

Generalsekretariat

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme

Auswertungsbericht Vernehmlassung «POLAP»

Generalsekretariat KKPks, Haus der Kantone, Speichergasse 6, 3011 Bern

Tel. +41 (0)31 512 87 20, info@kkpks.ch

Bern, 12. April 2024



Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme

Auswertungsbericht Vernehmlassung «POLAP»

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
Abkürzungen und Begriffe	3
Vernehmlassung "POLAP".....	4
1. Zusammenfassung	4
2. Auswertung Vernehmlassung «POLAP»	5
Zweckbestimmung.....	5
Verfassungsrechtliche Kompetenzordnung.....	5
Bedarf an polizeilichen Abfrageplattformen und gemeinsamen Datenbanksystemen ..	6
3. POLAP.....	10
Verantwortlichkeiten	10
Rechtsgrundlagen	11
Funktionsweise	11
Polizeiliche Kompetenzen	12
4. Gemeinsame Datenbanksysteme	13
5. Weiteres Vorgehen	14

Abkürzungen und Begriffe

Abkürzung	Definition
<i>Art.</i>	Artikel
<i>BPI</i>	Bundesgesetzes über die polizeilichen Informationssysteme des Bundes vom 13. Juni 2008, SR 361
<i>BV</i>	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101
<i>BGG</i>	Bundesgesetz über das Bundesgericht vom 17. Juni 2005 SR 173.110
<i>EDÖB</i>	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
<i>EinfG</i>	Einführungsgesetz
<i>EJPD</i>	Eidgenössisches Justiz- und Polizeidepartement
<i>fedpol</i>	Bundesamt für Polizei fedpol
<i>GUI</i>	Graphical User Interface
<i>ISC</i>	Informatik Service Center
<i>KAPO</i>	Kantonspolizei
<i>OAB</i>	Onlineanlagebetrug
<i>PICSEL</i>	PICSEL ist eine Datenbank, die spezifisch die Analyse von Cyberkriminalität-Erkenntnissen ermöglicht (System zur Informationsbeschaffung u.a. mit dem Ziel, Fallverknüpfungen und Serien innerhalb einer stetig steigenden Zahl von Cyberdelikten über die Kantonsgrenzen hinaus zu identifizieren).
<i>PKS</i>	Polizeiliche Kriminalstatistik
<i>POLAP</i>	Polizeiabfrageplattform
<i>PolG</i>	Kantonales Polizeigesetz
<i>PTI</i>	Polizeitechnik und -informatik Schweiz
<i>PTI-Vereinbarung</i>	Vereinbarung zwischen dem Bund und den Kantonen über die Harmonisierung und die gemeinsame Bereitstellung der Polizeitechnik und -informatik in der Schweiz (PTI-Vereinbarung)
<i>RIPOL</i>	Nationales Fahndungssystem
<i>SR</i>	Systematische Rechtssammlung
<i>VOSTRA</i>	Strafregister-Informationssystem
<i>ZEMIS</i>	Zentrales Migrationsinformationssystem



Vernehmlassung "POLAP"

1. Zusammenfassung

Die Vernehmlassung «POLAP» der KKJPD zur Interkantonalen Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme fand vom 23. November 2023 bis zum 23. Februar 2024 statt.

Rückmeldungen wurden vom EDÖB, vom fedpol, vom Bundesamt für Zoll und Grenzsicherheit, von privetim, der Digitalen Gesellschaft, der Konferenz der Städtischen Sicherheitsdirektorinnen und -direktoren, der Sozialdemokratischen Partei der Schweiz sowie den Kantonen Luzern, Zürich, Wallis, Uri, Basel-Landschaft, Freiburg, Waadt, Genf, Bern, Thurgau, Schwyz, Neuenburg, Solothurn, Obwalden, Glarus, Nidwalden, Aargau, Jura, Appenzell-Innerrhoden, Tessin, Schaffhausen, Appenzell-Ausserrhoden und Basel-Stadt eingereicht.

Die Schaffung einer interkantonalen Vereinbarung erhält weiterhin breite Unterstützung. Lediglich ein Kanton hält die Umsetzung einer interkantonalen Vereinbarung für unrealistisch und nur ein weiterer Kanton meldete, dass er dem Konkordatsentwurf nicht zustimmen könne, weil gewisse Bestimmungen fehlen würden.

Mehrfach bekräftigt wurde der Wunsch nach einer Regelung auf nationaler Ebene. Ausdrücklich begrüsst wurde darum die Motion 23.4311 zur Schaffung einer Verfassungsgrundlage für eine Bundesregelung des nationalen polizeilichen Datenaustauschs, welche von der Sicherheitskommission des Nationalrates eingereicht wurde. Auch der EDÖB ist der Ansicht, dass das Ziel der Vereinbarung nur mit der Schaffung einer neuen Bestimmung in der Bundesverfassung rechtmässig und glaubwürdig erreicht werden könne. Eine Verfassungsänderung wäre dem obligatorischen Referendum unterstellt und würde dem Schweizer Volk zur Abstimmung vorgelegt, womit der vorgesehene Polizeidatenaustausch eine breitere demokratische Legitimation geniessen würde.

