemeinsame Polizeidatenraum Schweiz umfasst die Gesamtheit der gemeinsam genutzten oder betriebenen Abfrageplattformen und Datenbanksysteme.
11. Quellsystem bezeichnet das Herkunftssystem der Daten. Dieses kann in der Verantwortung eines Kantons, einer Gemeinde oder des Bundes liegen.

werden oder nicht. Hier liegt also unabhängig davon, ob die Daten «temporär» (ad hoc) oder in einem «fixen Speichermedium» zusammengezogen werden, eine gemeinsame Bearbeitung vor. Auch unabhängig von der Begriffsdefinition ist offensichtlich, dass hier Daten konsolidiert werden, für deren Zusammenzug keine gesetzliche Grundlage besteht. Dieser «ad hoc» Zusammenzug kann sich in gewissen Bereichen positiv auf die Risiken auswirken – so sind beispielsweise «unerlaubte» Auswertungen schwieriger und bei allfälligen einer Kompromittierung des Systems ist die Wahrscheinlichkeit, dass grosse Datenbestände innert kürzester Zeit kopiert werden können, kleiner. Zudem muss beachtet werden, dass eine «Sichtung», ohne das die Daten «kopiert» werden können, schwierig bis nicht umsetzbar ist.

Sowohl bei einer Abfrageplattform als auch bei einem Gemeinsame Datenbanksysteme, bei welchem die Daten «untereinander ausgetauscht» werden, handelt es sich letztlich um Abrufverfahren.

Abs. 9: Es ist unklar, ob der Leistungserbringer ein «Verantwortlicher» im Sinne des Datenschutzrechts ist oder ein «Auftragsbearbeiter». Die Definition ist zudem unvollständig, weil sie «Leistungen» nennt, die ihrerseits nicht definiert sind (welche Leistungen, in wessen Auftrag etc.). Wir empfehlen eine Präzisierung der Definition.

Artikel 6. Bearbeitungsgrundsätze

1. Die Teilnehmenden haben ihre Kompetenzen nach dieser Vereinbarung rechtmässig, im öffentlichen Interesse und verhältnismässig wahrzunehmen.
2. Es dürfen nur diejenigen Daten in ein Informationssystem eingetragen, zugänglich gemacht, bearbeitet, daraus bezogen und eingesehen werden, welche für die Erfüllung der konkreten polizeilichen Aufgabe geeignet und erforderlich sind. Die Bearbeitung muss für die betroffene Person zumutbar sein.
3. Die Grund- und Menschenrechte sind zu wahren.

Artikel 7. Umfang der Datenbearbeitung und Datenschutz

1. Die Teilnehmenden bearbeiten ausschliesslich Daten, welche von Polizeibehörden der Kantone, der Gemeinden, des Bundes oder, sofern zur Erfüllung der polizeilichen Aufgaben notwendig, anderen Behörden und Partnerorganisationen aus dem In- oder Ausland rechtmässig erhoben und bekannt gegeben wurden.
2. Auf die Bearbeitung von Personendaten unter dieser Vereinbarung sind, soweit die Kapitel 2 und 3 keine abweichenden Regelungen definieren, das Datenschutzgesetz für den Bund oder das kantonale Recht für die Kantone anwendbar.
3. Insbesondere dürfen folgende Daten bearbeitet werden:
   a. Angaben zum Ereignis und zum Ereignisort;

Abs. 3: Aufgrund der Offenheit des Regelungsgehalts des Konkordats und der Tragweite der Regelungen erscheint uns die Delegation des Erlasses weiterer Datenkategorien auf die Ebene der Betriebsverordnungen nicht statthaft. Auf den Begriff «insbesondere» ist deshalb zu verzichten.

Bst. c: «Passnummern» ist in «Identifikationsnummern amtlicher Ausweise» enthalten.

b. Angaben zu Modus Operandi und Tatmittel insbesondere zu Hard-, Soft- und Malware;

c. Angaben zur bekannten und unbekannten Täterschaft und zu verdächtigen Personen: Name, Vorname, Geburtsdatum, Geschlecht, Alias Namen, Nationalität, Signalement, Bilder, Identifikationsnummern amtlicher Ausweise, Pass- bzw. Personalnummern, AHV-Nr., Firmen, Telefonnummern, IMEI (International Mobile Station Equipment Identity), IMSI (International Mobile Subscriber Identity), Adressen, IP-Adressen, MAC-Adressen, URI, E-Mail-Adressen, weitere Angaben zu den von dieser eingesetzten Informations- und Kommunikationstechnologien, Namensbezeichnungen in sozialen Medien und Spielen (Pseudonyme, etc.), Registrierungs- und Zugangsdaten (inklusive biometrische Daten) für Accounts und bevorzugte Modi Operandi;

d. Angaben zu geschädigten und weiteren betroffenen natürlichen und juristischen Personen: Name, Vorname, Geburtsdatum, Geschlecht und Kontaktdaten bzw. Firma und sowie Angaben zu Kommunikationsmitteln;

e. Angaben zum Deliktsgut;

f. Angaben zu Fahrzeugen, die in einem Zusammenhang mit dem Ereignis stehen könnten;

g. Angaben zu Fallverbindungen zwischen Ereignissen (situative und auf materiellen oder elektronischen Spuren basierende Verbindungen);

h. Ereignisbilder, Video- und Tonaufnahmen;

i. Angaben von Informationsquellen, wie Zeugen und Auskunftspersonen;

j. Prozesskontrollnummern gemäss Artikel 8 Absatz 3 DNA-Profil-Gesetz;

k. Informationen zu Zahlungsmitteln und Geldfluss;

l. Verfahrensdaten;

m. Angaben zu analogen und digitalen Spuren;

n. Zugangsdaten zu Datenbearbeitungssystemen.

4. Die zu bearbeitenden Datenkategorien und Daten werden in den~~r~~ Betriebsverordnungen der einzelnen Informationssysteme abschliessend bezeichnet.

Artikel 8. Haftung

1. Teilnehmende, ihre Mitarbeitende und Auftragnehmer, soweit ihnen eine öffentliche Aufgabe übertragen ist, haften nach den für sie anwendbaren Rechtsgrundlagen für den Schaden, den sie durch widerrechtliches Bearbeiten von Daten einem anderen Teilnehmenden oder Dritten zufügen.

2. Soweit eine Haftung des Leistungserbringers besteht, tritt anstelle der Staatshaftung die Beitragsverpflichtung nach der PTI-Vereinbarung. Der Haftungsanspruch ist nach dem Prozessrecht des Sitzkantons des Leistungserbringers geltend zu machen.

3. Das Klagerecht des haftbaren Teilnehmenden gegen Mitarbeitende eines anderen Teilnehmenden ist ausgeschlossen.

2. Kapitel: Gemeinsame Abfrageplattform

Artikel 9. Betrieb und Nutzung

1. Die Teilnehmenden betreiben gemeinsam eine Abfrageplattform. Für die Abfrageplattform wird durch die operative Versammlung PTI ein Betriebsreglement erlassen.
2. Der Bund kann sich an Abfrageplattformen beteiligen. Die Anbindung der Informationssysteme des Bundes und der internationalen Informationssysteme richtet sich nach Bundesrecht.
3. Die Nutzung der Abfrageplattform durch die Teilnehmenden bedingt die Anbindung der eigenen entsprechenden Informationssysteme und die Bereitstellung der darin enthaltenen Daten für die Abfrageplattform.
4. Die Teilnehmenden entscheiden über die Anbindung ihrer Informationssysteme an die Abfrageplattform.

Abs. 3 und 4: Während Abs. 3 für die Nutzung der Abfrageplattform im Sinne einer Gegenrechtsklausel den Anschluss von «eigenen entsprechenden» Informationssystemen voraussetzt, überlässt Abs. 4 die Auswahl der Systeme den Teilnehmenden. Damit der Aspekt des Gegenrechts korrekt umgesetzt wird, ist im Betriebsreglement zu beschreiben, welche Mindestanforderungen die Teilnehmenden beim Anschluss ihrer Systeme zu erfüllen haben.

Artikel 10. Verantwortlichkeiten und Rechte der betroffenen Personen

1. Die Verantwortung für die rechtmässige Datenbearbeitung im Quellsystem ändert durch die Anbindung an die Abfrageplattform nicht und verbleibt bei der für das Quellsystem zuständigen Stelle.
2. Teilnehmende, welche über die gemeinsame Abfrageplattform Daten von Informationssystemen (Quellsystemen) von anderen Teilnehmenden abfragen, sind für die weitergehende rechtmässige Bearbeitung der abgerufenen Daten verantwortlich.
3. Die Rechte der betroffenen Personen richten sich nach dem Recht des Verantwortlichen für das angeschlossene Informationssystem (Quellsystem). Diese unterliegen dem entsprechenden kantonalen Recht sowie der dafür zuständigen Aufsicht.
4. Auf die Datenbearbeitung in der Abfrageplattform ist das DSG anwendbar und die Aufsicht obliegt dem EDÖB, wenn sich der Bund an der ~~a~~Abfrageplattform beteiligt oder diese betreibt.
5. Die Datenbekanntgabe mittels Abfrageplattform wird im Quellsystem protokolliert und richtet sich nach den für das Quellsystem geltenden Vorschriften.

Abs. 1: Die *Gesamtverantwortung* für POLAP ist im Konkordat ausdrücklich zu regeln. Gemäss Bemerkung zu Art. 10 Abs. 4 liegt diese beim Fedpol. Die Gesamtverantwortung für die Austauschplattform umfasst u.a. technische Vorgaben für den Anschluss der Quellsysteme, die Verantwortung für das Benutzermanagement (IAM), die Verantwortung für die sichere Datenübermittlung sowie Vorgaben zur Protokollierung sowie Kontrolle der Einhaltung der Vorgaben.

Abs. 3: Diese Regelung trägt den Interessen der betroffenen Personen ungenügend Rechnung: Sinn und Zweck von POLAP ist die Informationskumulierung (durch Austausch) aus verschiedenen Quellsystemen – mit den entsprechenden Folgen für die betroffenen Personen (Täter, Opfer etc.). Es ist fraglich, wie diesem Umstand im Rahmen des Auskunftsrechts Rechnung getragen wird. Die Auskunft nur beim Verantwortlichen für ein einzelnes Quell- bzw. Informationssystem gibt nur eine Teilauskunft. Wie erhalten die betroffenen Personen die Gesamtübersicht über die sie betreffenden Abfragen bzw. «Einsichten» über POLAP? Bei wem und nach welchem anwendbaren Datenschutzrecht (nach bernischem KDSG gemäss Art. 4)?

Abs. 4: Welches Recht ist anwendbar, wenn sich der Bund *nicht* an der Abfrageplattform beteiligt oder diese nicht betreibt. Falls das Fedpol die Betreiberin ist, stellt sich v.a. die Frage, was alles zu dessen Verantwortung gehört (siehe Abs. 1); dass das Fedpol dafür dem DSG untersteht, ergibt sich bereits aus Art. 7 Abs. 2, so dass Abs. 4 nur deklaratorisch wirkt.

Abs. 5: Die Protokollierung von Datenbekanntgaben über die Abfrageplattform muss zwingend einheitlich geregelt sein (auch mit Blick auf Art. 11 und die Rechte der betroffenen Personen). Die Regelung muss vorsehen, dass Suchanfragen protokolliert und deren Rechtmässigkeit mittels periodischer Stichproben überprüft werden. Zudem ist festzulegen, welche Angaben die abfragende Stelle mitliefern muss, damit eine eindeutige Identifikation der abfragenden Person möglich ist. Zu prüfen ist sodann die Normierung der Konsequenzen bei der Feststellung von unrechtmässigen Zugriffen.

Artikel 11. Meldung von Missbrauch

1. Missbräuchliche Datenbearbeitungen sind der für die Abfrageplattform zuständigen Stelle des Bundes und den anderen betroffenen Teilnehmenden zu melden.
2. Die Teilnehmenden ergreifen in Absprache mit dem Leistungserbringer geeignete Massnahmen zum Schutz der Personendaten und um den Schaden für die betroffene Person möglichst gering zu halten.

Abs. 1: Es ist unklar, was genau geregelt werden soll: Kanton A hat ein Informationssystem angeschlossen und protokolliert die Zugriffe der anderen Kantone. Er stellt fest (bzw. wird es wohl zunächst nur ein Verdacht sein können), dass eine Person aus Kanton B missbräuchliche Abfragen getätigt hat. Wer macht jetzt was? Richtig wäre: Kanton A hat das *Recht*, die nötigen Abklärungen zu tätigen, um den Verdacht zu prüfen, und Kanton B hat die *Pflicht*, ihn dabei zu unterstützen.

Abs. 2: Es ist nicht klar, welche Teilnehmenden Massnahmen zu ergreifen haben (Alle Teilnehmenden können nicht gemeint sein).

Artikel 12. Kostentragung

1. Die Finanzierung der gemeinsamen Abfrageplattform richtet sich nach der PTI-Vereinbarung.
2. Die Kostenverteilung für den Betrieb der Abfrageplattform wird in einer separaten Vereinbarung geregelt.
3. Die Teilnehmenden tragen die Kosten für den Betrieb und Anschluss ihrer Informationssysteme.

Artikel 13. Ausführungsbestimmungen

1. Der Leistungserbringer erstellt ein Betriebsreglement, welches für die Teilnehmenden verbindlich durch die operative Versammlung PTI erlassen wird.
2. Im Hinblick auf die Nutzung der Abfrageplattform sind zu regeln:
   a. die Rollen und Zugriffsberechtigungen;
   b. die zur Abfrage zugelassenen Datenkategorien;
   c. die technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit.
3. In Ergänzung haben die Teilnehmenden gemäss ihren rechtlichen Vorgaben folgende Punkte zu regeln:
   a. Bezeichnung des oder der angeschlossenen Informationssysteme;
   b. Regelung der Verantwortlichkeiten für die angeschlossenen Informationssysteme.

Die Rolle des Leistungserbringers ist nicht vollständig geklärt. Wenn er die Rolle eines Auftragsdatenbearbeiters hat, sollte es nicht an ihm liegen, ein Betriebsreglement zu erlassen. Nach Art. 5 Abs. 9 ist er (lediglich) «verantwortlich» für die Umsetzung. Das Betriebsreglement muss u.E. vom Gesamtverantwortlichen – d.h. Fedpol – erlassen werden.

Artikel 14. Änderung des Betriebsreglements

Änderungen des Betriebsreglements werden durch die operative Versammlung PTI beschlossen und bedürfen bei der Teilnahme des Bundes seiner Zustimmung.

Artikel 15. Kündigung

1. Ein Teilnehmender kann den Anschluss seines Informationssystems (Quellsystem) mit einer Frist von 6 Monaten kündigen.
2. Mit Ablauf der Kündigungsfrist aller angeschlossenen Informationssysteme erlischt das Recht des Teilnehmenden, die Abfrageplattform zu nutzen.

3. Kapitel: Gemeinsame Datenbanksysteme

Artikel 16. Gemeinsame Datenbanksysteme

1. Die Teilnehmenden können Datenbanksysteme gemeinsam durch einen Leistungserbringer schaffen und betreiben.
2. Bei der Teilnahme an gemeinsamen Datenbanksystemen machen die Teilnehmenden ihre Daten allen Teilnehmenden zugänglich.
3. Der Bund kann unter Vorbehalt des Bundesrechts an den gemeinsamen Datenbanksystemen durch Abschluss einer Leistungsvereinbarung oder durch Übernahmen der Betriebsverordnung teilnehmen.

Siehe die Bemerkungen zu Art. 3.

Artikel 17. Betriebsverordnung

Abs. 1: Der Verweis auf das Bundesgerichtsurteil in den Erläuterungen ist unpräzise und verwirrend. Das

1. Die Ausführungsbestimmungen für jedes gemeinsame Datenbanksystem werden in einer separaten Betriebsverordnung geregelt.
2. Die Betriebsverordnungen und ihre Änderungen werden durch die strategische Versammlung PTI erlassen.
3. Betriebsverordnungen und ihre Änderungen bedürfen der Genehmigung durch das im teilnehmenden Kanton für den Erlass einer Verordnung kompetente Organ (Verordnungsinstanz). Die Kantone können Absatz 4 für nicht anwendbar erklären.
4. Geringfügige Änderungen der Betriebsverordnung, die keine oder nur untergeordnete materielle Rechtswirkung haben, können durch die strategische Versammlung in einem vereinfachten Verfahren mit einem Einstimmigkeitsbeschluss durchgeführt werden, ohne dass eine neue Genehmigung der Betriebsverordnung durch die Teilnehmenden erforderlich ist.

Artikel 18. Inhalt der Betriebsverordnung

Die Betriebsverordnung legt für jedes gemeinsame Datenbanksystem unter Berücksichtigung der in der vorliegenden Vereinbarung definierten Grundzüge insbesondere folgende Modalitäten fest, soweit diese von der PTI-Vereinbarung abweichen:

a. Name und Zweck des gemeinsamen Datenbanksystems;
b. Mögliche Datenbearbeitungen;
c. die zu bearbeitenden Datenkategorien;
d. Die Zuständigkeiten und Verantwortlichkeiten hinsichtlich des Betriebs der zentralen Datenbanken und des Datenschutzes;
e. Die Zuständigkeit für die Gewährung der datenschutzrechtlichen Betroffenenrechte;
f. Zugriffsberechtigungen auf die jeweilige Datenbank inkl. der Speicherung von Randdaten;
g. Gewährleistung der Rechtmässigkeit und Richtigkeit der Daten;
h. Aufbewahrung und Löschung von Daten;
i. Das anwendbare Recht gemäss Art. 21;
j. Regelung der Auftragsbearbeitung im Rahmen des anwendbaren Datenschutzrechts;
k. Regelung zur Kostentragung und Finanzierung, inklusive die finanziellen Folgen des Austritts eines Teilnehmenden aus einem gemeinsamen Datenbanksystem sowie allfälliger Liquidationskosten;
l. Regelung zur Haftung gemäss Art. 8 der Teilnehmenden im Innenverhältnis für Schäden aus unrechtmässiger Datenbearbeitung oder mangelnder Sorgfalt;
m. Regelung zum Beitritt, Kündigung und Austritt.

Artikel 19. Betriebsreglement

Die operative Versammlung PTI erlässt und aktualisiert ein Betriebsreglement. Es enthält insbesondere Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit.

Urteil befasst sich gerade nicht mit einem Konkordat und darauf gestützte Betriebsverordnungen, sondern mit einem kantonalen Polizeigesetz. Richtig ist, dass eine zulässige Gesetzesdelegation an den Verordnungsgeber voraussetzt, dass sich die Delegation auf eine bestimmte, genau umschriebene Materie beschränkt und dessen Umfang klar begrenzt sein muss. Gerade diesen Anforderungen vermag der aktuelle Konkordatsentwurf aufgrund seiner extrem weiten Zweckausrichtung jedoch nicht zu genügen (vgl. allgemeine Bemerkungen).

Abs. 3: Da der Anwendungsbereich des Konkordats ausserordentlich weit ist, ist zu erwarten, dass in den konkreten Datenbanken Datenbearbeitungen vorgesehen werden, die einer formellgesetzlichen Grundlage bedürfen. Diese Bestimmung erweckt den Anschein, dass das Konkordat diese formellgesetzliche Grundlage für alle Arten von Datenbearbeitungen selber darstelle, und nicht nur die Teilnahme am Austausch, was nicht zutrifft.

Bst. b: Siehe die Bemerkungen zu Art. 17 Abs. 3.

Bst. c: Gemäss Art. 6 Abs. 1 Richtlinie (EU) 2016/680 ist zwischen den Daten verschiedener Kategorien betroffener Personen zu unterscheiden. Sinnvollerweise wird dies im Konkordat ausdrücklich vorgesehen.

Bst. d und e: Auch für gemeinsame Datenbanksysteme sind die Gesamtverantwortung zu regeln (vgl. Bemerkungen zu Art. 10 Abs. 1) und der Gesamtsicht (vgl. Bemerkungen zu Art. 10 Abs. 3) Rechnung zu tragen. Dies ist in den Erläuterungen festzuhalten.

Artikel 20. Datenbearbeitungen

1. In gemeinsamen Datenbanksystemen können die Teilnehmenden auch:
   a. Profiling inkl. Profiling mit hohem Risiko zur Verhinderung und Aufklärung von Straftaten nach Art. 269 Abs. 2 der Schweizerischen Strafprozessordung vom 5. Oktober 2007 (SR 312.0) betreiben;
   b. Daten mittels automatisierten Abrufverfahren austauschen;
   c. automatisierte Auswertungen vornehmen.
2. Zudem können Erkenntnisse und Ergebnisse aus Analysen und Lagebildern ausgetauscht werden.
3. Die Teilnehmenden stellen sicher, dass ihre an die Datenbank übermittelten Daten rechtmässig und richtig sind.

Für die Formen der Datenbearbeitungen, die hier benannt sind, kann diese Beschreibung resp. Begründung kaum genügen. Alle Buchstaben umfassen die am weitesten in die Grundrechte eingreifenden Datenbearbeitungen und erfordern je sehr spezifische Auseinandersetzungen mit den Techniken bezogen auf die jeweiligen Anwendungszwecke, andernfalls wird hier ein Blankocheck für jede Polizeiarbeit in sämtlichen polizeilichen Tätigkeiten ausgestellt. Ergänzend ist festzuhalten, dass eine so weit gehende Vorlage es in den kantonalen Parlamenten sehr schwer haben dürfte, gerade weil mit einem Entscheid des Parlaments in absehbarer Zukunft keine Entscheidungen in diesen dynamischen Bereichen mehr möglich sein werden.

Artikel 21. Anwendbares Recht

Das anwendbare Recht richtet sich nach:

   a. Dem Bundesrecht, wenn der Bund an einem Datenbanksystem teilnimmt;
   b. Der PTI-Vereinbarung, wenn das Datenbanksystem allen Kantonen zur Teilnahme offensteht;
   c. Der PTI-Vereinbarung oder dem Recht eines Kantons, wenn das Datenbanksystem regional betrieben wird.

Allgemein: Die Regelung ist unklar, weil sie den Eindruck erweckt, als würde beim Betrieb eines gemeinsamen Datenbanksystems immer nur ein Recht zur Anwendung gelangen. Vielmehr müssen in einem ersten Schritt die (Teil-)Verantwortungen zugewiesen (vgl. Art. 18) und in einem zweiten Schritt festgehalten werden, welches Recht für den jeweiligen Träger von Aufgabe und Verantwortung (insbes. Betrieb der zentralen Infrastruktur, Datenlieferung und –abfrage) gilt. So kann z.B. kaum generell das Bundesrecht gelten, nur weil der Bund an einem Datenbanksystem teilnimmt (nur soweit er selbst ein solches technisch betreibt).

Bst. c.: Gemäss Art. 30 Abs. 1 stehen alle gemeinsamen Datenbanksysteme allen Teilnehmern offen, so dass sich das anwendbare Recht immer nach der PTI-Vereinbarung richtet (Bst. b). Was ist mit «regionalem Betrieb» gemeint und wann kommt Bst. c demnach zur Anwendung?

Artikel 22. Organisation

Organisation, Betrieb und Abwicklung gemeinsamer Datenbanksysteme richten sich nach der PTI-Vereinbarung.

Die Bestimmung ist unklar: Die verwendeten Begriffe sind unbestimmt und die PTI-Vereinbarung enthält keine Vorschriften über die «Organisation», den «Betrieb» und die «Abwicklung» von gemeinsamen Datenbanken.

Artikel 23. Meldung von Missbrauch

1. Missbräuchliche Datenbearbeitungen sind dem Verantwortlichen und dem Präsidenten des operativen Ausschusses PTI zu melden.
2. Der Verantwortliche ergreift in Absprache mit dem Leistungserbringer die geeigneten Massnahmen, um die Gefährdung für die Datensicherheit, den Datenschutz und den Schaden für die betroffene Person möglichst gering zu halten. Der Verantwortliche informiert die operative Versammlung PTI zeitnah über den Vorfall und im Anschluss über die getroffenen Massnahmen.

Allgemein: Siehe die Bemerkungen zu Art. 11.

Abs. 1 und 2: Hier wird (erneut) nicht klar, wer der Verantwortliche ist. Laut Erläuterungen zu Abs. 1 wird mit dem Leistungserbringer (als «Verantwortlichem»?) die zentrale Stelle des jeweiligen Informationssystems informiert. Abs. 2 unterscheidet dann wieder zwischen Verantwortlichem und Leistungserbringer.

Artikel 24. Zugriffsberechtigungen

Die Verwaltung der Zugriffsberechtigungen erfolgt durch den Leistungserbringer.

Artikel 25. Protokollierung

1. Die Datenbanksysteme zeichnen jede Einlieferung von Daten, deren Herkunft, jeden Zugriff sowie jede Bearbeitung von gespeicherten Daten auf und speichern die Protokolldaten während mindestens 12 und längstens

Ziff. 1: Eine Aufbewahrung von Protokolldaten während 5 Jahren ist sehr lange. Bewirtschaftete Daten über die Nutzung der elektronischen Infrastruktur werden beim Bund längstens 2 Jahre aufbewahrt (Art. 4 Abs. 1 Bst. b VBNIB)

60 Monaten. Nach Ablauf dieser Frist werden die gespeicherten Protokolldaten gelöscht. Die Betriebsverordnung regelt die effektive Aufzeichnungsdauer.

2. Eine Auswertung der Zugriffe kann nur unter folgenden Voraussetzungen erfolgen:
   a. im Rahmen der Erfüllung der Aufsichtspflicht des zuständigen Organs;
   b. bei einem konkreten Verdacht auf einen Missbrauch des Systems.

Artikel 26. Datenlöschung

1. Daten, die nach dieser Vereinbarung nicht mehr erforderlich sind, werden umgehend, spätestens jedoch nach 10 Jahren gelöscht. Massgebend für den Beginn des Fristenlaufs ist der letzte Datenzuwachs zum letzten erfassten Ereignis.
2. Soweit technisch möglich, werden Daten über geschädigte Personen unabhängig von den Fristen nach Absatz 1 vom Leistungserbringer gelöscht oder anonymisiert, sobald der Bearbeitungszweck es erlaubt.
3. Abweichende Bestimmungen des Bundes gehen Abs. 1 und 2 vor.

Abs. 1: Die Regelung ist unklar: Daten, die weder für die direkte Aufgabenerfüllung (sog. «aktive Phase» des Lebenszyklus') noch für den späteren Nachvollzug während einer bestimmten Aufbewahrungsfrist (sog. «semi-aktive Phase») benötigt werden, sind ohne weiteren Aufschub zu löschen. Was vielleicht gemeint ist:

- Die Datenhaltung im Rahmen der «aktiven» Phase (Bereitstellung für die polizeiliche Arbeit) dauert solange, bis der betreffende «Fall» abgeschlossen ist, danach werden die Daten umgehend gelöscht;
- nach Ablauf der Zeit x seit dem letzten Datenzuwachs werden die Daten unabhängig vom Geschäftsstand gelöscht, wobei das Betriebsreglement x festlegt;
- die Zeit x darf 10 Jahre nicht überschreiten.

Eine Aufbewahrung von Daten zu abgeschlossenen Geschäften im Sinne der semi-aktiven Phase erfolgt nicht im gemeinsamen Datenbanksystem.

Artikel 27. Betroffenenrechte

1. Betroffene Personen können ihre Rechte wie Auskunfts-, Einsichts- und Berichtigungsbegehren gemäss dem anwendbaren Recht nach Art. 4 und 21 dieser Vereinbarung geltend machen.
2. Die Rechte einer betroffenen Person gegenüber der Behörde, welche die Daten in der gemeinsamen Datenbank eingetragen hat oder hat eintragen lassen, bleiben vorbehalten.
3. Eine zentrale Auskunftsstelle erteilt die Auskunft nach Rücksprache mit der Behörde, welche die Daten eingetragen hat oder hat eintragen lassen.
4. Berichtigungen werden durch den Leistungserbringer nach Rücksprache mit der Behörde, welche die Daten eingetragen hat oder hat eintragen lassen, veranlasst.
5. Betroffenenrechte können aufgrund der Einschränkungsgründe gemäss dem anwendbaren Recht eingeschränkt, aufgeschoben oder verweigert werden.

Ziff. 3: Was ist der Stellenwert der Rücksprache mit der Behörde, von der die Daten stammen: Kann sie die Auskunft verweigern lassen? Und gegen wen richtet sich eine Beschwerde, wenn der Entscheid weitergezogen wird?

Artikel 28. Auftragsbearbeitung

1. Die Bearbeitung der Daten gemäss dieser Vereinbarung erfolgt grundsätzlich in einem sicheren Umfeld in der Schweiz.
2. Die Datenbearbeitung kann im Ausland erfolgen, sofern die Voraussetzungen von Art. 16 DSG erfüllt sind und die Sensitivität der unter dieser Vereinbarung zu bearbeitenden Daten mit geeigneten Massnahmen genügend berücksichtigt wird.
3. Die Auftragsbearbeitung, einschliesslich der Auslagerung des technischen Betriebes an Dritte, ist zulässig, sofern die Bestimmungen dieser Vereinbarung und Art. 9 DSG eingehalten werden. Die Verantwortlichkeiten nach dieser Vereinbarung bleiben bestehen.

Titel: Die Vorschrift regelt zwei Themen – Bearbeitungsort und Auftragsbearbeitung –, die nicht notwendigerweise zusammenhängen, was im Titel abzubilden ist.

Abs. 2: Die Begründung vermengt die Frage nach dem Bearbeitungsort («Ausland») mit jener nach der Person des Datenbearbeiters («Auslagerung»). Aus unserer Praxis ist uns kein Fall bekannt, in welchem eine Auslagerung erfolgt, ohne dass Kosten- und/oder Effizienzgründe vorliegen (ohne solche wäre eine Auslagerung mit den damit verbundenen Risiken kaum verhältnismässig). Entgegen den Erläuterungen bringt die Bestimmung deshalb keine Einschränkung für Auslagerungen.

Polizeidaten sind regelmässig besonders sensitiv und von erhöhtem Schutzbedarf. Deshalb kann eine Auslagerung ins Ausland nur ausnahmsweise und aus triftigen Gründen, d.h. wichtigen öffentlichen Interessen, erfolgen. Reine Kosten- und Effizienzgründe reichen dafür nicht aus (rein finanzielle Interessen stellen auch keine tauglichen öffentlichen Interessen zur Rechtfertigung eines Grundrechtseingriffes nach Art. 36 BV

4. Nimmt der Bund an einem gemeinsamen Datenbanksystem teil, so ist die Auslagerung mit ihm abzusprechen.

dar).

Artikel 29. Kostentragung

1. Jeder Teilnehmende trägt seine eigenen Infrastruktur- und Lizenzkosten.
2. Die Finanzierung und Kosten werden unter den Teilnehmenden an einem gemeinsamen Datenbanksystem aufgeteilt. Anstelle der Kostentragung gemäss der PTI-Vereinbarung kann der anwendbare Verteilschlüssel in der Betriebsverordnung abweichend festgelegt werden. Mögliche Verteilschlüssel sind:
   a. Anteilsmässige Aufteilung analog zu den Artikeln 21 und 22 der PTI-Vereinbarung;
   b. Ständige Wohnbevölkerung;
   c. Datenmenge;
   d. Nutzen für einen Teilnehmenden;
   e. Anzahl teilnehmende Behörden eines Teilnehmenden.
3. Die Verteilschlüssel können kombiniert und mit Sockelbeiträgen verbunden werden.
4. Der Leistungserbringer stellt den Teilnehmenden jährlich die Kostenrechnung zu. Er kann Akontozahlungen verlangen.

Artikel 30. Beitritt

1. Es steht jedem Teilnehmenden dieser Vereinbarung frei, an einem gemeinsamen Datenbanksystem durch die Genehmigung der Betriebsverordnung teilzunehmen. Der Genehmigungsprozess richtet sich nach dem Recht des Teilnehmenden. Die Teilnahme des Bundes richtet sich nach Art. 16 Abs. 3 und dem Bundesrecht.

Ziff. 1: Siehe die Bemerkungen zu Art. 21 Bst. c.

2. Das Gesuch um Teilnahme ist an den Leistungserbringer zu richten.

Artikel 31. Änderung der Betriebsverordnung

Genehmigt ein Teilnehmender die Änderung einer Betriebsverordnung nicht, scheidet er in der festgelegten Übergangsfrist aus dem Informationssystem aus.

Artikel 32. Kündigung und Austritt

1. Unter Einhaltung einer Frist von sechs Monaten kann die Teilnahme an einem gemeinsamen Datenbanksystem auf das Ende eines Kalenderjahres gekündigt werden. Die Kündigung ist schriftlich an den Leistungserbringer zu richten.
2. Mit Eintritt der Kündigungswirkung geht das Recht verloren, das gemeinsame Datenbanksystem zu nutzen. Gleichzeitig entfällt die Kostenpflicht vorbehältlich der Kosten, die mit dem Austritt verbunden sind.
3. Eine Rückerstattung für geleisteten Sach- oder Personalaufwand des ausgetretenen Teilnehmenden ist grundsätzlich ausgeschlossen.
4. Die vom austretenden Teilnehmenden bis dahin eingetragenen Daten werden aus der Datenbank gelöscht, sofern sie nicht in Verbindung zu einem Ereignis stehen, das von einem anderen Teilnehmenden erfasst wurde.

Artikel 33. Liquidation eines gemeinsamen Datenbanksystems

1. Wird der Betrieb eines gemeinsamen Datenbanksystems eingestellt, sorgt der Verantwortliche für die fachgerechte Löschung der Daten. Vorbehalten bleibt die Überführung der Daten in ein Nachfolgesystem.
2. Allfällige Liquidationskosten sind von den Teilnehmenden gemäss dem in der Betriebsverordnung festgelegten Verteilschlüssel zu tragen.

4. Kapitel: Schlussbestimmungen

Artikel 34. Änderungen dieser Vereinbarung

1. Änderungen der Vereinbarung bedürfen der Zustimmung aller Teilnehmenden.
2. Einfache Berichtigungen dieser Vereinbarung, die keine materielle Rechtswirkung haben, können durch die strategische Versammlung PTI in einem vereinfachten Verfahren mit einem Einstimmigkeitsbeschluss durchgeführt werden, ohne dass eine neue Ratifikation der Vereinbarung durch die Teilnehmenden erforderlich ist. Die Kantone können vorsehen, dass dieser Absatz nicht zur Anwendung kommt.

Artikel 35. Beitritt und Kündigung

1. Jeder Kanton kann dieser Vereinbarung jederzeit beitreten. Der Beitritt wird sofort wirksam.
2. Jeder Kanton kann unter Einhaltung einer Frist von sechs Monaten auf das Ende eines Kalenderjahres aus dieser Vereinbarung austreten.
3. Das Beitrittsgesuch sowie die Kündigung sind an die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren zu richten.