Inhaltlich wurde in vielen Rückmeldungen auf datenschutz- und grundrechtliche Bedenken hingewiesen. Angezweifelt wurde vor allem, ob der Entwurf dem verfassungsmässigen Bestimmtheitsgebots und Verhältnismässigkeitsprinzip gerecht werde. Auch wurde die Ansicht vertreten, dass ein automatisierter Datenaustausch im Abrufverfahren und gemeinsame Datenbanksysteme zwischen den Kantonen einerseits und zwischen den Kantonen und dem Bund andererseits gegen die staatsrechtliche Kompetenzverteilung im Polizeibereich verstosse.

Diverse Rückmeldungen betrafen auch die kantonalen Polizeigesetze, die kürzlich revidiert wurden oder die sich gerade in einem Revisionsprozess befinden und bereits eine Rechtsgrundlage für einen kantonsübergreifenden Datenaustausch beinhalten.

Eingereicht wurden Rückmeldungen und Fragen zum anwendbaren Recht und zu der datenschutzrechtlichen Verantwortlichkeit für die unter diesem Konkordat zu schaffenden



Informationssysteme. In diesen Themen soll die Überarbeitung des Konkordatstexts und des erläuternden Berichts Klarheit verschaffen.

2. Auswertung Vernehmlassung «POLAP»

Zweckbestimmung

Die KKPKS stellt fest, dass insbesondere zum Gegenstand und Zweck (Art. 1) und zum Anwendungsbereich (Art. 3) angemerkt wurde, dass die offenen und breiten Formulierungen beinahe alle polizeilichen Aufgabenfelder umfassen und die Vereinbarung folglich nicht mit dem Legalitätsprinzip, dem Bestimmtheitsgebot und dem Verhältnismässigkeitsprinzip vereinbar sei. Es bestehen darum Zweifel, ob die Vorlage in der gegenwärtigen Form einem Normenkontrollverfahren standhalten würde. Gestellt wurde auch die Frage, ob auf der ganzen Breite des Konkordats ein überwiegendes öffentliches Interesse bestehe, welches die Grundrechtseingriffe aus dem Datenaustausch rechtfertige (Art. 36 Abs. 2 BV).

Um dem Bestimmtheitsgebot gerecht zu werden und den Zweck der Vereinbarung einzugrenzen, prüft die KKPKS zurzeit die Option, die Voraussetzung einer Abfrage über die POLAP an die Schwere der Straftat zu knüpfen. Konkret werden verschiedene Deliktskataloge geprüft, die ein ausbalanciertes Verhältnis zwischen Abfragebedarf und Grundrechtseingriff bieten. Würde diese Option eingeführt, bedeutete dies, dass nur beim Vorliegen bestimmter Straftaten eine Polizeibehörde über die POLAP Daten abrufen dürfte. Der Deliktskatalog sollte Voraussetzung für die Bekanntgabe der Daten sein, denn die Schwere des Delikts entscheidet über die Berechtigung zur Bekanntgabe der Informationen. Ob die abfragende Behörde, die aus POLAP erhaltenen Informationen dann weiterbearbeiten darf, richtet sich nach den Rechtsgrundlagen dieser Behörde.

Aus grundrechtlicher Sicht würde die Einführung eines Deliktskataloges, welcher nur bei Vorliegen bestimmter – u.U. nur schwerer – Straftaten zu einer Abfrage berechtigt, bedeuten, dass die Voraussetzungen für einen Grundrechtseingriff erhöht würden. Ein solche Option wird von der KKPKS auch für die gemeinsamen Datenbanksysteme in Erwägung gezogen.

Verfassungsrechtliche Kompetenzordnung

Aus einigen Rückmeldungen vernahm die KKPKS, dass wegen dem breiten Anwendungsbereich das Konkordat der verfassungsrechtlichen Kompetenzordnung widerspreche, welche die Polizeikompetenzen primär den Kantonen zuweist (Art. 3 und 57 BV). Die verfassungsrechtlich vorgegebene Aufgabenteilung zwischen Bund und Kantone bei der Verhinderung, Bekämpfung und Ermittlung von Straftaten würde dadurch verwischt werden.

Die KKPKS stellt sich auf den Standpunkt, dass wegen der kantonalen Polizeihöhe (Art. 3 BV) die Gesetzgebungskompetenz im Bereich der Polizeiarbeit bei den Kantonen liegt. Sie können ihre Aufgaben in diesem Bereich unter den rechtlichen Rahmenbedingungen souverän wahrnehmen. Auf der Gegenseite verfügt der Bund nur über jene Befugnisse, die ihm die Verfassung zuweist.