Artikel 36. Kantonale Gesetzesanpassungen

Die Kantone erlassen die zum Beitritt und Vollzug dieser Vereinbarung notwendigen Gesetzesgrundlagen oder passen diese an.

Artikel 37. Inkrafttreten

Diese Vereinbarung tritt in Kraft, sobald ihr acht Kantone beigetreten sind.

Artikel 38. Notifikation

Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren informiert die Bundeskanzlei über die vorliegende Vereinbarung. Das Verfahren richtet sich nach der Regierungs- und Verwaltungsorganisationsverordnung (RVOV, SR 172.010.1).

Abs. 2: Die Erläuterungen sprechen von einer Ermächtigung der strategischen Versammlung zum Erlass rechtsetzender Bestimmungen. Dies geht weit über den Begriff der «einfachen Berichtigung, die keine materielle Rechtswirkung haben» hinaus. Die Tragweite der Delegation ist unklar.

In welcher Form können die Kantone eine Nichtanwendbarkeit dieser Bestimmung vorsehen? Und was ist die Folge, wenn einzelne Kantone davon Gebrauch machen?

GS KKPKS - Bern, 24. Oktober 2023

Regierung des Kantons St.Gallen

Regierung des Kantons St.Gallen, Regierungsgebäude, 9001 St.Gallen

Konferenz der Kantonalen Justiz- und
Polizeidirektorinnen und -direktoren
Haus der Kantone
Speichergasse 6
Postfach
3001 Bern

Regierung des Kantons St.Gallen
Regierungsgebäude
9001 St.Gallen
T +41 58 229 89 42
info.sk@sg.ch

St.Gallen, 15. Februar 2024

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme; Stellungnahme

Sehr geehrte Frau Präsidentin, sehr geehrter Herr Präsident

Mit Schreiben vom 23. November 2023 laden Sie uns zur Stellungnahme zum Entwurf einer interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme ein. Wir danken für diese Gelegenheit und äussern uns wie folgt:

Wir sind der Meinung, dass es im Interesse einer wirksamen kantonsübergreifenden oder gesamtschweizerischen Polizeizusammenarbeit (insbesondere zwecks Kriminalitätsverhinderung und -bekämpfung) notwendig ist, dass vermehrt unter den Polizeibehörden des Bundes, der Kantone und der Gemeinden elektronisch zusammengearbeitet werden kann und zu diesem Zweck Daten übermittelt werden können.

Um schweizweit eine verlässliche Grundlage für den Datenaustausch zu schaffen, ist dabei aus unserer Sicht eine nationale Lösung klar zu favorisieren. Wir begrüssen deshalb die von der Sicherheitspolitischen Kommission des Nationalrates eingereichte Motion 23.4311 betreffend die Schaffung einer Verfassungsgrundlage für eine Bundesregelung des nationalen polizeilichen Datenaustauschs. Diese Lösung gilt es rasch voranzutreiben.

Der Kanton St.Gallen ist aktuell im Begriff, eine kantonale Rechtsgrundlage für den interkantonalen Datenaustausch, die auch erhöhten datenschutzrechtlichen Anforderungen genügen sollte, zu schaffen. Wir verweisen hierzu auf die Ergänzungsbotschaft der Regierung vom 21. November 2023 (zu finden unter www.ratsinfo.sg.ch, Geschäfts-Nr. 22.22.23). Mit Art. 39^{quater} des Entwurfs legen wir, gestützt auf die bisherige Mustervorlage und der Rechtsprechung des Bundesgerichtes folgend, eine auf das kantonale Recht aufbauende Regelung des Datenaustauschs vor, der insbesondere dem kantonalen Gesetzgeber grössere Gestaltungsfreiheit einräumt als ein rechtsetzendes Konkordat. Die vorberatende Kommission des Kantonsrates unterstützt diese Regelung; der Kantonsrat wird das Geschäft noch im Februar 2024 in erster Lesung behandeln.

Gleichsam als «dritte Schiene» nebst Bundeslösung (die aber noch erhebliche Zeit beanspruchen wird) und formell-gesetzlicher Regelung im kantonalen Recht befürworten wir

auch die Schaffung der interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme. Als Grundlage der interkantonalen Zusammenarbeit im Polizeibereich ist dieses Konkordat für die Verbreitung des automatisierten, interkantonalen Datenaustausches unter den Polizeibehörden zweifellos hilfreich. Dabei ist anzustreben, alle Kantone oder zumindest eine grössere Zahl mit der vorliegenden Vereinbarung zu einem einheitlich geregelten Datenaustausch zu bringen.

Einzelne Bemerkungen zum Entwurf der interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme finden Sie im Anhang dieses Schreibens.

Wir danken Ihnen für die Berücksichtigung unserer Ausführungen.

Im Namen der Regierung

Stefan Kölliker
Präsident

KANTON ST. GALLEN · REGIERUNG ·

Dr. Benedikt van Spyk
Staatssekretär

Beilage:
Anhang

Zustellung auch per E-Mail (pdf- und Word-Version) an:
info@kkjpd.ch

RRB 2024/118 / Beilage 2

Anhang zur Stellungnahme «Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme»

Im Zusammenhang mit der genannten Vorlage weist die Regierung des Kantons St.Gallen im Einzelnen auf folgende Punkte hin:

Dem vorliegenden Entwurf der interkantonalen Vereinbarung ist nicht zu entnehmen, ob sich diese Vereinbarung als rechtsetzendes Konkordat oder als blosse Verwaltungsvereinbarung versteht. Mit Blick auf das Zustimmungsverfahren – für rechtsetzende Konkordate ist im Kanton St.Gallen ein Beschluss des Kantonsrates mit fakultativem Referendum erforderlich – wie auch mit Blick auf die Zuständigkeit für den Erlass von Ausführungsrecht ist diese Frage indessen von zentraler Bedeutung.

Sodann sollte geprüft werden, ob es auch dem Fürstentum Liechtenstein möglich sein soll, dem vorliegenden Konkordat auf der Grundlage seiner eigenen Gesetzgebung beizutreten. Die Landespolizei Liechtenstein verwendet in vielerlei Hinsicht dieselben Systeme wie die Schweizer Polizeibehörden und beide Seiten würden aufgrund der Grenznähe von der gemeinsamen Zusammenarbeit profitieren.

Bei der Formulierung der Interkantonalen Vereinbarung wurde die bundesgerichtliche Rechtsprechung aus dem Urteil 1C_39/2021 vom 29. November 2022 berücksichtigt. Gemäss unserer Einschätzung ist jedoch der Mustertext, den die Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS) den Kantonen zur Übernahme im kantonalen Recht empfiehlt, im Hinblick auf die bundesgerichtliche Rechtsprechung zu allgemein und zu wenig bestimmt. Einerseits werden die Informationssysteme, die gemeinsam betrieben werden können oder zu welchen Schnittstellen eingerichtet werden, nicht näher umschrieben. Anderseits fehlt eine grobe Umschreibung der Daten, die ausgetauscht werden können. Letzteres ist unseres Erachtens notwendig, damit der geforderten Regelungsdichte der Norm genügend Rechnung getragen wird. Wir verweisen diesbezüglich auf die entsprechende Bestimmung in unserer Ergänzungsbotschaft zum XIV. Nachtrag zum Polizeigesetz (abrufbar unter: www.ratsinfo.sg.ch; Geschäftsnummer 22.22.23 betreffend Art. 39^{quater}).

Im erläuternden Bericht wird den Kantonen empfohlen, gleichzeitig zum Konkordat die kantonalen Rechtsgrundlagen so anzupassen, dass ihre Vertretungen in der strategischen Versammlung PTI die Kompetenz erhalten, die Betriebsverordnungen zu genehmigen. Die Kantone können dann mittels Delegation die Kompetenz zur Genehmigung der Betriebsverordnung an die Vorsteherin oder den Vorsteher des zuständigen Departementes als Mitglied der strategischen Versammlung PTI oder an den Gesamtregierungsrat erteilen oder gar einen Parlamentsbeschluss vorsehen. Derartigen Rechtsetzungsdelegationen stehen wir skeptisch gegenüber; sie verwischen die interkantonalen und die innerkantonalen Rechtsgrundlagen und sind für die Rechtsanwendenden nicht nachvollziehbar.

Art. 5 Ziff. 6 hält fest, dass gemeinsame Datenbanken von mehreren Teilnehmenden betrieben werden. Gemäss unserem Verständnis können solche Systeme aber auch nur von einer einzigen Stelle betrieben werden (zum Beispiel KasewareCH). Eine gemeinsame Datenbank kann also nicht nur bestehen, wenn sie von mehreren Teilnehmenden betrieben wird, sondern auch,

wenn sie lediglich von einer Stelle betrieben, aber von anderen Teilnehmern ebenfalls zum Datenaustausch genutzt wird. Eine solche Datenbank könnte die Nachfolge von Picsel sein, die derzeit im Rahmen des PTI-Projekts allenfalls als Bestandteil von KasewareCH aufgebaut wird.

Art. 7 Ziff. 3 Bst. l erwähnt «Verfahrensdaten», die bearbeitet werden dürfen. Für uns stellt sich hier die Frage nach dem sachlichen Anwendungsbereich. Der Begriff «Verfahrensdaten» ist unserer Einschätzung nach zu unbestimmt und es ist nicht klar, was diese beinhalten – ob damit z.B. Daten aus polizeilichen Vorermittlungen und/oder gerichtspolizeilichen Ermittlungen gemeint sind. Aufgrund des Erfordernis der genügenden Bestimmtheit der Rechtsgrundlage kann nach unserer Ansicht eine Konkretisierung nicht erst in einer Betriebsverordnung gemäss Art.7 Ziff. 4 erfolgen.

Letztlich fehlen im Entwurf Regelungen, ob und wie ein Datenaustausch vorgesehen werden soll mit Kantonen, die der interkantonalen Vereinbarung nicht beigetreten sind, aber ein vergleichbares oder besseres Datenschutzniveau haben. Es stellt sich hier die Frage, ob mit diesen Kantonen kein Datenaustausch möglich sein soll oder ob das Konkordat ermächtigt werden soll, auch mit weiteren Partnern (z.B. mit solchen Kantonen oder auch mit der Transportpolizei des Bundes) allenfalls bilaterale Datenaustauschvereinbarungen abzuschliessen.

Anhang zur Stellungnahme «Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrage-plattformen und Datenbanksysteme»

Im Zusammenhang mit der genannten Vorlage weist die Regierung des Kantons St.Gallen im Einzelnen auf folgende Punkte hin:

Dem vorliegenden Entwurf der interkantonalen Vereinbarung ist nicht zu entnehmen, ob sich diese Vereinbarung als rechtsetzendes Konkordat oder als blosse Verwaltungsvereinbarung versteht. Mit Blick auf das Zustimmungsverfahren – für rechtsetzende Konkordate ist im Kanton St.Gallen ein Beschluss des Kantonsrates mit fakultativem Referendum erforderlich – wie auch mit Blick auf die Zuständigkeit für den Erlass von Ausführungsrecht ist diese Frage indessen von zentraler Bedeutung.

Sodann sollte geprüft werden, ob es auch dem Fürstentum Liechtenstein möglich sein soll, dem vorliegenden Konkordat auf der Grundlage seiner eigenen Gesetzgebung beizutreten. Die Landespolizei Liechtenstein verwendet in vielerlei Hinsicht dieselben Systeme wie die Schweizer Polizeibehörden und beide Seiten würden aufgrund der Grenznähe von der gemeinsamen Zusammenarbeit profitieren.

Bei der Formulierung der Interkantonalen Vereinbarung wurde die bundesgerichtliche Rechtsprechung aus dem Urteil 1C_39/2021 vom 29. November 2022 berücksichtigt. Gemäss unserer Einschätzung ist jedoch der Mustertext, den die Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS) den Kantonen zur Übernahme im kantonalen Recht empfiehlt, im Hinblick auf die bundesgerichtliche Rechtsprechung zu allgemein und zu wenig bestimmt. Einerseits werden die Informationssysteme, die gemeinsam betrieben werden können oder zu welchen Schnittstellen eingerichtet werden, nicht näher umschrieben. Anderseits fehlt eine grobe Umschreibung der Daten, die ausgetauscht werden können. Letzteres ist unseres Erachtens notwendig, damit der geforderten Regelungsdichte der Norm genügend Rechnung getragen wird. Wir verweisen diesbezüglich auf die entsprechende Bestimmung in unserer Ergänzungsbotschaft zum XIV. Nachtrag zum Polizeigesetz (abrufbar unter: www.ratsinfo.sg.ch; Geschäftsnummer 22.22.23 betreffend Art. 39^{quater}).

Im erläuternden Bericht wird den Kantonen empfohlen, gleichzeitig zum Konkordat die kantonalen Rechtsgrundlagen so anzupassen, dass ihre Vertretungen in der strategischen Versammlung PTI die Kompetenz erhalten, die Betriebsverordnungen zu genehmigen. Die Kantone können dann mittels Delegation die Kompetenz zur Genehmigung der Betriebsverordnung an die Vorsteherin oder den Vorsteher des zuständigen Departementes als Mitglied der strategischen Versammlung PTI oder an den Gesamtregierungsrat erteilen oder gar einen Parlamentsbeschluss vorsehen. Derartigen Rechtsetzungsdelegationen stehen wir skeptisch gegenüber; sie verwischen die interkantonalen und die innerkantonalen Rechtsgrundlagen und sind für die Rechtsanwendenden nicht nachvollziehbar.

Art. 5 Ziff. 6 hält fest, dass gemeinsame Datenbanken von mehreren Teilnehmenden betrieben werden. Gemäss unserem Verständnis können solche Systeme aber auch nur von einer einzigen Stelle betrieben werden (zum Beispiel KasewareCH). Eine gemeinsame Datenbank kann also nicht nur bestehen, wenn sie von mehreren Teilnehmenden betrieben wird, sondern auch,

wenn sie lediglich von einer Stelle betrieben, aber von anderen Teilnehmern ebenfalls zum Datenaustausch genutzt wird. Eine solche Datenbank könnte die Nachfolge von Picsel sein, die derzeit im Rahmen des PTI-Projekts allenfalls als Bestandteil von KasewareCH aufgebaut wird.

Art. 7 Ziff. 3 Bst. l erwähnt «Verfahrensdaten», die bearbeitet werden dürfen. Für uns stellt sich hier die Frage nach dem sachlichen Anwendungsbereich. Der Begriff «Verfahrensdaten» ist unserer Einschätzung nach zu unbestimmt und es ist nicht klar, was diese beinhalten – ob damit z.B. Daten aus polizeilichen Vorermittlungen und/oder gerichtspolizeilichen Ermittlungen gemeint sind. Aufgrund des Erfordernis der genügenden Bestimmtheit der Rechtsgrundlage kann nach unserer Ansicht eine Konkretisierung nicht erst in einer Betriebsverordnung gemäss Art.7 Ziff. 4 erfolgen.

Letztlich fehlen im Entwurf Regelungen, ob und wie ein Datenaustausch vorgesehen werden soll mit Kantonen, die der interkantonalen Vereinbarung nicht beigetreten sind, aber ein vergleichbares oder besseres Datenschutzniveau haben. Es stellt sich hier die Frage, ob mit diesen Kantonen kein Datenaustausch möglich sein soll oder ob das Konkordat ermächtigt werden soll, auch mit weiteren Partnern (z.B. mit solchen Kantonen oder auch mit der Transportpolizei des Bundes) allenfalls bilaterale Datenaustauschvereinbarungen abzuschliessen.

Kanton Schaffhausen
Regierungsrat
Beckenstube 7
CH-8200 Schaffhausen
www.sh.ch

T +41 52 632 71 11
F +41 52 632 72 00
staatskanzlei@sh.ch

Regierungsrat

KKJPD

per E-Mail:
info@kkjpd.ch

Schaffhausen, 20. Februar 2024

Vernehmlassung betreffend interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme; Stellungnahme

Sehr geehrte Frau Co-Präsidentin
Sehr geehrter Herr Co-Präsident

Mit Schreiben vom 23. November 2023 haben Sie uns eingeladen, in vorerwähnter Angelegenheit Stellung zu nehmen. Wir danken Ihnen für diese Gelegenheit.

Dem Regierungsrat des Kantons Schaffhausen ist es ein Anliegen, dass zeitnah schweizweit eine Grundlage für den polizeilichen Datenaustausch geschaffen wird, um die Kriminalität künftig effizienter bekämpfen zu können und die innere Sicherheit der Schweiz bestmöglich zu gewährleisten. Wir hoffen, dass eine eidgenössische Regelung geschaffen werden kann (Motion 23.4311 betreffend Schaffung einer Verfassungsgrundlage für eine Bundesregelung des nationalen polizeilichen Datenaustausches). Wir unterstützen aber auch den vorliegenden Weg der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) zur Schaffung einer interkantonalen Vereinbarung für den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme.

Zu einzelnen Bestimmungen haben wir folgende Hinweise anzubringen:

Titel: Der Titel der Vereinbarung ist sehr schwerfällig, weshalb wir anregen, einen knapperen Titel wie "Vereinbarung über den polizeilichen Datenaustausch" zu wählen.

Ingress: Ausführungen zu Sinn und Zweck des Konkordats sollten nicht im Ingress, sondern im nachfolgenden Artikel 1 betreffend Gegenstand und Zweck aufgeführt werden.