Gemeinsam ist dem Bund und den Kantonen, dass sie die Sicherheit des Landes zu wahren haben (Art. 2 Abs. 1 BV) und sich gegenseitig bei der Erfüllung ihrer Aufgaben unterstützen (Art. 44 BV). Daraus schliesst die KKPKS, dass es durchaus verfassungskonform ist, über den Bund betriebene Abfrageplattformen für den Datenaustausch zwischen kantonalen Quellsystemen und gemeinsame Datenbanksysteme zu errichten und zu betreiben. Einerseits unterstützt der Bund so die Kantone in der Erfüllung ihrer polizeilichen Aufgaben. Andererseits können die Kantone aber auch gestützt auf ihre Polizeihoheit den Bund bei der polizeilichen Aufgabenerfüllung beiziehen und gemeinsame Datenbanksysteme errichten, indem sie die entsprechenden Rechtsgrundlagen schaffen. Mit anderen Worten ergibt es sich aus der Polizeihoheit der Kantone, dass sie mit dem Bund zusammenarbeiten können, wenn sie dies zu ihrer Aufgabenerfüllung als opportun erachten. Nur weil Bund und Kantone in unterschiedlichen Konstellationen an gemeinsamen Abfrageplattformen und Datenbanken teilnehmen, heisst dies noch nicht, dass ein Widerspruch zur verfassungsrechtlichen Kompetenzordnung vorliegt. Es ergibt sich aus den jeweiligen Rechtsgrundlagen, ob Bund oder Kantone in gemeinsamen Abfrageplattformen oder Datenbanken Polizeidaten eintragen und abfragen dürfen.

Die KKPKS zieht daraus den Schluss, dass unter diesem Blickwinkel die Verwendung des Begriffs „nationaler Schweizer Polizeidatenraum“ irreführend war und im zukünftigen Konkordatstext nicht mehr gebraucht werden soll. Der Begriff wurde unter Bezugnahme auf die Motion Eichenberger vom 9. Dezember 2019 in den Entwurf eingeführt, um den Zusammenhang zwischen dieser und dem Konkordat aufzuzeigen. Es geht jedoch nicht darum, einen einzigen nationalen Polizeidatenraum zu schaffen, welcher sämtlichen Polizeibehörden pauschal und jederzeit Zugriff auf sämtliche vorhanden Polizeidaten gewährt. Das Konkordat hat zum Ziel, die Rechtsgrundlagen dafür zu schaffen, dass die Polizeibehörden bei ausgewiesenen Bedarf und unter Einhaltung rechtsstaatlicher Prinzipien gemeinsame Abfrageplattformen und Datenbanksysteme schaffen und betreiben können. Mit dem gezielten Einsatz moderner Technologien können sie ihre polizeilichen Aufgaben effizienter und effektiver erfüllen.

Bedarf an polizeilichen Abfrageplattformen und gemeinsamen Datenbanksystemen

Die KKPKS vertritt den Standpunkt, dass die Frage nach einem interkantonalen Datenaustausch nicht neu sei und in den Kantonen seit längerer Zeit diskutiert werde. Auch gab es bereits gewisse Arbeiten, welche die Thematik aufnahmen. So wurde die Interkantonale Vereinbarung über die computergestützte Zusammenarbeit der Kantone bei der Aufklärung von Gewaltdelikten (ViCLAS-Konkordat) bereits am 2. April 2009 unterzeichnet. Per Februar 2012 trat die Erweiterung des Konkordats über Massnahmen gegen Gewalt bei Sportveranstaltungen in Kraft. Und gemäss Art. 24a des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (SR 120) besteht ein zentrales Informationssystem, betrieben von fedpol, in welchem die Massnahmen gemäss Konkordat eingetragen werden. Aber aufgrund des föderalistischen Aufbaus der Schweiz bilden kantonsübergreifende oder nationale Systeme die Ausnahme. Aktuell hat jedes Polizeikorps neben den nationalen Systemen (RIPOL, ZEMIS, Polizeiindex, VOSTRA u.a.) insbesondere ein eigenes Vorgangsbearbeitungssystem, welches alle polizeilichen Vorgänge abbildet.



Polizeibehörden sind nur vereinzelt berechtigt, in den polizeirelevanten Datenbanken anderer Gemeinwesen Daten abzurufen (z.B. im Bereich der gerichtspolizeilichen Ermittlungen nach Art. 10 Abs. 4 BPI). Die Daten müssen in der Regel bei jeder Behörde einzeln und seriell abgefragt werden. Bei den heutigen Kriminalitätsformen ist die KKPKS der Ansicht, dass für eine effektive und effiziente Verhinderung, Bekämpfung und Ermittlung von Straftaten ein automatisierter Datenaustausch notwendig sei, wie aus den nachfolgenden Beispielen hervorgeht.