Artikel 6 ist nicht optimal formuliert. Wenn schon, sollte in Absatz 1 festgehalten werden, dass die verfassungsmässigen Rechte zu achten sind, was aber ohnehin gilt. Erst hernach sollte der Grundsatz der Verhältnismässigkeit aufgeführt und bezogen auf die Datenbearbeitung konkretisiert werden.

Artikel 12 und 29: Dass sich die Kostenteilung für den Betrieb der gemeinsamen Abfrageplattform und das gemeinsame Datenbanksystem nach der PTI-Vereinbarung richtet, darüber hinaus aber jeder seine eigenen Infrastruktur- und Lizenzkosten trägt, wird ausdrücklich begrüsst.

Artikel 36 sieht vor, dass die Kantone die zum Beitritt und Vollzug dieser Vereinbarung notwendigen Gesetzesgrundlagen erlassen oder diese anpassen. Dies ist eine Voraussetzung für den Beitritt zur Vereinbarung und somit nicht in der Vereinbarung zu normieren.

Wir danken Ihnen für die Kenntnisnahme und Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse
Im Namen des Regierungsrates
Der Präsident:

Patrick Strasser

Der Staatsschreiber:

Dr. Stefan Bilger

Sicherheitsdepartement
Vorsteher

Bahnhofstrasse 9
Postfach 1200
6431 Schwyz
Telefon 041 819 20 15

kantonschwyz

6431 Schwyz, Postfach 1200
Per E-Mail
KKJPD
Haus der Kantone
3001 Bern

info@kkjpd.ch

Unser Zeichen 2023.0616
Direktwahl 041 819 20 00
E-Mail xaver.schuler@sz.ch
Datum 19. Dezember 2023

KKJPD: Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksystemen (POLAP)
Stellungnahme

Sehr geehrte Damen und Herren

Um die innere Sicherheit in der Schweiz zu gewährleisten, ist neben der operativen Zusammenarbeit auch ein effizienter Austausch polizeilicher Daten unabdingbar. Die dazu nötige Vernetzung der Polizeidatenbanken zwischen den Kantonen untereinander sowie mit dem Bund ist bisher jedoch erst ungenügend realisiert.

Der Kanton Schwyz unterstützt, den Prozess für eine interkantonale Gesetzgebung weiterzuverfolgen und stimmt dem in die Vernehmlassung geschickten Entwurf einer interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksystemen zu. Dabei hat der Kanton Schwyz auch die datenschutzrechtlichen Bedenken berücksichtigt und kam im Rahmen einer Güterabwägung zum Schluss, dass das Interesse an einer effizienten Bekämpfung von Terrorismus bzw. transkantonaler und internationaler Schwerstkriminalität überwiegt.

Freundliche Grüsse
Sicherheitsdepartement des Kantons Schwyz

Xaver Schuler, Regierungsrat

Regierungsrat

Rathaus
Barfüssergasse 24
4509 Solothurn
so.ch

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)
Generalsekretariat
Haus der Kantone
Speichergasse 6
Postfach
3001 Bern

20. Februar 2024

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme; Vernehmlassung

Sehr geehrter Herr Generalsekretär
Sehr geehrte Damen und Herren

Mit Schreiben vom 23. November 2023 haben Sie uns zur Vernehmlassung über die Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme eingeladen. Besten Dank für die Gelegenheit zur Meinungsäusserung.

1. Grundsätzliche Bemerkungen

Die Polizei ist in ihrer täglichen Arbeit auf aktuelle, vollständige und rasch verfügbare Informationen zur Kriminalitätsbekämpfung angewiesen. Ohne diese elementare Voraussetzung ist eine effiziente Polizeiarbeit nicht möglich. In der Schweiz fehlt aktuell eine national einheitliche Rechtsgrundlage für den automatisierten Datenaustausch zwischen den kantonalen Polizeibehörden untereinander sowie mit dem Bund. Ausserdem werden unterschiedliche Systeme zur Datenbearbeitung genutzt. Dementsprechend schwerfällig und aufwändig gestaltet sich der heutige Informationsaustausch: Im Nationalen Polizeiindex ist zunächst abzuklären, ob eine andere kantonale Polizeibehörde oder das Bundesamt für Polizei (fedpol) Daten zu einer bestimmten Person bearbeiten. Bestehen Daten, muss die jeweilige Polizeiorganisation im Rahmen der Rechts- und Amtshilfe um weitere Informationen ersucht werden (Art. 17 Bundesgesetz über die polizeilichen Informationssysteme des Bundes [BPI; SR 361]). Die weitgehende Begrenztheit auf die eigenen Informationen und der ineffiziente Informationsaustausch erschweren die präventive und repressive Kriminalitätsbekämpfung über Gebühr.

Die geltenden Bestimmungen über den polizeilichen Informationsaustausch sind der Lebenswelt einer hochmobilen Gesellschaft entsprechend anzupassen, ansonsten die Polizeibehörden ihren gesetzlichen Aufgaben nicht angemessen nachkommen können. Die fehlende Vernetzung birgt das Risiko von Sicherheitsrisiken. Der Handlungsbedarf ist weitgehend unbestritten und dringlich.

Aus diesen Gründen begrüssen wir die Schaffung einer national einheitlichen Rechtsgrundlage vorbehaltlos. Bereits 2018 wurde der Bundesrat in einer Motion beauftragt, eine zentrale nationale Polizeidatenbank oder eine Vernetzungsplattform für die bestehenden kantonalen Polizeidatenbanken zu schaffen[1]. Allerdings muss dafür zunächst eine entsprechende Kompetenznorm in der Bundesverfassung geschaffen werden[2] Wir begrüssen dieses Vorhaben. Während der dafür nötigen Zeit darf der mangelhafte Informationsaustausch jedoch nicht zu einer unangemessenen Beeinträchtigung der öffentlichen Sicherheit führen. Die Unzulänglichkeiten der heutigen Abläufe machen es demnach unerlässlich, einen effizienten, der veränderten Lebenswirklichkeit angepassten Informationsaustausch in einem alternativen, rascher umsetzbaren Rechtsrahmen zu ermöglichen. Um den nötigen polizeilichen Informationsaustausch zumindest mittelfristig sicherzustellen, bietet sich die Regelung in einer interkantonalen Vereinbarung an. Der Vereinbarungsentwurf stellt diese Rechtsgrundlage dar. Vorgeschlagen wird der Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme.

Nicht nur aufgrund des aufgezeigten dringlichen Handlungsbedarfs, sondern auch wegen den Unwägbarkeiten der beabsichtigten Verfassungsänderung verdient der Entwurf grundsätzliche Unterstützung. Berechtigte Fragen wie insbesondere die demokratische Kontrolle im Zusammenhang mit dem Erlass der Betriebsreglemente verdienen allerdings eine vertiefte Klärung.

Der Vereinbarungsentwurf berührt zwei für uns elementare Bereiche: Das öffentliche Interesse an der Gewährleistung der inneren Sicherheit einerseits und die Wahrung der verfassungsmässig garantierten Grundrechte andererseits. Sicherheit und Freiheit schliessen sich nicht aus, sondern bedingen sich gegenseitig. Nur eine fein austarierte Balance vermag beiden Anliegen gleichermassen gerecht zu werden. Bereits eine Unausgewogenheit kann unangemessene Auswirkungen zu Ungunsten eines Anliegens nach sich ziehen.

Im Grundsatz kommt der Vereinbarungsentwurf dieser Vorgabe nach. Er ermöglicht den effizienten Informationsaustausch im nötigen Umfang, ohne in die Rechte der betroffenen Person über Gebühr einzugreifen. Die Polizei ist auch gar nicht an einer Akkumulation von unnötigen Informationen interessiert. Vielmehr erfüllen Polizeiorganisationen ihre Arbeit nur dann effizient, wenn sie bei Bedarf rechtmässig erhobene, sachdienliche und korrekte Informationen rasch und gesichert untereinander austauschen können. Es sind demnach dieselben Grundsätze der recht- und verhältnismässigen Datenbearbeitung, welche sowohl die Effizienz der Polizeiarbeit sicherstellen als auch die verfassungsmässigen Rechte der Betroffenen wahren (vgl. § 16 Informations- und Datenschutzgesetz des Kantons Solothurn [BGS 114.1]).

Die vorgenommenen Güterabwägungen beurteilen wir im Grundsatz als ausgewogen. Die Ausgewogenheit zeigt sich beispielsweise darin, dass der Vereinbarungsentwurf das Betreiben eines Profiling (inklusive Profiling mit hohem Risiko) in einem gemeinsamen Datenbanksystem lediglich zur Verhinderung und Aufklärung bestimmter Straftaten gemäss StPO zulässt (Art. 20).

Dennoch sind einzelne wichtige Punkte vertieft zu überprüfen. Wir regen die Ergänzung des Vereinbarungsentwurfs mit besonderen Kontrollmechanismen sowie Transparenz- und Publikationsvorschriften an. Die Datenbearbeitungen in der gemeinsamen Abfrageplattform (POLAP) und in den betriebenen Datenbanksystemen sind zur Gewährleistung der verfassungsmässigen Nutzung regelmässig (vorzugsweise jährlich) durch ein unabhängiges Kontrollorgan auf ihre Recht- und Verhältnismässigkeit zu überprüfen (vgl. BGE 149 I 218, E. 8.11.2 ff.). Zumindest die Grundzüge der Kontrollmechanismen sind in der Vereinbarung zu regeln. Die Bestimmung könnte wie folgt lauten:

Artikel 7a. Unabhängiges Kontrollorgan

1. *Die strategische Versammlung PTI bestimmt ein unabhängiges Kontrollorgan. Das Kontrollorgan erfüllt seine Aufgaben fachlich selbständig und weisungsungebunden.*

[1] Motion 18.3592 vom 14.06.2018: Nationaler polizeilicher Datenaustausch.
[2] Motion SIK-N 23.4311 vom 10.10.2023: Schaffung einer Verfassungsgrundlage für eine Bundesregelung des nationalen polizeilichen Datenaustausches.

2. *Das unabhängige Kontrollorgan überprüft die nach dieser Vereinbarung erfolgenden Datenbearbeitungen mindestens jährlich auf ihre Verfassungskonformität, insbesondere auf ihre Rechtmässigkeit und Verhältnismässigkeit sowie auf die Einhaltung der Datensicherheit. Sofern es dies als nötig erachtet, kann das Kontrollorgan zusätzliche Kontrollen durchführen.*
3. *Zu diesem Zweck kann das Kontrollorgan bei Behörden und Dritten, die Daten nach dieser Vereinbarung bearbeiten, ungeachtet allfälliger Geheimhaltungspflichten Auskünfte einholen, Unterlagen herausverlangen, Besichtigungen durchführen und sich Datenbearbeitungen vorführen lassen. Die Behörden und Dritte sind zur Mitwirkung verpflichtet.*
4. *Das Kontrollorgan erstattet der strategischen Versammlung PTI und der Bevölkerung jährlich sowie bei Bedarf Bericht über seine Tätigkeit, die durchgeführten Kontrollen, wichtige Feststellungen sowie abgegebene Empfehlungen. Die Berichte werden veröffentlicht.*
5. *Stellt das Kontrollorgan Datenbearbeitungen oder Verwaltungsabläufe fest, die den massgebenden Rechtsvorschriften nicht entsprechen, orientiert es die strategische Versammlung PTI und gibt zuhanden dieser eine schriftliche Empfehlung ab.*
6. *Die strategische Versammlung PTI hat dem Kontrollorgan innert Jahresfrist die Umsetzung der Empfehlung zu bestätigen oder die Gründe, weshalb diese nicht umgesetzt wurde, schriftlich darzulegen.*

Die vorgeschlagene Bestimmung nimmt die Anforderungen des Bundesgerichts auf und orientiert sich an der im Kanton Solothurn bewährten Lösung bezüglich eines unabhängigen Kontrollorgans über den Nachrichtendienst (vgl. Dienstaufsichtsverordnung [BGS 511.121]). Es müsste noch vertiefter abgeklärt werden, ob die strategische Versammlung Polizeitechnik und -informatik (PTI) das richtige Organ für die Bezeichnung des Kontrollorgans ist bzw. ob sie Adressatin der Berichte und Empfehlungen des Kontrollorgans sein soll. In den Erläuterungen ist ferner klarzustellen, dass für die Abfrageplattform und allfällige gemeinsamen Datenbanksysteme auch unterschiedliche Kontrollorgane bestimmt werden können.

Ausserdem empfehlen wir klare Regelungen der Aufgaben und Verantwortlichkeiten auf Vereinbarungsstufe (vgl. Bemerkungen zu den Artikel 5, 10 f. und Art. 21 ff.).

Wichtig erscheint uns die rasche Aufnahme der nötigen Arbeiten unter direkter Mitwirkung entsprechender Fachleute. Sollte es zu Verzögerungen kommen, machen wir beliebt, die Arbeiten zur Ermöglichung von POLAP prioritär zu behandeln. Mit dem Beitritt des Kantons Solothurn zur interkantonalen bzw. interbehördlichen Vereinbarung über den Datenaustausch zum Betrieb von Lage- und Analysesystemen im Bereich der seriellen Kriminalität (BGS 511.553) hat für uns die möglichst rasche Inbetriebnahme von POLAP klar Vorrang.

2. Bemerkungen zu einzelnen Bestimmungen

Zu Artikel 1:

Der Zweck nach Art. 1 Abs. 1 Bst. a ist auf die «öffentliche Sicherheit» einzuschränken.

Zu Artikel 2:

Nicht alle in einem kantonalen Informationssystem bearbeiteten Personendaten sind zur Zweckerreichung nach Art. 3 nötig und geeignet beziehungsweise rechtfertigen einen direkten Zugriff durch die Polizeiangehörigen anderer Korps. Insbesondere darf POLAP keinen Zugriff auf die besonders sensiblen Personendaten der getrennt geführten Datenbank des kantonalen Bedrohungsmanagements gewähren. Dasselbe gilt für Daten, die im Zusammenhang mit der Erhebung von Ordnungsbussen bearbeitet werden. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte äusserte sich gegenüber der Presse ähnlich (NZZ vom 08.02.2024).

Aus diesen Gründen erachten wir vertiefte Diskussionen über den Kreis der auszutauschenden Daten als unerlässlich. Die Vereinbarung hat den Kreis der kantonal erhobenen, auf POLAP schweizweit abrufbaren Daten sowie die in den gemeinsamen Datenbanksystemen erfassten Daten ausdrücklich zu definieren. Dabei darf es sich nur um Daten handeln, welche zur Zweckerreichung nach Art. 3 der Vereinbarung nötig und geeignet sind. Zudem sind in der Vereinbarung nebst den Kontrollen weitere Massnahmen aufzulisten, welche die jederzeitige Einhaltung des Grundsatzes der Verhältnismässigkeit sicherstellt.

Zu Artikel 3:

Vertieft abzuklären ist die eigenständige Nennung von Daten aus Verkehrskontrollen (Bst. h). In den allermeisten Fällen dürfte die Bearbeitung solcher Daten unter die Bst. a, b oder d fallen. Wir verweisen an dieser Stelle auch auf unsere grundsätzlichen Bemerkungen.

Zu Artikel 5 Absatz 9:

Es ist unklar, ob der Leistungserbringer ein «Verantwortlicher» im Sinne des Datenschutzrechts oder ein «Auftragsbearbeiter» ist. Die Definition ist zudem unvollständig, weil sie «Leistungen» nennt, die ihrerseits nicht definiert sind (welche Leistungen, in wessen Auftrag etc.). Wir raten, die Definition zu präzisieren (vgl. grundsätzliche Bemerkungen).

Zu Artikel 7:

In den Erläuterungen zu Abs. 1 ist festzuhalten, dass sich die Rechtmässigkeit der Datenerhebung nach dem jeweils anwendbaren (Polizei-)Recht (sei dies kantonal oder vom Bund) richtet. Die Ergänzung stellt klar, dass sich die Rechtmässigkeit der Datenerhebung bei gemeinsamen Datenbanken nicht ausschliesslich nach dem bernischen kantonalen Recht richtet, wie etwa Art. 21 Bst. b in Verbindung mit Art. 25 Abs. 1 der PTI-Vereinbarung vermuten lassen könnte.

In Abs. 3 empfehlen wir, auf den Begriff «insbesondere» zu verzichten.

Zu Artikel 9:

Während Abs. 3 für die Nutzung der Abfrageplattform im Sinne einer Gegenrechtsklausel den Anschluss von «eigenen entsprechenden» Informationssystemen voraussetzt, überlässt Abs. 4 die Auswahl der Systeme den Teilnehmenden. Damit der Aspekt des Gegenrechts korrekt umgesetzt wird, ist im Betriebsreglement zu beschreiben, welche Mindestanforderungen die Teilnehmenden beim Anschluss ihrer Systeme zu erfüllen haben.

Artikel 10:

Abs. 1 hat die *Gesamtverantwortung* für POLAP ausdrücklich zu regeln. Die Gesamtverantwortung für die Austauschplattform umfasst u.a. technische Vorgaben für den Anschluss der Quellsysteme, die Verantwortung für das Benutzermanagement (IAM), die Verantwortung für die sichere Datenübermittlung, Vorgaben zur Protokollierung sowie die Kontrolle der Einhaltung der Vorgaben. Sinnvollerweise sind diese Aufgaben durch fedpol zu erfüllen. Vollständigkeitshalber sollte in den Erläuterungen dargelegt sein, wer diesen Aufgaben nachzukommen hat, sollte fedpol der Vereinbarung nicht beitreten.

Die Datenherrschaft über die in POLAP bearbeiteten Daten verbleibt beim Polizeikorps, aus dessen Quellsystem die Daten stammen. Die Rechte der betroffenen Personen und die Aufsicht richten sich nach der jeweiligen kantonalen Datenschutzgesetzgebung.

In Abs. 5 ist die Protokollierung von Datenabfragen über POLAP einheitlich zu regeln. Die Protokollierung an sich und die periodische, stichprobeweise Überprüfung der Rechtmässigkeit sind zwingend. Zudem ist festzulegen, welche Angaben die abfragende Stelle mitliefern muss, damit eine eindeutige Identifikation der abfragenden Person möglich ist. Zu prüfen ist sodann die Normierung der Konsequenzen bei der Feststellung von unrechtmässigen Zugriffen.

Zu Artikel 11:

Abs. 1 ist unseres Erachtens zu wenig präzise und unvollständig. Wünschenswert ist eine klare und vollständige Regelung der Verantwortlichkeiten. Im Rahmen der Überarbeitung könnte die Bestimmung gleichzeitig mit den Aufgaben und Zuständigkeiten des unabhängigen Kontrollorgans ergänzt werden.

Ausserdem sollten zumindest die Erläuterungen zu Abs. 2 näheren Aufschluss darüber geben, welche Teilnehmenden zur Ergreifung der notwendigen Massnahmen verpflichtet sind.

Zu Artikel 13 Absatz 1:

Die Rolle des Leistungserbringers ist nicht vollständig geklärt. Wenn er die Rolle eines Auftragsbearbeiters hat, sollte es nicht an ihm liegen, ein Betriebsreglement zu erlassen. Nach Art. 5 Abs. 9 ist er (lediglich) «verantwortlich» für die Umsetzung. Das Betriebsreglement muss u.E. vom Gesamtverantwortlichen – d.h. fedpol – erlassen werden.

Zu Artikel 18:

Zu Bst. b: Es handelt sich um eine sehr offene Formulierung. Zumindest die Erläuterungen müssen einschränkend dazu festhalten, dass es sich dabei ausschliesslich um eine rechtmässige Datenbearbeitung nach kantonalem beziehungsweise eidgenössischem Recht handeln kann, die ausserdem unter Berücksichtigung der Zweckbindung der vorliegenden Vereinbarung erfolgt.

Zu Bst. c: Gemäss Art. 6 Abs. 1 der Richtlinie (EU) 2016/680 ist zwischen den Daten verschiedener Kategorien betroffener Personen zu unterscheiden. Sinnvollerweise wird dies in der Vereinbarung ausdrücklich vorgesehen.

Zu Artikel 20 Absatz 1:

Sollte mit «automatisierte Auswertungen» (Bst. c) die eigentliche Nutzung von künstlicher Intelligenz (KI) gemeint sein, wäre die Vereinbarung zwingend mit entsprechenden Regelungen im nötigen Detaillierungsgrad zu ergänzen. Umgekehrt sollten die Erläuterungen festhalten, wenn die Vereinbarung keine Nutzung von KI vorsieht.

Zu Artikel 21:

Die Regelung ist unklar, weil sie den Eindruck erweckt, als würde beim Betrieb eines gemeinsamen Datenbanksystems immer nur ein Recht zur Anwendung gelangen. Vielmehr müssen in einem ersten Schritt die (Teil-)Verantwortungen zugewiesen (vgl. Art. 18) und in einem zweiten Schritt festgehalten werden, welches Recht für den jeweiligen Träger von Aufgabe und Verantwortung (insbesondere Betrieb der zentralen Infrastruktur, Datenlieferung und -abfrage) gilt. So kann z.B. kaum generell Bundesrecht gelten, nur weil der Bund an einem Datenbanksystem teilnimmt (sondern nur soweit er selbst ein solches technisch betreibt).

Zu Artikel 22:

Die Bestimmung ist unklar: Die verwendeten Begriffe sind unbestimmt und die PTI-Vereinbarung enthält keine Vorschriften über die «Organisation», den «Betrieb» und die «Abwicklung» von gemeinsamen Datenbanken. Die angedachten Führungs- und Organisationsstrukturen sind vollständig und ihrer eminenten Bedeutung entsprechend ausdrücklich festzulegen.

Zu Artikel 23:

Siehe die Bemerkungen zu Art. 11. Zudem wird (erneut) nicht klar, wer der Verantwortliche ist. Laut Erläuterungen zu Abs. 1 wird mit dem Leistungserbringer (als «Verantwortlicher»?) die zentrale Stelle des jeweiligen Informationssystems informiert. Abs. 2 unterscheidet dann aber wieder zwischen Verantwortlichem und Leistungserbringer. Die Erläuterungen haben näheren Aufschluss darüber zu geben.

Zu Artikel 25:

Eine Aufbewahrung von Protokolldaten während 5 Jahren ist sehr lange. Bewirtschaftete Daten über die Nutzung der elektronischen Infrastruktur werden beim Bund längstens 2 Jahre aufbewahrt (Art. 4 Abs. 1 Bst. b VBNIB [SR 172.010.442]).

Zu Artikel 26:

Die Bestimmung könnte missverstanden werden. Die folgenden Grundsätze sind klar zu formulieren:

- Daten, die weder für die direkte Aufgabenerfüllung (sog. «aktive Phase» des Lebenszyklus') noch für den späteren Nachvollzug während einer bestimmten Aufbewahrungsfrist (sog. «semi-aktive Phase») benötigt werden, sind ohne weiteren Aufschub zu löschen.
- Nach Ablauf der Zeit x seit dem letzten Datenzuwachs werden die Daten unabhängig vom Geschäftsstand gelöscht, wobei das Betriebsreglement x festlegt;
- die Zeit x darf die maximal festgelegte Aufbewahrungsdauer y nicht überschreiten.

Zu Artikel 27 Absatz 3:

Die Erläuterungen sollten ausführen, was genau mit «Rücksprache» gemeint ist und gegen wen sich eine Beschwerde richtet.

Zu Artikel 28:

Die Datenbearbeitung im Ausland und die Auftragsbearbeitung sind nicht dasselbe. Die Sachüberschrift und die Bestimmungen sind entsprechend anzupassen.

Zu Artikel 34 Absatz 2:

Die Erläuterungen sprechen von einer Ermächtigung der strategischen Versammlung zum Erlass rechtsetzender Bestimmungen. Dies geht weit über den Begriff der «einfachen Berichtigungen, die keine materielle Rechtswirkung haben» hinaus. Die Tragweite der Delegation ist unklar. In welcher Form können die Kantone eine Nichtanwendbarkeit dieser Bestimmung vorsehen? Und was ist die Folge, wenn einzelne Kantone davon Gebrauch machen? Die Erläuterungen sind zu präzisieren. Eine zulässige Delegation ist eng und auf Bereiche untergeordneter Bedeutung zu begrenzen.

Besten Dank für die Berücksichtigung unserer Anregungen.

IM NAMEN DES REGIERUNGSRATES

sig.	sig.
Peter Hodel	Andreas Eng
Landammann	Staatsschreiber

Bern, 16. Februar 2024

Generalsekretariat KKJPD
Haus der Kantone
Speichergasse 6
3001 Bern

info@kkjpd.ch

Vernehmlassung zur Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksystem

Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zur Stellungnahme, die wir gerne wie folgt wahrnehmen:

Die SP Schweiz unterstützt die hier vorgeschlagene Interkantonale Vereinbarung über den Datenschutz zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksystem. Es ist unserer Ansicht nach von Bedeutung, dass der automatisierte interkantonale Informationsaustausch für die Polizeiarbeit der kantonalen Polizeibehörden gestärkt wird und eine Rechtsgrundlage dafür geschaffen wird. Dafür spricht auch die starke Befürwortung der Kantone. Von besonderer Bedeutung ist jedoch, dass der Datenschutz genügend Beachtung findet. Dies insbesondere in Hinblick darauf, dass es sich (wie im erläuternden Bericht festgehalten) regelmässig um besonders schützenswerte Daten handelt. Deshalb ist nach Ansicht der SP Schweiz der Anwendungsbereich weiter einzuschränken und sicherzustellen, dass Daten nur dann zur Verfügung gestellt werden, wenn die Übertragung dem Prinzip der Verhältnismässigkeit entspricht. Insbesondere ist zu prüfen, wann auf Daten zu Bagatelldelikten und leichteren Störungen zugegriffen werden kann. Besondere Vorsicht ist auch im Hinblick auf Daten von Opfern geboten. Da die Polizeibehörden mit der Amtshilfe bereits heute die Möglichkeit hat, Personendaten aus einem anderen Zuständigkeitsgebiet zu beziehen, rechtfertigen sich diese Einschränkungen des Anwendungsbereichs.

Wir bitten Sie um Kenntnisnahme unserer Stellungnahme.

Mit freundlichen Grüssen

SOZIALDEMOKRATISCHE PARTEI DER SCHWEIZ

Mattea Meyer
Co-Präsidentin

Cédric Wermuth
Co-Präsident

Jessica Gauch
Politische Fachreferentin

Sozialdemokratische Partei der Schweiz
Theaterplatz 4
Postfach · 3001 Bern
Telefon 031 329 69 69
Telefax 031 329 69 70
info@spschweiz.ch
www.spschweiz.ch

Numero			Bellinzona
791	sl	0	21 febbraio 2024

Consiglio di Stato
Piazza Governo 6
Casella postale 2170
6501 Bellinzona
telefono +41 91 814 41 11
fax +41 91 814 44 35
e-mail can@ti.ch
web www.ti.ch

Repubblica e Cantone
Ticino

Il Consiglio di Stato

Conferenza delle direttrici e dei direttori dei dipartimentali cantonali di giustizia e polizia

Invio per posta elettronica (indicare Word o pdf): info@kkjpd.ch

Procedura di consultazione concernente il concordato intercantonale sullo scambio dati per il funzionamento di comuni piattaforme di interrogazione e di sistemi di banca dati centralizzati

Gentili signore,
egregi signori,

abbiamo ricevuto la vostra lettera del 23 novembre 2023 in merito alla summenzionata procedura di consultazione concernente la creazione di un concordato intercantonale sullo scambio dati per il funzionamento di comuni piattaforme di interrogazione e di sistemi di banca dati centralizzati. Il progetto, unitamente al rapporto esplicativo, è stato da noi esaminato in collaborazione con la Polizia cantonale.

Ringraziando per l'opportunità che ci viene offerta di esprimere il nostro giudizio, formuliamo le seguenti osservazioni.

Lo scrivente Consiglio di Stato accoglie positivamente il progetto qui sottoposto in consultazione, sia dal punto di vista del contenuto, il quale permette una migliore collaborazione e cooperazione tra le autorità di polizia in relazione allo scambio dati, sia dal punto di vista della forma in cui è stato presentato, ovvero in qualità di concordato.

Data la difficoltà dovuta alla sovranità cantonale in materia di polizia di creare una banca dati nazionale condivisa, rispettivamente una base legale federale unica che ne regoli le condizioni, si ritiene che l'emanazione di disposizioni legali che disciplinano lo scambio di informazioni tra polizia sotto forma di concordato sia un'ottima soluzione per rispondere alle esigenze di polizia di poter disporre celermente di tutte le informazioni necessarie all'adempimento dei propri compiti legali, e garantire così un'efficace interoperabilità su tutto il territorio elvetico. Parimenti, il concordato soddisfa perfettamente le norme in materia di protezione dati, garantendo nello specifico che il principio della determinatezza e della proporzionalità vengano ossequiati e che la proprietà e la responsabilità dei dati interessati rimangano delle singole polizie cantonali.

Il presente concordato crea quindi le basi legali indispensabili per uno scambio uniforme e armonizzato di informazioni di polizia a livello intercantonale e federale: da un lato, esse rendono possibile il recupero automatizzato di informazioni dalle banche dati di polizia dei Cantoni o della Confederazione tramite procedura di richiamo su una piattaforma nazionale di interrogazione (POLAP). Il fatto che POLAP permetta unicamente la visione di determinate categorie di dati delle altre polizie cantonali senza che possano essere estrapolati, rispettivamente senza possibilità di accedere alle altre banche dati, risponde perfettamente alle esigenze imposte dalla legislazione in materia di protezione dei dati, garantendo il mantenimento della proprietà e della responsabilità sui propri dati alle singole polizie cantonali.

Nell'ambito delle proprie revisioni di leggi che riguardano la legge sulla polizia, così come la legge speciale per l'elaborazione di dati da parte della polizia, la Polizia del Cantone Ticino si sta già adoperando in tal senso, inserendo nei due progetti le disposizioni legali necessarie atte a permettere il collegamento ad una piattaforma di interrogazione, così come ad autorizzare la visione dei propri dati tramite procedura di richiamo.

Dall'altro lato, il Concordato prevede altresì le basi legali formali per poter creare e gestire congiuntamente dei sistemi di informazione di polizia centralizzati volti alla lotta di specifiche categorie di reati (anche in collaborazione con la Confederazione), comprensive di una procedura di richiamo per poter rendere accessibili a tutte le polizie: in questo modo, la creazione di questi sistemi di informazione così come la loro regolamentazione ed eventuale annessione avverrà in maniera semplificata, poiché gli aspetti fondamentali che devono essere contenuti in una legge formale saranno già presenti nel Concordato: non dovranno più essere elaborati specifici concordati per ogni banca dati comune (come ad esempio nel caso del concordato ViCLAS) ma sarà sufficiente stabilire e concretizzare le condizioni e il contenuto dei sistemi di banche dati comuni nelle singole ordinanze elaborate dall'assemblea strategia TIP, che regolamenteranno l'utilizzo di tali sistemi, alle quali ogni Cantone potrà decidere se aderire.

Vogliate gradire, gentili signore, egregi signori, i sensi della nostra massima stima.

PER IL CONSIGLIO DI STATO

Il Presidente
Raffaele De Rosa

Il Cancelliere
Arnoldo Coduri

Copia a:
- Dipartimento delle istituzioni (di-dir@ti.ch)
- Segreteria generale del Dipartimento delle istituzioni (di-sg.ap@ti.ch)
- Comando della Polizia cantonale (polizia-segr@polca.ti.ch; servizio.giurico@polca.ti.ch)
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch)
- Pubblicazione in Internet

Der Regierungsrat des Kanton Thurgau

Thurgau

Staatskanzlei, Regierungskanzlei, 8510 Frauenfeld

Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
Frau Karin Kayser-Frutschi, Co-Präsidentin
Herr Alain Ribaux, Co-Präsident
Haus der Kantone
Speichergasse 6
Postfach
3001 Bern

Frauenfeld, 13. Februar 2024
85

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme

Vernehmlassung

Sehr geehrte Frau Präsidentin, sehr geehrter Herr Präsident

Wir danken Ihnen für die Möglichkeit der Stellungnahme zum Entwurf für eine Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme und teilen Ihnen mit, dass wir die Zielsetzung der Vereinbarung grundsätzlich unterstützen. Allerdings hat der Grosse Rat am 22. November 2023 eine Änderung des Polizeigesetzes (PolG; RB 551.1) beschlossen und mit § 56a PolG das Melde- und Auskunftsrecht geregelt. Die Referendumsfrist dauert noch bis zum 1. März 2024. Dem Regierungsrat sind im Moment keine Bestrebungen bekannt, das Referendum gegen die erwähnte Gesetzesänderung zu ergreifen. Die Revision des PolG wird somit im Verlaufe des Jahres 2024 in Kraft gesetzt werden können. Damit wird der Kanton Thurgau in absehbarer Zeit über eine ausreichende gesetzliche Grundlage für den Datenaustausch mit anderen Kantonen und dem Bund verfügen. Die vorliegend zur Diskussion stehende Vereinbarung ist daher für unseren Kanton nicht notwendig. Ungeachtet dessen gestatten wir uns zu einzelnen Bestimmungen die nachfolgenden Bemerkungen.

Art. 1 Ziff. 2

Der Begriff der besonders schützenswerten Daten ist datenschutzrechtlich nicht definiert. Dieser sollte durch den Begriff der besonders schützenswerten Personendaten ersetzt werden. Im weiteren Verlauf der Vereinbarung wird denn auch der Begriff der Personendaten verwendet (vgl. z.B. Art. 5 der Vereinbarung).

Regierungsgebäude, Postfach, 8511 Frauenfeld
T +41 58 345 53 10
www.tg.ch

Thurgau

Art. 3 Abs. 1 lit. b

Grenzkontrollen gehören nicht zur polizeilichen Zusammenarbeit und stützen sich auf andere Rechtsgrundlagen. Diese Ausweitung ist daher zu streichen.

Art. 3 Abs. 1 lit. f

Es ist fraglich, ob verwaltungspolizeiliche Bewilligungsverfahren wirklich vom verlangten Zweck der Vereinbarung abgedeckt sind und dies nicht eine zu weitgehende Massnahme darstellt.

Art. 3 Abs. 1 lit. g

Die Massnahmen auch auf den Bereich der Personensicherheitsüberprüfungen ausdehnen zu wollen, kann bei der Ausweitung auf mehrere Kantone einen schwerwiegenden Eingriff in den Schutz der Privatsphäre darstellen. Wir lehnen daher diese Ausweitung ab.