Polizeiliche Vorgänge einer bestimmten Person: Die Kantonspolizei Bern ist regelmässig mit Personen konfrontiert, welche andere Personen in der psychischen, physischen oder sexuellen Integrität gefährden. Diese Gefährdung kann sich gegen Personen aus dem privaten, beruflichen oder schulischen Umfeld, aber auch gegen Angehörige von Behörden, Amtsstellen, Institutionen oder Firmen richten. Solche Personen treten häufig in verschiedenen Kantonen in Erscheinung (z.B. ausserkantonaler Arbeitsort oder Bezugspersonen in anderen Kantonen). Insbesondere bei akuten Gefährdungssituationen ist eine zeitverzugslose Erkennung von sämtlichen polizeilichen Vorgängen der betreffenden Person für eine fundierte Lageeinschätzung zentral. Nur so können die erforderlichen Massnahmen rechtzeitig getroffen werden.

«Gefährder»: Eine Person sprach im Kanton Bern massive Drohungen gegenüber einer Gerichtspräsidentin aus, weshalb mit einer unmittelbar bevorstehenden Eskalation der Gewalt gerechnet werden musste. Der Wohnort der drohenden Person ist ausserkantonale, ihr Arbeitsort befindet sich in einem dritten Kanton. In sämtlichen betreffenden Kantonen ist die Person mit schweren Drohungen sowie teilweise gewalttätigem Verhalten in Erscheinung getreten. In einer ersten Phase haben sämtliche Kantone eigenständig Massnahmen zur Gefahrenabwehr eingeleitet. Erst im Rahmen der weiteren Überprüfung zeigten sich die Zusammenhänge und die Massnahmen konnten koordiniert werden. Eine rasche Lagebeurteilung unter Berücksichtigung sämtlicher bekannter Vorfälle ist insbesondere in solchen akuten Situationen von zentraler Bedeutung und kann dazu beitragen, dass Gewalttaten rechtzeitig verhindert werden können. Mit den vorhandenen Mitteln zum Datenaustausch können derartige Informationen für solche akuten Bedrohungslagen nicht rechtzeitig beschafft werden, weil die gerichtspolizeiliche Abarbeitung erst später erfolgt bzw. Anfragen nicht zeitverzugslos bearbeitet werden.

Ermittlungsdaten: In der komplexen kriminellen Realität können Ermittlungen nicht mehr innerhalb der kantonalen Strukturen bewältigt werden. Kriminelle Gruppierungen agieren interkantonal und oft international. Dies gilt insbesondere in den Bereichen Cyber, Menschenhandel, Terrorismus sowie bei bandenmässig begangenen Vermögensdelikten, wo die Tätergruppierungen typischerweise vernetzt vorgehen. In solchen Fällen ist der Austausch von Ermittlungsdaten von zentraler Bedeutung. Nur wenn den Ermittlungsdiensten diese Daten zur Verfügung stehen, können sie entsprechende Serien und Zusammenhänge erkennen.



Tötungsdelikt: In einem ausserkantonalen ColdCase (Tötung einer Prostituierten) wurden verschiedene Kantone mit einer Massen-DNA-Profilerstellung beauftragt. Die Kantonspolizei Bern ist mit zwei Personen betroffen. Eine dieser Personen ist im Kanton Bern wegen Gewaltpornografie (Tötungsfantasien) polizeilich bekannt. Aufgrund der konkreten Umstände wäre diese Person für den fallführenden Kanton von höchstem Interesse gewesen. Dieser Zusammenhang wurde jedoch erst erkannt, als im Zusammenhang mit dem Wangenschleimhautabstrich eine Überprüfung der Person durch die Kantonspolizei Bern erfolgte. Auf den Namen der betroffenen Person war die zuständige Polizei vorgehend lediglich aufgrund von Mitteilungen aus der Bevölkerung nach einem Beitrag in der Sendung «Aktenzeichen XY Un gelöst» gestossen.

Um in vergleichbaren Fällen – oder aber auch bei anderen Delikten – solche Zusammenhänge zu erkennen, muss (Stand heute) eine Anfrage an die Polizeikörpers der Schweiz (Verbreitung national) getätigt werden. Dabei kommt es leider nicht selten vor, dass die Rückmeldungen unvollständig sind oder sogar vergessen gehen. Dabei spielt es sicher auch eine Rolle, dass die antwortende Behörde nicht über Fallkenntnisse verfügt und damit u.U. nicht erkennt, welche Informationen für die Ermittlungen von Bedeutung sind.

Cyber: Im Unterschied zu Delikten in der analogen Welt weisen Delikte im Bereich der Cyberkriminalität einen hohen globalen Impact auf. Das bedeutet, dass ein Angriff in der Regel unzählige Betroffene weltweit oder zumindest in einer bestimmten Region betrifft. Dabei entstehen digitale Indikatoren (zum Beispiel IP-Adressen, Domain-Namen, Krypto-Transaktionen, Malware-Signaturen, Phishing-Links etc.), die erst im Gesamtzusammenhang ein Spurenbild ergeben, das ermöglicht, die Täterschaft zu identifizieren. Mit dem automatisierten Austausch dieser Indikatoren könnten parallele Untersuchungen vermieden werden. Aktuell müssen die Fälle einzeln behandelt werden, was einen enormen Mehraufwand nach sich zieht.

Aufgrund einer Strafanzeige wegen eines Online-Anlagebetrugs konnte anhand der numerischen Kennung (IP-Adresse) der durch die Täterschaft verwendeten Infrastruktur (Remote-Zugriff, Mailversand und durch die Täterschaft betriebene Handelsplattform) Server erkannt, sichergestellt und die Täterschaft identifiziert werden. In einem weiteren Fall eines Online-Anlagebetrugs konnte lediglich die Site Technologie zzgl. Zertifikat der durch die Täterschaft betriebenen Handelsplattformen identifiziert werden. Mit dem automatisierten Austausch solcher Daten könnten künftig Zusammenhänge zwischen den beiden Fällen früher bzw. überhaupt erkannt und damit wertvolle Erkenntnisse zur Identifikation der Täterschaft gewonnen und allenfalls weitere Fälle verhindert werden.

Cybercrime: Einzig mittels einer nationalen Datenbank kann ein nationales Lagebild erstellt werden. Solange kein gemeinsames Datenbanksystem besteht, weiss eine Polizeibehörde einzig, was in ihrem Kanton vor sich geht.

Ebenso ist eine solche Datenbank notwendig, um zuverlässig feststellen zu können, ob in anderen Kantonen gegen dieselbe Täterschaft ermittelt wird. Da im Bereich Cyber zu Beginn eines Verfahrens fast immer eine unbekanntes Tätergruppierung steht, gibt auch kein Strafregisterauszug Auskunft über allfällig weitere pendente oder abgeschlossene Verfahren in anderen Kantonen oder beim Bund. Dadurch entstehen Doppelspurigkeiten (mehrfach



dieselben Beweiserhebungen durch verschiedene Kantone, doppelter Personalaufwand etc.) und die Klärung der Zuständigkeitsfrage gestaltet sich schwierig und langwierig. Ein gutes Beispiel dafür ist eine Ransomware-Gruppierung, die eine Vielzahl von Unternehmen in der Schweiz angreift und erpresst.

Ebenso wenig können Referenzierungsmerkmale (wie täterische Krypto-, IP- oder E-Mail-Adressen, Rufnummern etc.) national abgeglichen und (unabhängig vom Phänomen) einzelne Fälle einer Deliktsserie – begangen durch dieselbe Täterschaft – zugeordnet werden. Da ein Einzelfall in der Regel kaum Ermittlungsansätze bietet, hat dieser Umstand zur Folge, dass die einzelnen Fälle sistiert oder eingestellt (bzw. ins Archiv rapportiert) werden. Würden die Fälle jedoch zufolge übereinstimmender Referenzierungsmerkmale als Deliktsserie erkannt und die entsprechenden Verfahren vereinigt, erhöhten sich die Chancen massiv, dass sich daraus erfolgversprechende Ermittlungsansätze ergeben und folglich die Täterschaft identifiziert und zur Rechenschaft gezogen werden kann.

Wirtschaftsdelikte: Die sog. OAB-Datenbank heisst «PICSEL» und wird durch die Aargauer und Genfer Kantonspolizei betrieben. Es werden dort seit ca. zwei Jahren die Referenzierungsmerkmale aus sämtlichen OAB-Rapporten in der Schweiz eingespeist. Die Daten werden laufend analysiert und im Rahmen von OAB-Sitzungen der Single-Point-of-Contact sämtlicher Kantone (organisiert durch das Netzwerk digitaler Ermittlungsunterstützung Internetkriminalität) regelmässig besprochen.

«PICSEL» ist eigentlich ein Proof of Concept. Es hat gezeigt, dass sich im Bereich serieller «Cyber-Wirtschaftskriminalität» in einer ersten Phase erhebliche Ressourcen einsparen lassen, wenn man sich auf das «Datensammeln» beschränkt. «PICSEL» erlaubt es dann, «auf Knopfdruck» sämtliche Informationen zu Verfahren, die mit bestimmten Referenzierungsmerkmalen übereinstimmen, gesamtschweizerisch zusammenzuziehen (IP-Adressen, Telefonnummern, Aliasnamen der Telefonverkäufer, Kontonummern, Krypto-Adressen etc.). Derzeit laufen in verschiedenen Kantonen Sammelverfahren, bei denen so vorgegangen wurde. Auch hinsichtlich internationaler Koordination und Kooperation sind die Polizeibehörden grundsätzlich gut aufgestellt.