Art. 4

Der Verweis auf die Regelung der Vereinbarung zwischen dem Bund und den Kantonen über die Harmonisierung und die gemeinsame Bereitstellung der Polizeitechnik und -informatik in der Schweiz (PTI-Vereinbarung; SR 367.1) darf nicht umfassend übernommen werden. Im dortigen Regelwerk steht in Art. 25, dass für Rechtsfragen das kantonale bernische Recht anzuwenden sei. Die PTI-Vereinbarung stützt sich darauf, dass die PTI Schweiz eine öffentlich-rechtliche Körperschaft mit Sitz in der Stadt Bern ist. Für die vorliegende interkantonale Vereinbarung das Datenschutzgesetz des Kantons Bern anwenden zu wollen, stellt eine Verletzung des Gesetzes über den Datenschutz des Kantons Thurgau (TG DSG; RB 170.7) dar. Die ungenaue Formulierung in der Vereinbarung ist somit neben den Bereichen der Haftung, der Kostentragung und dem Verfahrensrecht auch mit dem Bereich des Datenschutzrechts zu ergänzen. Dies ist insbesondere auch deshalb erforderlich, weil in Art. 7 des Vereinbarungsentwurfes ein Verweis auf das kantonale Datenschutzgesetz erfolgt.

Art. 5 Ziff. 5

Der Begriff der Personendaten ist falsch definiert. Es genügt, wenn sich diese auf bestimmte oder bestimmbare Personen beziehen. Die Erfüllung der öffentlichen Aufgabe als Kriterium beiziehen zu wollen, geht zu weit.

Art. 7 Ziff. 3 lit. c

Die Bearbeitung der biometrischen Daten aus erfassten Registrierungs- und Zugangsdaten bei Accounts stützt sich auf keine genügende gesetzliche Grundlage. Eine solche Regelung wäre insbesondere für die Digitalisierung mit der e-ID problematisch. Das Vertrauen der Bevölkerung würde bei der Bearbeitung dieser Daten schwinden. Da sol-

Thurgau

che Daten in den Kantonen nicht erfasst werden dürfen, können sie auch interkantonal nicht weitergegeben werden. Die zu bearbeitenden Daten sind genauer zu umschreiben.

Art. 10 Ziff. 4

Es genügt nicht, die Kontrollaufgabe an den Bund zu delegieren, nur weil dieser die Plattform mitfinanziert. Die Kontrolle durch die kantonalen Aufsichtsstellen muss weiterhin möglich sein, da kantonale Daten bearbeitet werden. Die Verantwortung für die Daten verbleibt weiterhin bei den Polizeiorganen der Kantone.

Mit freundlichen Grüssen

Der Präsident des Regierungsrates

Der Staatsschreiber

DER REGIERUNGSRAT · DES KANTONS THURGAU ·

Landammann und Regierungsrat des Kantons Uri

Konferenz der Kantonalen Justiz- und
Polizeidirektorinnen und -direktoren (KKJPD)
Speichergasse 6
Postfach
3001 Bern

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme; Vernehmlassung

Sehr geehrte Frau Präsidentin, sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Mit Schreiben vom 23. November 2023 laden Sie den Regierungsrat des Kantons Uri ein, zum Entwurf der Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme Stellung zu nehmen. Gerne nehmen wir die Möglichkeit wahr und äussern uns wie folgt:

Die Kantone verfügen heute nicht durchgehend über die notwendigen Rechtsgrundlagen, um ihre polizeilichen Daten über die Polizeiliche Abfrageplattform (POLAP) dem Bund und anderen Kantonen bekannt zu geben. Die Rechtsgrundlagen können mittels der Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme geschaffen werden oder mittels nationaler Gesetzgebung.

Aus Sicht des Regierungsrats ist es in der heutigen Zeit nicht nachvollziehbar, dass der Bund der EU und den Kantonen polizeiliche Daten bekanntgeben kann, die Kantone hingegen die Daten untereinander und mit dem Bund nicht austauschen dürfen. Im heutigen Zeitalter der digitalen Vernetzung, der Notwendigkeit des Lernens über kriminelle Banden, die an der Kantonsgrenze keinen Halt machen, und des schnellen Reagierens ihnen gegenüber ist diese Situation nicht mehr erklärbar. Es geht darum, die Schweizer Bevölkerung besser zu schützen und die transnationale Kriminalität besser zu bekämpfen - aber eben nicht nur die transnationale Kriminalität, sondern auch die transkantonale

Kriminalität. Nimmt heute ein Kanton eine verdächtige Person fest, die einen Einbruch verübt hat, kann dieser Kanton nicht mit einer einzigen Abfrage überprüfen, ob die gleiche Person allenfalls schon andere Delikte in anderen Kantonen verübt hat. Es müssen alle anderen 25 Kantone einzeln angefragt werden. Aus polizeilicher Sicht ist die vorliegende Interkantonale Vereinbarung absolut notwendig. Damit wird ein gemeinsamer Polizeidatenraum geschaffen, in dem die schweizerischen Polizeibehörden direkt auf Daten in kantonalen, nationalen und internationalen Polizei-Informationssystemen zugreifen können.

Demgegenüber bestehen aus Sicht des Regierungsrats Bedenken im Zusammenhang mit dem Datenschutzrecht. So erachten wir den Anwendungsbereich (Art. 3) des vorliegenden Entwurfs der Interkantonalen Vereinbarung als sehr breit gefasst. Der Vereinbarung käme trotz der wiederholten Bekräftigung des Legalitätsprinzips, des Bestimmtheitsgebots und des Verhältnismässigkeitsprinzips einer Blankoermächtigung für den Datenaustausch im Polizeibereich gleich, die rechtlich heikel und daher zu überprüfen ist. Zudem ergibt sich aus der Vereinbarung, dass viele erhebliche Rechtsfragen erst auf der Stufe der Betriebsverordnungen (siehe bspw. Art. 7 und Art. 17) geregelt werden sollen. Hierdurch haben die kantonalen Parlamente und das Volk nur noch wenig bis keinen Einfluss auf die Regelungsmaterie und verlieren so zudem weitestgehend die Kontrolle über die rechtmässige Abfrage und Nutzung der Daten in den von ihnen verantworteten angeschlossenen Informationssystemen. Wir empfehlen daher, die damit verbundenen Delegationsnormen einer Prüfung zu unterziehen.

Schliesslich weisen wir auf den aktuell laufenden Gesetzgebungsprozess zum Urner Polizeigesetz hin - die Volksabstimmung findet am 3. März 2024 statt. Die Vorlage zeigt, dass Uri bestrebt ist, die für den polizeilichen Datenaustausch zeitgemässen Rechtsgrundlagen zu schaffen. Zu guter Letzt möchten wir darauf hinweisen, dass aus unserer Sicht eine nationale Gesetzgebung nach wie vor wünschenswert und anzustreben wäre.

Nach dem Ausgeführten begrüsst der Regierungsrat die Vereinbarung im Grundsatz und die damit verfolgten Ziele. Gleichzeitig verweisen wir auf die geäusserten datenschutzrechtlichen und staatspolitischen Bedenken.

Sehr geehrte Frau Präsidentin, sehr geehrter Herr Präsident, sehr geehrte Damen und Herren, wir bedanken uns für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Altdorf, 6. Februar 2024

REGIERUNGSRAT DES KANTONS URI

Im Namen des Regierungsrats

Der Landammann	Der Kanzleidirektor
Urs Janett	Roman Balli

18.10.2023

Convention intercantonale sur l'échange de données à des fins d'exploitation de plates-formes de recherche et de systèmes de bases de données communs

Préambule

Vu

- l'art. 2, al. 1, en relation avec l'art. 57 et l'art. 3 ainsi que l'art. 43a et l'art. 48 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst, RS 101),
- la loi fédérale sur les systèmes d'information de police de la Confédération du 13 juin 2008 (LSIP, RS 361),
- la Convention entre la Confédération et les cantons sur l'harmonisation et la mise à disposition commune de la technique et de l'informatique policières en Suisse du 2 septembre 2020 (Convention TIP; RS 367.1),

avec pour finalité de créer un espace commun de données de police pour l'échange de données policières,

dans l'intention de créer les bases légales formelles de l'échange intercantonal automatisé de données,

afin de rendre possible la collaboration au moyen de systèmes d'information communs sur la base de la compétence d'édicter des dispositions législatives,

et dans l'intention de créer les bases nécessaires pour que les cantons puissent collaborer de la même manière avec la Confédération et pour que cette dernière puisse participer aux systèmes d'information, moyennant des conventions de prestations ou en reprenant les ordonnances d'exploitation,

les cantons, agissant par l'intermédiaire de leurs directrices et directeurs de la justice, concluent la convention intercantonale ci-après:

Chapitre premier Dispositions générales

Article 1. Objet et but

1. La convention a pour but, moyennant une collaboration efficiente des autorités de police des cantons et des communes (ci-après: les «participants») entre elles, ainsi qu'avec la Confédération dans le cadre du droit fédéral:
   a. de garantir la sécurité et l'ordre publics;
   b. de détecter et d'empêcher des infractions;
   c. de lutter contre la criminalité;
   d. de contribuer à l'efficience et à la coordination des enquêtes.
2. La convention crée les bases légales de l'échange intercantonal de données de police, y compris de données particulièrement sensibles, ainsi que pour l'exploitation de systèmes d'information communs.

Article 2. Plates-formes de recherche et systèmes de bases de données communs

1. A cet effet, les participants peuvent:
   a. raccorder leurs systèmes d'information à des plates-formes de recherche communes des cantons et/ou de la Confédération et permettre l'accès à des données de police par une procédure d'appel;
   b. créer et exploiter des systèmes de bases de données communs et, à cet effet, permettre l'accès à des données de police par une procédure d'appel;
   c. créer et exploiter conjointement avec la Confédération des systèmes de bases de données ou permettre l'accès aux propres systèmes d'information, par une procédure d'appel.
2. La mesure dans laquelle la convention s'applique ou non pour les communes est réglée dans le droit cantonal.

Article 3. Champ d'application

Dans l'espace commun de données de police, des données peuvent être traitées et rendues accessibles, par une procédure d'appel, à d'autres participants ainsi qu'à la Confédération pour l'accomplissement des tâches policières suivantes:

a. enquêtes (enquêtes préliminaires de police et enquêtes pénales);
b. contrôles de personnes et contrôles aux frontières;
c. prévention d'actes délictueux, notamment par la défense policière et la prévention de la violence;
d. recherche de choses et de personnes;
e. présentation de la situation ainsi qu'analyse stratégique, opérationnelle et tactique de données de police de sécurité et de police judiciaire;
f. mise en œuvre de procédures d'autorisation et de mesures de police administrative;
g. contrôles de sécurité de personnes;
h. contrôles de la circulation.

Article 4. Droit applicable

Les dispositions de la Convention TIP s'appliquent pour autant que la présente convention ne crée pas de cadre juridique s'en écartant, notamment en ce qui concerne la responsabilité, la prise en charge des coûts et le droit procédural.

Article 5. Notions

1. Les notions de «données personnelles», «données personnelles sensibles», «personne concernée», «traitement (de données personnelles)», «communication» ainsi que «profilage» et «profilage à risque élevé» et «responsable du traitement» correspondent à celles utilisées dans la loi fédérale sur la protection des données du 25 septembre 2020 (LPD; RS 235.1).
2. La notion de plate-forme de recherche désigne des systèmes et des possibilités techniques permettant, au moyen d'une fonction de recherche, d'appeler et d'afficher des données de systèmes de bases de données raccordés.
3. La procédure d'appel est une communication automatisée de données, dans laquelle le ou la destinataire décide quelles données peuvent être appelées quand, conformément à l'assentiment du responsable du traitement compétent ou à des conditions définies d'avance, sans contrôle préalable au cas par cas. Il s'agit d'une communication régulière sous la forme d'une autorisation générale d'accès (en ligne).
4. Les ordonnances d'exploitation, qui se situent en aval de la présente convention, sont des dispositions contenant des règles de droit; elles entrent en vigueur par décision de l'assemblée stratégique TIP ou sont soumises aux participants pour approbation.
5. Par données, on entend les données relatives aux choses et aux personnes en relation avec l'accomplissement d'une tâche publique, y compris les données personnelles sensibles, et indépendamment de leur forme de présentation et du support d'information.
6. Les systèmes de bases de données communs sont des systèmes d'information comportant une base de données centrale, qui sont exploités par plusieurs participants pour accomplir leurs tâches policières.
7. Les moyens informatiques sont des appareils, des dispositifs et des services, tels que des systèmes et des programmes d'ordinateur ou des services de communication, utilisés pour la saisie, le traitement, l'enregistrement, la transmission, l'analyse, l'archivage ou la destruction d'informations.
8. La notion de système d'information est générique pour les plates-formes de recherche ainsi que les systèmes de bases de données; elle désigne un système de traitement de données composé d'un ou de plusieurs moyens informatiques.
9. Le prestataire de services est responsable de la fourniture des prestations. Selon l'art. 10 de la Convention TIP, il peut s'agir de TIP ou d'un tiers désigné à cet effet.
10. La notion d'espace commun de données de police Suisse recouvre l'ensemble des plates-formes de recherche et des systèmes de bases de données utilisés ou exploités conjointement.
11. La notion de système source désigne le système de provenance des données. Ce système peut être de la responsabilité d'un canton, d'une commune ou de la Confédération.

Article 6. Principes de traitement

1. Les participants doivent faire usage de leurs compétences en vertu de la présente convention en respectant la légalité et la proportionnalité, à des fins d'intérêt public.
2. Seules les données nécessaires et appropriées pour l'accomplissement de tâches policières concrètes peuvent être enregistrées dans un système d'information, y être rendues accessibles et traitées, et en être extraites et consultées. Le traitement doit être acceptable pour la personne concernée.
3. Les droits fondamentaux et les droits humains doivent être respectés.

Article 7. Etendue du traitement des données et de la protection des données

1. Les participants traitent exclusivement des données provenant d'autorités de police des cantons, des communes, de la Confédération ou, si nécessaire pour l'accomplissement des tâches policières, d'autres autorités et organisations partenaires suisses et étrangères, qui ont été relevées et communiquées de manière légale.
2. Pour le traitement de données personnelles dans le cadre de la présente convention, et pour autant que les chapitres 2 et 3 ne contiennent pas de dispositions contraires, la loi fédérale sur la protection des données s'applique pour la Confédération et le droit cantonal s'applique pour les cantons.
3. Les données suivantes, notamment, peuvent être traitées:

a. indications relatives à l'événement et au lieu de l'événement;
b. indications relatives au mode opératoire et aux moyens utilisés, notamment le hardware, les softwares et les malwares;
c. indications relatives aux auteurs d'actes, connus et inconnus, ainsi qu'aux personnes suspectes, à savoir nom, prénom, date de naissance, sexe, surnom(s), nationalité, signalement, photos, numéro d'identification de pièces officielles, numéro de passeport ou numéro personnel, numéro AVS, entreprises, numéros de téléphone, identité internationale d'équipement mobile IMEI, identité internationale d'abonné mobile IMSI, adresses, adresses IP, adresses MAC, URI, adresses de courriel, autres indications en relation avec la technologie d'information et de communication utilisée, noms utilisés dans les médias sociaux et les jeux (pseudonymes, etc.), données d'enregistrement et d'accès (y compris données biométriques) pour les comptes, de même que mode opératoire favori;
d. indications relatives aux personnes physiques ou morales lésées ou concernées: nom, prénom, date de naissance, sexe et données de contact, respectivement raison sociale, de même que données relatives aux moyens de communication;
e. indications relatives à l'objet du délit;
f. indications relatives aux véhicules éventuellement en relation avec l'événement;
g. indications relatives aux liens entre des événements (relations spécifiques au cas ou reposant sur des traces matérielles ou électroniques);
h. images des événements, enregistrements vidéo et sonores;
i. indications sur les sources d'information, telles que des témoins ou des personnes interrogées;
j. numéro de contrôle de processus selon l'art. 8, al. 3 de la loi sur les profils d'ADN;
k. informations relatives aux moyens de paiement et aux flux financiers;
l. données relatives à la procédure;
m. données relatives aux traces analogiques et numériques;
n. données d'accès à des systèmes de traitement de données.

4. Les catégories de données ainsi que les données à traiter sont énumérées exhaustivement dans les ordonnances d'exploitation des différents systèmes d'information.

Article 8. Responsabilité

1. Les participants et leur personnel, ainsi que leurs mandataires auxquels des tâches publiques sont confiées, répondent conformément au droit applicable pour eux des dommages causés à d'autres participants ou à des tiers par suite du traitement illégal de données.
2. S'il y a responsabilité du fournisseur de prestations, l'obligation de fournir des contributions conformément à la Convention TIP est subrogée à la responsabilité de l'Etat. La prétention en responsabilité doit être invoquée conformément au droit procédural du canton de domicile du fournisseur de prestations.
3. Tout droit de plainte du participant responsable contre les collaboratrices ou collaborateurs d'un autre participant est exclu.

Chapitre 2 Plate-forme commune de recherche

Article 9. Exploitation et utilisation

1. Les participants exploitent conjointement une plate-forme de recherche. L'assemblée opérationnelle TIP édicte un règlement d'exploitation pour la plate-forme de recherche.
2. La Confédération peut participer à des plates-formes de recherche. Le raccordement des systèmes d'information de la Confédération et des systèmes internationaux d'information est régi par le droit fédéral.
3. L'utilisation de la plate-forme de recherche par les participants présuppose le raccordement de leurs propres systèmes d'information correspondants et la préparation des données qu'ils contiennent, en vue de leur consultation par la plate-forme de recherche.
4. La décision concernant le raccordement de leurs systèmes d'information à la plate-forme de recherche est du ressort des participants.