«PICSEL» greift aber in diversen Punkten zu kurz. Insbesondere was den Umfang der «einzuliefernden» Delikte angeht (derzeit beschränkt auf OAB), bei der Datenanalyse (sehr «handgestrickt»), beim Datenaustausch interkantonal und international (keine Zuständigkeit definiert) und beim Wirkungsgrad (kein Einsatz im Rahmen von Präventionsmassnahmen und hinsichtlich der Disruption krimineller Netzwerke) ist das Konzept erheblich ausbaubedürftig. Es sollen die Daten sämtlicher «Cyber-Wirtschaftskriminalität-Delikte» (gemäss Terminologie der PKS) sowie der Geldwäscherei-Verfahren (insb. Money Mule) in einer modernen Datenbank gesammelt und in einer professionellen Analyse zugänglich gemacht werden. Zudem muss ein zentral gesteuerter Prozess implementiert werden, der einen effizienten Zusammenschluss von Verfahren im Rahmen nationaler und internationaler Kooperationen sicherstellt. Auch bei «Enkeltrick-Betrügen» geht es um ein serielles Vorgehen durch international organisierte Verbrecherbanden. Letztendlich ist aber wohl auch hier die Sammlung von Daten (verwendetes Betrugskonzept, Telefonnummern, Aliasnamen, Stimmenmuster etc.) ein zentrales Element bei der Verfolgung dieser Deliktskategorie. Entsprechend



macht es Sinn, auch die spezifischen Referenzierungsmerkmale der Einzeltrick-Betrüger in der Schweiz in einer zentral geführten Datenbank zu erfassen.

Strassenverkehrsdelikte, häusliche Gewalt, Bedrohungsmanagement: Bei einer Fahrzeugkontrolle erhalten die Mitarbeitenden ohne POLAP nur ein unvollständiges Bild über die zu kontrollierende Person. Das zeigt illustrativ, wenn einem Lenker im Kanton X bereits mehrfach (innert kürzester Zeit) der Führerschein abgenommen wurde, er jetzt aber im Kanton Y erstmals kontrolliert wird. Die Polizeibeamten werden zwar auf das Fahren trotz Entzug rapportieren, aber das Auto als «Tatwaffe» nicht sicherstellen, weil bei einem erstmaligen Vorfall davon abgesehen wird. Könnten die Polizisten aber seine Vorakten über POLAP einsehen, würden die Zwangsmassnahmen gegen den Beschuldigten sicherlich härter ausfallen. Es liesse sich rechtfertigen, das Fahrzeug sicherzustellen und man könnte u.U. auf Untersuchungshaft wegen Wiederholungsgefahr beantragen.

Fälle häuslicher Gewalt enden für die beschuldigte Person, sofern sie niederschwellig sind, nicht mit einer Zuführung zur Staatsanwaltschaft. Sähen die Polizisten hingegen von Beginn weg die Vorakten des oder der Beschuldigten aus allen Kantonen, wäre eine Zuführung selbst bei grenzwertigen Fällen (Tätlichkeit Ja/Nein/unklar oder Intensität der Drohung unklar) möglich.

Das gleiche Bild ergibt sich in Fällen, wo lediglich eine Ausführungsgefahr rapportiert wurde. Beispielsweise schreit eine Person in einer S-Bahn, dass in einer Woche der ganze Bahnhof X explodieren und es zu zahlreichen Toten und Verletzten kommen werde. Es liegt bei dieser Ausgangslage kein Delikt vor, weil kein Geschädigter einen Strafantrag wegen Drohung stellen konnte und der Staatsanwalt muss aufgrund dieses einen Vorfalls entscheiden, ob er den Beschuldigten für eine Begutachtung in Untersuchungshaft nimmt oder ihn ambulant und damit in Freiheit von einer Fachperson begutachten lässt. Es ist enorm schwierig und riskant, die Beschuldigten innert der kurzen Zeit einer Hafteinvernahme richtig einzuschätzen. Lügen hingegen Hinweise auf ähnliche Verhaltensmuster aus anderen Kantonen oder gar Verurteilungen vor, würde das den Entscheid für oder gegen einen Antrag auf Untersuchungshaft sehr erleichtern.

3. POLAP

Verantwortlichkeiten

Die KKPKS informiert, dass sich mittlerweile für POLAP die technischen und rechtlichen Strukturen der Abfrageplattform weiter ausdifferenziert haben. Für den Betrieb und die Datenbearbeitungen in POLAP ist fedpol als Verantwortlicher im Sinne des DSG und als Betreiber festgelegt. POLAP wird für die Polizeibehörden der Kantone und des Bundes betrieben. Das ISC-EJPD übernimmt den technischen Betrieb.

Deswegen können die Aufgaben und die Verantwortlichkeiten von PTI für POLAP reduziert werden. Der Konkordatstext ist in dieser Hinsicht zu überarbeiten und zu vereinfachen. Der Fokus des Entwurfs liegt bei der Schaffung der Rechtsgrundlagen, so dass Polizeidaten automatisiert über eine Abfrageplattform abgerufen und bekannt gegeben werden können.

Rechtsgrundlagen

Auf Bundesebene werden die Rechtsgrundlagen mit der BPI-Revision geschaffen, welche nach dem jetzigen Kenntnisstand 2026 in Kraft treten sollte.

Auf kantonaler Ebene hält die KKPKS fest, dass in den meisten Kantonen bereits die heutigen Rechtsgrundlagen in den Polizeigesetzen den Polizeibehörden ermöglichen, mit Polizeibehörden aus anderen Kantonen Daten auszutauschen und ihnen bekannt zu geben. Dies geschieht heute teilweise noch über die Amtshilfe per Telefon oder per E-Mail. Mittels POLAP sollen den Polizeibehörden keine neuen polizeilichen Kompetenzen erteilt werden, sondern nur das Abrufverfahren geregelt werden. Der Datenaustausch, welcher heute schon physisch und analog stattfindet, soll neu in einem automatisierten Abrufverfahren stattfinden. Damit können die Polizeidatenbanken interoperabel ausgestaltet werden, was für eine moderne Schweizer Polizeiarbeit unabdingbar ist.

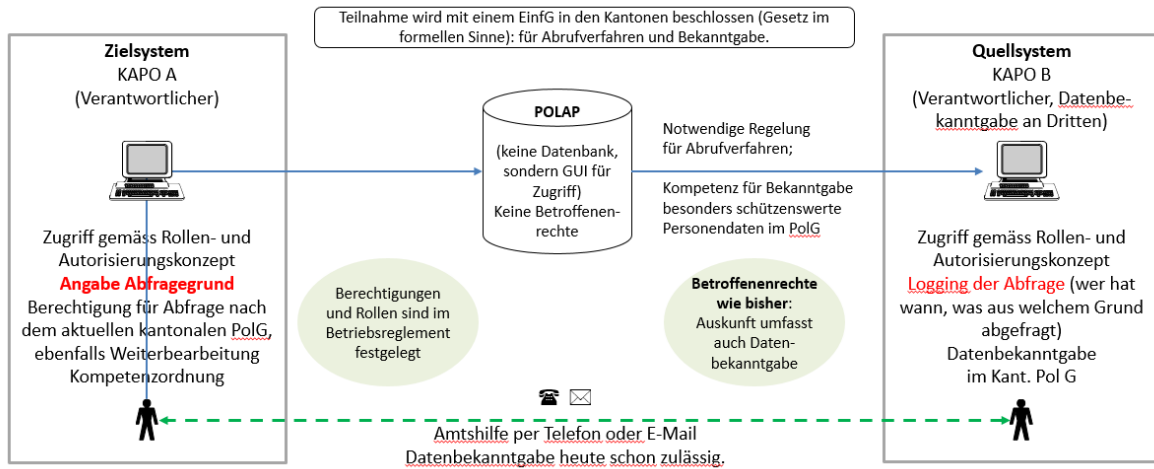
Da diverse kantonale Polizeigesetze bereits Bestimmungen zum Polizeidatenaustausch und Abrufverfahren enthalten, bietet es sich an, die aktuellen Rechtsgrundlagen in den einzelnen Kantonen und die laufenden Revisionen zu analysieren und gegenüberzustellen. Die KKPKS erhofft sich so die Erkenntnis, inwiefern bereits die aktuellen oder in naher Zukunft revidierten Polizeigesetze eine genügende Rechtsgrundlage bieten, damit kantonale Polizeibehörden ihre Quellsysteme an die POLAP anschliessen können und darin enthaltene Daten im Abrufverfahren bekannt geben können.

Fraglich in dieser Hinsicht ist das Verhältnis und die Konsequenz voneinander abweichender Regulierungen in kantonalen Polizeigesetzen und auf Stufe Konkordat. Diese Frage soll gutachterlich durch eine Expertenmeinung aufgearbeitet werden.

Funktionsweise

Die KKPKS betont, dass POLAP keine Vernetzungsplattform ist. Es handelt sich um eine reine Abfrageplattform. Die Informationen können zwecks «Sichtung» aufgerufen werden und POLAP liefert eine standardisierte Ansicht mit den für die zugewiesene Rolle (z.B. gerichts-, sicherheits-, verwaltungspolizeiliche Aufgaben etc.) und des gewählten Kontextes (z.B. Grenzkontrolle Schengen Aussengrenze, Personenkontrolle, Verkehrskontrolle, waffenrechtliche Bewilligung etc.) abrufbaren Daten. Die Daten verbleiben in den Quellsystemen.