Article 10. Responsabilités et droits des personnes concernées

1. La responsabilité du traitement légal des données dans le système source reste inchangée en cas de raccordement à la plate-forme de recherche, c'est-à-dire qu'elle reste auprès de l'organe compétent pour le système source.
2. Les participants qui procèdent, via la plate-forme commune de recherche, à des recherches de données provenant de systèmes d'information (systèmes sources) d'autres participants sont responsables de la légalité du traitement subséquent des données obtenues lors d'une recherche.
3. Les droits des personnes concernées sont régis par le droit du responsable du système d'information raccordé (système source). Le droit cantonal correspondant et les dispositions sur la surveillance s'appliquent.
4. Si la Confédération participe ou exploite une plate-forme de recherche, la LPD s'applique pour le traitement des données dans la plate-forme de recherche et l'organe de surveillance est le Préposé fédéral à la protection des données et à la transparence (PFPDT).
5. Le procès-verbal des communications de données effectuées via la plate-forme de recherche est enregistré dans le système source, conformément aux prescriptions s'appliquant pour ce dernier.

Article 11. Annonce d'abus

1. Les traitements abusifs de données doivent être annoncés à l'organe de la Confédération compétent pour la plate-forme de recherche ainsi qu'aux autres participants concernés.
2. Les participants prennent, d'entente avec le prestataire de services, les mesures appropriées pour protéger les données personnelles et maintenir aussi faibles que possible les dommages à la personne concernée.

Article 12. Prise en charge des coûts

1. Le financement de la plate-forme commune de recherche s'aligne sur la Convention TIP.
2. La répartition des coûts d'exploitation de la plate-forme de recherche est réglée dans une convention distincte.
3. Les participants assument les coûts d'exploitation et de raccordement de leurs systèmes d'information.

Article 13. Dispositions d'exécution

1. Le prestataire de services élabore un règlement d'exploitation contraignant pour les participants, qui est édicté par l'assemblée opérationnelle TIP.
2. Les aspects suivants doivent être réglés en vue de l'utilisation de la plate-forme de recherche:
   a. rôles et droits d'accès;
   b. catégories de données pouvant faire l'objet de recherches;
   c. mesures techniques et organisationnelles propres à garantir la sécurité des données.
3. En complément, les participants doivent régler les points suivants conformément à leurs bases légales:
   a. désignation du ou des systèmes d'information raccordés;
   b. responsabilité des systèmes d'information raccordés.

Article 14. Modification du règlement d'exploitation

Les modifications du règlement d'exploitation sont adoptées par décision de l'assemblée opérationnelle TIP. En cas de participation de la Confédération, l'assentiment de cette dernière est requis.

Article 15. Résiliation

1. Un participant peut résilier le raccordement de son système d'information (système source) en respectant un délai de 6 mois.
2. Le droit du participant d'utiliser la plate-forme de recherche s'éteint pour tous les systèmes d'information raccordés à l'échéance du délai de résiliation.

Chapitre 3 Systèmes de bases de données communs

Article 16. Systèmes de bases de données communs

1. Les participants peuvent créer et exploiter conjointement des systèmes de bases de données auprès d'un prestataire de services.
2. En cas de participation à un système commun de bases de données, un participant rend ses données accessibles à tous les participants.
3. Sous réserve du droit fédéral, la Confédération peut participer aux systèmes de bases de données communs en concluant une convention de prestations ou en reprenant l'ordonnance d'exploitation.

Article 17. Ordonnance d'exploitation

1. Les dispositions d'exécution relatives à chaque système commun de bases de données figurent dans des ordonnances d'exploitation distinctes.
2. Les ordonnances d'exploitation et leurs modifications sont édictées par l'assemblée stratégique TIP.
3. Les ordonnances d'exploitation et leurs modifications doivent être approuvées par l'organe du canton participant qui dispose de la compétence d'édicter une ordonnance. Les cantons peuvent décider la non-applicabilité de l'al. 4.
4. Les modifications minimes de l'ordonnance d'exploitation, qui ne déploient aucun effet juridique matériel ou seulement des effets mineurs, peuvent être effectuées par décision prise à l'unanimité par l'assemblée stratégique, moyennant une procédure simplifiée, sans qu'une nouvelle approbation de l'ordonnance d'exploitation par les participants ne soit nécessaire.

Article 18. Teneur de l'ordonnance d'exploitation

Dans la mesure où elle s'écarte de la Convention TIP, l'ordonnance d'exploitation fixe notamment les modalités suivantes pour chaque système commun de bases de données, en tenant compte des grandes lignes arrêtées dans la présente convention:

a. nom et but du système commun de bases de données;
b. traitements de données possibles;
c. catégories de données à traiter;
d. compétences et responsabilités pour l'exploitation de la base de données centrale et concernant la protection des données;
e. compétences relatives à l'exercice des droits des personnes concernées en vertu de la législation sur la protection des données;
f. droits d'accès à chaque base de données, y compris enregistrement de données secondaires;
g. garantie de la légalité et de l'exactitude des données;
h. conservation et suppression de données;
i. droit applicable selon l'art. 21;
j. dispositions concernant le traitement par un sous-traitant conformément au droit applicable sur la protection des données;
k. dispositions concernant la prise en charge des coûts et le financement, y compris les suites financières de la sortie d'un participant d'un système commun de bases de données, de même qu'éventuels coûts de liquidation;
l. dispositions concernant la responsabilité des participants, selon l'art. 8, dans les relations internes en cas de dommages découlant du traitement illégal de données ou de manque de diligence;
m. dispositions concernant l'adhésion, la résiliation et la sortie.

Article 19. Règlement d'exploitation

L'assemblée opérationnelle TIP édicte et actualise un règlement d'exploitation. Ce règlement contient notamment des indications relatives à l'organisation interne et aux procédures de traitement des données et de contrôle, ainsi que des mesures propres à garantir la sécurité des données.

Article 20. Traitements de données

1. Dans des systèmes de bases de données communs, les participants peuvent par ailleurs:
   a. exploiter des profilages et des profilages à risque élevé visant à prévenir et à élucider des actes délictueux, conformément à l'art. 269, al. 2 du Code de procédure pénale suisse du 5 octobre 2007 (RS 312.0);
   b. échanger des données au moyen de procédures d'appel automatisées;
   c. procéder à des analyses automatisées.
2. Par ailleurs, les résultats et les enseignements tirés d'analyses ainsi que des images de la situation peuvent être échangés.
3. Les participants garantissent que les données qu'ils transmettent à la base de données sont légales et exactes.

Article 21. Droit applicable

Le droit applicable découle:

a. du droit fédéral si la Confédération participe à un système de bases de données;
b. de la Convention TIP si tous les cantons ont la possibilité de participer au système de bases de données;

c. de la Convention TIP ou du droit d'un canton si un système de bases de données est exploité au niveau régional.

Article 22. Organisation

L'organisation, l'exploitation et le fonctionnement de systèmes de bases de données communs reposent sur la Convention TIP.

Article 23. Annonce d'abus

1. Les traitements abusifs de données doivent être annoncés au responsable du traitement et au président du comité opérationnel TIP.
2. D'entente avec le prestataire de services, le responsable du traitement prend les mesures appropriées pour maintenir aussi faibles que possible la mise en danger de la sécurité et de la protection des données, ainsi que les dommages à la personne concernée. Le responsable du traitement informe rapidement l'assemblée opérationnelle TIP sur les événements et sur les mesures prises.

Article 24. Droits d'accès

La gestion des droits d'accès est du ressort du prestataire de services.

Article 25. Procès-verbal

1. Les systèmes de bases de données enregistrent toute entrée de données, la provenance de ces dernières, tout accès à des données enregistrées et tout traitement de ces données, et ils conservent les données de procès-verbal pendant 12 mois au minimum et 60 mois au maximum. Une fois le délai échu, les données de procès-verbal enregistrées sont effacées. L'ordonnance d'exploitation fixe la durée effective d'enregistrement.
2. L'analyse des accès n'est permise qu'aux conditions suivantes:
   a. dans le cadre de l'exercice du devoir de surveillance de l'organe compétent;
   b. en cas de suspicion concrète d'usage abusif du système.

Article 26. Effacement de données

1. Les données qui ne sont plus nécessaires en vertu de la présente convention sont effacées immédiatement, mais au plus tard après 10 ans. Le délai est calculé à partir de la dernière croissance de données pour le dernier événement saisi.
2. Dans la mesure de la faisabilité technique, et indépendamment des délais selon l'al. 1, le prestataire de services efface ou anonymise les données relatives aux lésés dès que le but du traitement le permet.
3. Les dispositions divergentes de la Confédération priment les al. 1 et 2.

Article 27. Droits des personnes concernées

1. Les personnes concernées peuvent faire valoir leurs droits, comme le droit aux renseignements, le droit de consultation et le droit de rectification, conformément au droit applicable selon les art. 4 et 21 de la présente convention.
2. Les droits d'une personne concernée envers l'autorité qui a entré ou fait entrer les données dans la base de données commune sont réservés.
3. Les renseignements sont donnés par un organe central de renseignement, qui le fait d'entente avec l'autorité qui a entré ou fait entrer les données.
4. Les rectifications sont apportées par le prestataire de services d'entente avec l'autorité qui a entré ou faire entrer les données.
5. L'exercice du droit des personnes concernées peut être restreint, ajourné ou refusé pour des motifs de restriction, conformément au droit applicable.

Article 28. Traitement par un sous-traitant

1. Le traitement des données selon la présente convention est effectué fondamentalement dans un environnement sûr, en Suisse.
2. Le traitement de données à l'étranger est possible à condition de respecter l'art. 16 LPD et pour autant qu'il soit tenu compte suffisamment, par des mesures appropriées, de la sensibilité des données à traiter dans le cadre de la présente convention.
3. Le traitement par un sous-traitant, y compris l'externalisation de l'exploitation technique auprès de tiers, est autorisé pour autant que la présente convention et l'art. 9 LPD soient respectés. Les responsabilités selon la présente convention continuent de s'appliquer.
4. Si la Confédération participe à un système commun de bases de données, l'externalisation doit être convenue avec elle.

Article 29. Prise en charge des coûts

1. Chaque participant assume ses propres coûts d'infrastructure et de licences.
2. Le financement et les coûts sont répartis entre les participants à un système commun de bases de données. En lieu et place de la répartition des coûts conformément à la Convention TIP, il est possible de prévoir une clé de répartition différente dans l'ordonnance d'exploitation. Des clés de répartition possibles sont:
   a. répartition au prorata au sens des art. 21 et 22 de la Convention TIP;
   b. population résidente permanente;
   c. volume de données;
   d. utilité pour un participant;
   e. nombre d'autorités impliquées d'un participant.
3. Les clés de répartition peuvent être combinées et s'ajouter à des contributions de base.
4. Le prestataire de services facture annuellement les coûts aux participants. Il peut exiger le paiement d'acomptes.

Article 30. Entrée

1. Tout participant à la présente convention est libre d'adhérer à un système commun de bases de données en en approuvant l'ordonnance d'exploitation. Le processus d'approbation repose sur le droit du participant. La participation de la Confédération est réglée à l'art. 16, al. 3 et dans le droit fédéral.
2. La demande de participation doit être adressée au prestataire de services.

Article 31. Modification de l'ordonnance d'exploitation

Si un participant rejette une modification de l'ordonnance d'exploitation, il sort du système d'information à l'échéance du délai transitoire fixé.

Article 32. Résiliation et sortie

1. La participation à un système commun de bases de données peut être résiliée avec effet à la fin d'une année civile, en respectant un délai de six mois. La résiliation doit être adressée par écrit au prestataire de services.
2. Le droit à l'utilisation du système commun de bases de données s'éteint au moment où la résiliation déploie ses effets. L'obligation d'assumer les coûts s'éteint simultanément, sous réserve des coûts liés à la sortie.
3. Le remboursement de charges de matériel ou de personnel du participant sortant est en principe exclu.
4. Les données entrées jusqu'à la sortie du participant sont effacées dans la base de données pour autant qu'elles n'aient pas de lien avec un événement saisi par un autre participant.

Article 33. Liquidation d'un système commun de bases de données

1. En cas de cessation d'exploitation d'un système commun de bases de données, le responsable du traitement veille à l'effacement correct des données. Le transfert des données dans un système subséquent est réservé.
2. Les éventuels coûts de liquidation doivent être payés par les participants conformément à la clé de répartition fixée dans l'ordonnance d'exploitation.

Chapitre 4 Dispositions finales

Article 34. Modifications de la présente convention

1. Les modifications de la présente convention nécessitent l'assentiment de tous les participants.
2. Des corrections mineures de la présente convention, sans effet juridique matériel, peuvent être effectuées par décision prise à l'unanimité par l'assemblée stratégique TIP, moyennant une procédure simplifiée, sans qu'une nouvelle ratification de la convention par les participants ne soit nécessaire. Les cantons peuvent décider la non-applicabilité de cet alinéa.

Article 35. Entrée et résiliation

1. Chaque canton peut adhérer en tout temps à la présente convention. L'adhésion prend effet immédiatement.
2. Chaque canton a la possibilité de sortir de la présente convention avec effet à la fin d'une année civile, en respectant un délai de six mois.
3. Les demandes d'adhésion et les résiliations doivent être adressées à la Conférence des directrices et directeurs des Départements cantonaux de justice et police.

Article 36. Adaptations des lois cantonales

Les cantons édictent ou adaptent les bases nécessaires à l'adhésion et à l'exécution de la présente convention.

Article 37. Entrée en vigueur

La présente convention entre en vigueur dès que huit cantons y ont adhéré.

Article 38. Notification

La Conférence des directrices et directeurs des Départements cantonaux de justice et police informe la Chancellerie fédérale sur la présente convention. La procédure repose sur l'Ordonnance sur l'organisation du gouvernement et de l'administration (OLOGA, RS 172.010.1).

SG CCPCS - Berne, mardi, 24 octobre 2023 10:15:00

canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ETAT

Château cantonal
1014 Lausanne

Conférence des directrices et directeurs
des départements cantonaux de justice et
police (CCDJP)
Madame Karin Kayser-Frutschi, Co-
présidente
Monsieur Alain Ribaux, Co-président
Speichergasse 6 - Case postale
3001 Berne

Par courriel : info@kkjpd.ch

Réf. : 23_GOV_1236

Lausanne, le 7 février 2024

Convention intercantonale sur l'échange de données pour l'exploitation de plateformes de recherches et systèmes de bases de données communs

Madame la Co-présidente,
Monsieur le Co-président,

Nous avons bien reçu votre consultation du 23 novembre dernier, laquelle a retenu toute notre attention.

Nous avons pris note avec satisfaction que les suggestions émanant de nos services ont été repris en grande partie.

Le Conseil d'Etat vaudois se déclare favorable à la poursuite des travaux pour aboutir à un échange de données entre polices suisses qui soit efficace et respectueux du cadre juridique.

Comme souhaité, vous trouverez en annexe le texte de la convention contenant nos commentaires détaillés.

Nous vous prions de croire, Madame la Co-présidente, Monsieur le Co-président, à l'assurance de notre considération distinguée.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE — LE CHANCELIER a.i.

Christelle Luisier Brodard — François Vodoz

Annexe mentionnée

Copies

- Mme Sylvia Bula, Commandante de la Police cantonale

Conseil d'Etat
Staatsrat
CP 478, 1951 Sion

CANTON DU VALAIS
KANTON WALLIS

2024.00131

P.P. CH-1951 Sion A-PRIORITY Poste CH SA

Conférence des directrices et directeurs
des départements cantonaux de justice
et police (CCDJP)
Madame Karin Kayser-Frutschi et
Monsieur Alain Ribaux
Co-Présidents
Maison des cantons
Speichergasse 6
3001 Berne

Notre réf. 60
Votre réf. /

Date 24 JAN. 2024

Convention intercantonale sur l'échange de données à des fins d'exploitation de plates-formes de recherche et de systèmes de bases de données communs

Madame, Monsieur les Co-Présidents,

Le Conseil d'Etat du canton du Valais fait suite à votre correspondance du 23 novembre 2023 et vous remercie de l'avoir associé à la consultation précitée.

Pour une rapide mise en place d'une base de données permettant l'échange d'informations de manière efficace sur le plan national, nous soutenons le projet de convention intercantonale. Nous estimons également que l'adoption d'une base légale constitutionnelle retarderait considérablement la mise en place de ce projet.

Nous attirons votre attention sur le besoin de modifier les lois cantonales afin d'y intégrer les bases légales nécessaires pour permettre l'échange de données. Les deux articles actuellement proposés par la Conférence des commandantes et commandants des polices cantonales de Suisse (CCPCS) n'ont pas reçu l'approbation de la part du préposé cantonal valaisan à la protection des données qui a été consulté par la Police cantonale valaisanne dans le cadre de la modification de la loi sur la police cantonale. Ces articles ont ainsi été retirés de la modification en cours et nous restons dans l'attente de l'évolution du projet.

Nous vous prions d'agréer, Madame, Monsieur les Co-Présidents, l'assurance de notre considération distinguée.

Au nom du Conseil d'Etat

Le président — La chancelière

CANTON DU VALAIS CONSEIL D'ETAT

Christophe Darbellay — **Monique Albrecht**

Copie à M. Christian Varone, Commandant de la Police cantonale

Place de la Planta 3, CP 478, 1951 Sion
Tél. 027 606 21 00 · Fax 027 606 21 04

Regierungsrat, Postfach, 6301 Zug

Nur per E-Mail
Generalsekretariat KKJPD
Haus der Kantone
Speichergasse 6
Postfach
3001 Bern

Zug, 30. Januar 2024 rv

Vernehmlassung zur interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme
Stellungnahme des Kantons Zug

Sehr geehrte Damen und Herren

I. Allgemeines

Mit Schreiben vom 23. November 2023 haben Sie die Kantonsregierungen eingeladen, sich bis am 23. Februar 2024 vernehmen zu lassen. Nach Rücksprache mit dem Obergericht teilen wir Ihnen gerne mit, dass wir die Bestrebungen der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) bzgl. Schaffung einer gesetzlichen Grundlage für den interkantonalen Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksystemen begrüssen. Eine stärkere Vernetzung des polizeilichen Datenaustausches erscheint uns unabdingbar, um Kriminalität künftig effizienter bekämpfen zu können und – in den heutigen europa- wie auch weltpolitisch unruhigen Zeiten – die innere Sicherheit der Schweiz bestmöglich zu gewährleisten.

Im Einzelnen stellen wir folgende Anträge:

II. Anträge und Stellungnahmen sowie Begründung

1. Es sei eine kurze und treffende Abkürzung der Vereinbarung zu definieren.
Eine kurze und treffende Abkürzung erleichtert die einheitliche Zitierweise des Konkordats. Die Abkürzung könnte bspw. wie folgt lauten: «*Konkordat betreffend den interkantonalen Datenaustausch*».

2. Die Struktur des Ingresses sei anzupassen und die Vereinbarung gesetzestechnisch zu überarbeiten.
In Übereinstimmung mit anderen interkantonalen Vereinbarungen ist eine Struktur in der Art der folgenden zu wählen:

- Konkordatstitel
- Abkürzung
- «Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) verabschiedet gestützt auf ...»
- «... folgende interkantonale Vereinbarung: ...»

Ausführungen zu Sinn und Zweck des Konkordats sind im Zweckartikel (vgl. Art. 1 nachfolgend) aufzunehmen und entsprechend im Ingress zu streichen.

Gesetzestechnisch ist die Vereinbarung generell zu überarbeiten, wobei als Vorlage z.B. das Hooligan-Konkordat oder das ViCLAS-Konkordat genommen werden kann. Insbesondere sollte es Art. 1, Art. 2 etc. anstelle von Artikel 1. und Artikel 2. heissen oder es ist mit Absätzen (hochgestellte Ziffern ohne Punkt) anstelle der nun aufgeführten Ziffern innerhalb eines Artikels zu arbeiten. Da innerhalb der Vereinbarung auf Absätze verwiesen wird, nehmen wir an, dass dies eigentlich so gewollt und einfach eine falsche Formatierung gewählt wurde.

3. **Art. 2 Abs. 2 sei in Art. 36 zu integrieren und die Überschrift von Art. 36 in «Kantonale Gesetzgebung» zu ändern.**
Art. 2 und Art. 36 gehören systematisch zusammen. Beide regeln das kantonale Recht. Folglich erscheint ein Zusammenzug bzw. eine Regelung an einem Ort oder in einem Artikel sinnvoll. Abs. 2 von Art. 2 ist als Abs. 1 von Art. 36 aufzunehmen. In der Folge bzw. unabhängig davon ist auch die Überschrift von Art. 36 anzupassen, da Art. 36 (neu) allgemein die kantonale Gesetzgebung und nicht nur die kantonalen Gesetzesanpassungen regelt.

4. **Art. 3 Bst. c sei mit dem Begriff «Bedrohungsmanagement» zu ergänzen**
Die Begrifflichkeiten «Gefahrenabwehr», «Gewaltschutz» und «Bedrohungsmanagement» werden differenziert verwendet, sodass eine explizite Erwähnung des Begriffs «Bedrohungsmanagement» in Bst. c sinnvoll ist. So könnte Bst. c bspw. lauten: «Verhinderung von Straftaten, insbesondere Gefahrenabwehr im Sinne des Gewaltschutzes und des Bedrohungsmanagements».

5. **Der erläuternde Bericht zu Art. 4 sei dahingehend anzupassen, dass klargestellt wird, dass noch nicht sämtliche Kantone der PTI-Vereinbarung beigetreten sind. Ausserdem sei auf die im konkreten Fall geltende Fassung der PTI-Vereinbarung hinzuweisen (z. B. «die jeweils geltende Fassung der PTI-Vereinbarung»).**
Beide Anpassungen dienen der Rechtsklarheit bzw. -sicherheit.

6. **In Art. 5 sei der Begriff «Betriebsreglement» aufzunehmen und zu definieren.**
Der in Art. 19 verwendete Begriff «Betriebsreglement» bzw. dessen Definition fehlt bislang in den Begriffsdefinitionen von Art. 5.

7. **Art. 5 Abs. 5 sei wie folgt zu ergänzen: «*Daten sind Sach- und Personendaten inkl. besonders schützenswerter Personendaten, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von ihrer Darstellungsform und ihrem Informationsträger.*»**
Die Ergänzung ist sprachlich sinnvoll.

8. **Art. 5 Abs. 9 sei entsprechend der Funktion des Leistungserbringers zu formulieren (bspw. «*Der Leistungserbringer ist der für die Umsetzung der Leistungen verantwortliche Betreiber des Informationssystems*»).**
Die Neuformulierung erscheint passender und verständlicher.

9. **Es sei zu prüfen, wie Art. 6 und Art. 20 zueinanderstehen bzw. ob Art. 20 Abs. 3 aufgehoben werden kann. Allenfalls sei die Rechtmässigkeit dahingehend zu präzisieren, als zwischen der «rechtmässigen Erhebung» und der «inhaltlichen Richtigkeit» differenziert wird.**
Es ist unklar, ob die Rechtmässigkeit von Art. 20 Abs. 3 bereits in Art. 6 umfasst ist.

10. **Es sei in Art. 7 Abs. 1 zu prüfen, ob die Bestimmung um die Datenbearbeitungen gemäss Art. 20 Abs. 1 und 2 zu erweitern ist.**
Die in Art. 20 aufgeführten Datenbearbeitungen scheinen u. E. allgemeinverbindlichen Charakter zu haben bzw. nicht nur für Datenbanksysteme massgeblich zu sein.

11. **Art. 7 Abs. 2 sei als Abs. 4 aufzunehmen.**
Systematisch erscheint Abs. 2 eher als Abs. 4.

12. **Abs. 1 von Art. 8 sei so zu formulieren, dass die Teilnehmenden (die für die Datenbearbeitung verantwortlichen Gemeinwesen) einzige Haftungsverantwortliche sind.**
Dies im Sinne einer für die betroffene Person möglichst einfachen Haftungsregelung. Das verantwortliche Gemeinwesen wiederum kann auf fehlbare Mitarbeitende und Auftragnehmende Rückgriff nehmen.

13. **Der Hintergrund für die Regelung gemäss Art. 8 Abs. 2 sei im erläuternden Bericht wiederzugeben.**
Ansonsten entsteht der Eindruck, dass es keine Leistungserbringer ausserhalb des Instituts der Polizeitechnik und -informatik Schweiz (PTI) gibt.

14. **Es sei im erläuternden Bericht klar festzuhalten, ob sich Art. 9 ff. einzig POLAP widmen oder POLAP nur eine der möglichen Abfrageplattformen darstellt. Je nachdem seien allenfalls weitere Bestimmungen anzupassen.**
Im erläuternden Bericht geht nicht klar hervor, ob Art. 9 ff. einzig auf POLAP Anwendung finden. Dies muss klar sein, auch vor dem Hintergrund, als gemäss den Ausführungen zu Art. 13 des erläuternden Berichts auf die Ebene Betriebsverordnung verzichtet werden kann, da die gesetzliche Grundlage im revidierten BPI die Funktion einer solchen über-

nimmt. Sollen Art. 9 ff. Grundlage weiterer Abfrageplattformen bilden, ist der Erlass einer Betriebsverordnung vorzusehen respektive die entsprechende Regelung gemäss Art. 17 f. in die allgemeinen Bestimmungen aufzunehmen (mit der Einschränkung «wo nicht bereits durch übergeordnetes Recht definiert»). Gleiches gilt auch für die Bestimmungen bezüglich Erlass, Inhalt und Änderung eines Betriebsreglements in den Art. 9, 13, 14 und 19. Je nach Verständnis des Anwendungsbereichs von Art. 9 ff. ist die Formulierung «Abfrageplattform» oder «Abfrageplattformen» zu verwenden.

15. **Art. 11 Abs. 1 sei POLAP unabhängig wie folgt zu formulieren: «*Missbräuchliche Datenbearbeitungen sind der für die Abfrageplattform zuständigen Stelle und den anderen betroffenen Teilnehmenden zu melden*» (ohne den Zusatz «*des Bundes*»). Alternativ sei die gesamte Formulierung durch den «Verantwortlichen» zu ersetzen.**
Die interkantonale Vereinbarung regelt nicht nur die Abfrageplattform POLAP, für die fedpol die zuständige Meldestelle ist. Da es gemäss dem Bericht zu Art. 9 Abs. 1 in Zukunft auch andere und weitere Abfrageplattformen mit oder ohne «Bund» geben kann, muss Art. 11 Abs. 1 offener formuliert werden.

16. **In Abs. 2 von Art. 11 sei der Teilsatz «*und um den Schaden für die betroffene Person möglichst gering zu halten*» zu löschen.**
Es ist beim Teilsatz kein Mehrwert oder kein eigenständiger Inhalt ersichtlich. Wenn dies doch der Fall sein sollte, wäre dies entsprechend aufzuzeigen.

17. **Der Vereinbarungstext bzw. die Erläuterungen von Art. 12 Abs. 2 seien dahingehend zu präzisieren bzw. aufeinander abzustimmen, dass klar ersichtlich ist, dass für die Betriebskosten eine PTI-unabhängige Vereinbarung getroffen werden kann.**
Der Vereinbarungstext und die Erläuterungen von Art. 12 Abs. 2 stimmen nicht überein. Nicht jede Abfrageplattform wird zwingend durch sämtliche PTI-Kantone betrieben bzw. nur von PTI-Kantonen genutzt.

18. **Abs. 1 von Art. 13 sei zu löschen und infolgedessen Abs. 2 von Art. 13 anzupassen.**
Abs. 1 von Art. 13 (Erlass des Betriebsreglements) scheint obsolet, da dieser bereits in Art. 9 Abs. 1 geregelt ist. Falls dem nicht so sein sollte, wäre dies entsprechend zu präzisieren, indem der Mehrwert der Bestimmung aufgezeigt wird. Infolgedessen ist Art. 13 Abs. 2 (neuer Abs. 1) wie folgt zu ergänzen: «*Im Hinblick auf die Nutzung der Abfrageplattform sind im Betriebsreglement zu regeln: ...*».

19. **Art. 13 und Art. 14 sind aufeinander abzustimmen.**
Erstellung (Art. 13) und Änderung (Art. 14) des Betriebsreglements sollten den gleichen Anforderungen unterstehen. Bzgl. der Änderung des Betriebsreglements wird «nur» im erläuternden Bericht auf die Erstellung verwiesen. In der Konsequenz wird auch bei der Erstellung des Betriebsreglements die Zustimmung des Bundes explizit vorausgesetzt, was im Gesetzestext (Art. 13) ebenso ersichtlich bzw. vermerkt sein sollte.

20. Die Systematik und die Begrifflichkeiten des 3. Kapitels seien zu überprüfen bzw. der Systematik des 2. Kapitels anzugleichen.

Die vorliegende Vereinbarung regelt zwei Bereiche: gemeinsame Abfrageplattformen (Kapitel 2) und Datenbanksysteme (Kapitel 3). Folglich sollten die Systematik und die Begrifflichkeiten der beiden Bereiche übereinstimmen. In diesem Zusammenhang wäre bspw. folgende Systematik denkbar:

- Art. 16 Gemeinsame Datenbanksysteme (Titel ersetzen durch «Betrieb und Nutzung»)
- Art. 22 Organisation
- Art. 24 Zugriffsberechtigungen
- Art. 25 Protokollierung
- Art. 26 Datenlöschung
- Art. 28 Auftragsbearbeitung (Titel ersetzen durch «Bearbeitungsort und Auftragsbearbeitung»)
- Art. 27 Betroffenenrechte
- Art. 23 Meldung von Missbrauch
- Art. 29 Kostentragung
- Art. 17 Betriebsverordnung (Titel ersetzen durch «Ausführungsbestimmungen»)
- Art. 18 Inhalt der Betriebsverordnung (Titel ersetzen durch «Betriebsverordnung»)
- Art. 19 Betriebsreglement (besser: aufnehmen als Art. 17 Abs. 4)
- Art. 30 Beitritt (unter Umständen Art. 30–32 als «Beitritt, Kündigung und Ausscheiden» zusammenfassen)
- Art. 31 Änderung der Betriebsverordnung (besser: in Art. 32 aufnehmen)
- Art. 32 Kündigung und Austritt (Titel ersetzen durch «Kündigung und Ausscheiden»)
- Art. 33 Liquidation eines gemeinsamen Datenbanksystems

21. Es sei zu prüfen, ob Abs. 2 und Abs. 3 von Art. 17 zusammengefasst werden können.

In beiden Absätzen wird der Erlass der Betriebsverordnung und ihrer Änderungen geregelt, sodass diese allenfalls zusammengefasst werden können.

22. Art. 19 sei wie folgt anzupassen: «*Die operative Versammlung PTI erlässt ~~und aktualisiert~~ ein Betriebsreglement und passt dieses bei Bedarf an.*»

Mit der vorgeschlagenen Formulierung wird präzisiert, dass eine Aktualisierung bzw. Anpassung des Betriebsreglements (nur) bei Bedarf erfolgt.

23. In Art. 19 sei eine allfällige Beteiligung des Bundes zu berücksichtigen.

Vgl. Antrag zu Art. 13 und Art. 14 oben (wo die Erstellung und Änderung des Betriebsreglements der Abfrageplattform geregelt ist).

24. In Abs. 2 von Art. 23 sei der Teilsatz «und um den Schaden für die betroffene Person möglichst gering zu halten» zu löschen.

Vgl. Antrag zu Art. 11 Abs. 2 oben (wo die Missbrauchsmeldung bei der Abfrageplattform geregelt ist).

25. **Art. 26 Abs. 1 sei wie folgt anzupassen: «*Die Daten sind umgehend zu löschen, wenn feststeht, dass sie nicht mehr benötigt werden. Die Löschung erfolgt jedoch spätestens zehn Jahre nach Erfassung des letzten Datenzuwachses.*»**
Das Recht auf Löschung ist ein verfassungsmässiges Recht, welches sich aus Art. 13 Abs. 2 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101) ableitet. Werden Daten für die in Art. 3 umschriebenen Zwecke nicht mehr benötigt, sind sie umgehend zu löschen, was in Abs. 1 unmissverständlich festgehalten bzw. präzisiert werden sollte.

26. **Der Titel von Art. 28 sei wie folgt anzupassen: «*Bearbeitungsort und Auftragsbearbeitung*».**
Art. 28 regelt nicht nur die Auftragsbearbeitung, sondern ebenso den Bearbeitungsort, was im Titel entsprechend zu vermerken ist.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und die Berücksichtigung unserer Anträge.

Zug, 30. Januar 2024

Freundliche Grüsse
Regierungsrat des Kantons Zug

Silvia Thalmann-Gut
Frau Landammann

Tobias Moser
Landschreiber

Versand per E-Mail an:
- Generalsekretariat KKJPD (info@kkjpd.ch als PDF- und Word-Version)
- Sicherheitsdirektion (info.sd@zg.ch)
- Finanzdirektion (info.fd@zg.ch)
- Zuger Polizei (kommandooffice.polizei@zg.ch; Rechtsdienst.Polizei@zg.ch)
- Obergericht des Kantons Zug (Marc.Siegwart@zg.ch)
- Datenschutzstelle des Kantons Zug (datenschutz.zug@zg.ch)
- Zuger Mitglieder der Bundesversammlung
- Staatskanzlei (info.staatskanzlei@zg.ch zur Aufschaltung der Vernehmlassungsantwort im Internet)

Kanton Zürich
Regierungsrat

Co-Präsidium der Kantonalen Justiz- und
Polizeidirektorinnen und -direktoren
Generalsekretariat KKJPD
Haus der Kantone
Speichergasse 6
Postfach
3001 Bern

24. Januar 2024 (RRB Nr. 52/2024)

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme (Stellungnahme)

Sehr geehrte Frau Präsidentin
Sehr geehrter Herr Präsident

Wir beziehen uns auf Ihr Schreiben vom 23. November 2023, mit dem Sie uns zur Konsultation zum Entwurf einer interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme eingeladen haben. Wir danken für die Gelegenheit zur Stellungnahme und äussern uns wie folgt:

Wir begrüssen ausdrücklich die eidgenössische Lösung, die mit der von der Sicherheitskommission des Nationalrates eingereichten Motion 23.4311 betreffend Schaffung einer Verfassungsgrundlage für eine Bundesregelung des nationalen polizeilichen Datenaustausches angestrebt wird. Der Nationalrat hat diese am 19. Dezember 2023 ohne Gegenstimme überwiesen. Diese Lösung ist nun rasch voranzutreiben, um schweizweit eine verlässliche Grundlage für den Datenaustausch zu schaffen.

Die Umsetzung einer interkantonalen Vereinbarung erachten wir als unrealistisch. Zu bemerken ist, dass in der Vergangenheit vielfach verschiedene Kantone nicht zuletzt aus demokratiepolitischen Überlegungen nicht zur Unterzeichnung solcher Vereinbarungen bereit waren.

Genehmigen Sie, sehr geehrte Frau Präsidentin,
sehr geehrter Herr Präsident,
den Ausdruck unserer vorzüglichen Hochachtung.

Im Namen des Regierungsrates

Der Präsident:	Die Staatsschreiberin:
Mario Fehr	Dr. Kathrin Arioli