Schematisch lässt sich die POLAP Abfrageplattform wie folgt darstellen:



POLAP als Abfrageplattform verfügt selbst über keine Datenhaltung, sondern zeigt nur die bestehenden Daten aus kantonalen Quellsystemen an. Weder werden neue Daten über die betroffenen Personen geschaffen noch werden Daten aus den abgefragten Quellsystemen in POLAP gespeichert. POLAP protokolliert die Abfragen der Benutzer sowie Systemantworten nicht. Die Protokollierung findet in den abgefragten Quellsystemen statt. Die angeschlossenen Quellsysteme prüfen auch, ob die Voraussetzungen einer Abfrage erfüllt sind und gibt erst im Anschluss in einer standardisierten Ansicht die vorhandenen Daten bekannt.

Für die KKKPKS muss sich logischerweise das für ein Quellsystem anwendbare Recht nach der Verantwortlichkeit für das Quellsystem richten. Es ist darum konsequent, die Verantwortlichkeit für die Datenbearbeitung und die Zuständigkeit für die Betroffenenrechte bei den Verantwortlichen der Quellsysteme zu belassen. Auskunftsbegehren und weitere Betroffenenrechte müssen an die Verantwortlichen der Quellsysteme gerichtet werden. Deshalb führt POLAP zu keinem grundlegenden Wechsel in den datenschutzrechtlichen Verantwortlichkeiten.

Polizeiliche Kompetenzen

Aus dem Gesagtem folgert die KKKPKS, dass durch die vorliegende interkantonale Vereinbarung für die POLAP keine neuen polizeilichen Kompetenzen geschaffen werden. Der Zweck der vorliegenden Vereinbarung muss lediglich darin liegen, dass interkantonale Abrufverfahren und Datenbekanntgabe sowie die damit verbundenen datenschutzrechtlichen Fragen (Verantwortung, Aufsicht, Datensicherheit, Akteneinsichtsrecht) in einem übergreifendem Rechtsrahmen zu regulieren, sofern dies nicht bereits durch die kantonalen Polizeigesetze gewährleistet ist.



4. Gemeinsame Datenbanksysteme

Den Kantonen wurde empfohlen, die Kompetenz zur Genehmigung der Betriebsverordnungen an ihre Vertretung in der strategischen Versammlung PTI zu delegieren (Erl. Bericht, S. 15). Dies ist gemäss Art. 6. Abs. 2 PTI-Vereinbarung die kantonale Justiz- und Polizeidirektorin. Eine Rechtsgrundlage gemeinsamer Datenbanksysteme auf Stufe Betriebsverordnung wird von einigen Kantonen als zu tiefe Normstufe betrachtet, um die damit verbundenen Grundrechtseingriffe zu rechtfertigen. Damit hätten das Volk und die Parlamente nach Inkrafttreten des Konkordats auf die Regelungsmaterie wenig bis keinen Einfluss mehr, die aber in vielen Fällen derartige Wichtigkeit aufweise, die eigentlich eine Regelung in einem formellen Gesetz erforderlich mache. Die in Art. 18 aufgeführten Punkte seien gemäss Rückmeldungen zwingend durch den Gesetzgeber und nicht in einer Betriebsverordnung zu regeln. Es reiche darum nicht, ein gemeinsames Datenbanksystem auf einer Betriebsverordnung abzustützen, sondern es sei eine neuerliche interkantonale Vereinbarung für jedes gemeinsame Datenbanksystem abzuschliessen, welche die grundlegenden Punkte in Art. 18 regle.

Die KKPKS vertritt den Standpunkt, dass eine zulässige Gesetzesdelegation an den Verordnungsgeber zulässig ist, sofern sich die Delegation auf eine bestimmte, genau umschriebene Materie beschränkt und dessen Umfang klar begrenzt ist. Die KKPKS versuchte diesen Anforderungen bei der Formulierung der Interkantonalen Vereinbarung gerecht zu werden, so wie sie vom Bundesgericht im Urteil 1C_39/2021 vom 29. November 2022 formuliert wurden. Die zu regelnde Materie – der polizeiliche Datenaustausch – wurde im Entwurf möglichst genau umschrieben. Gleichzeitig wurde aber versucht genügend Raum belassen, um den kantonalen Polizeibehörden die Möglichkeit zu geben, sich neuer Technologien zu bedienen und neue Informationssysteme für weitere polizeiliche Zwecke zu errichten, ohne dabei die Rechtsstaatsprinzipien auszuhöhlen.

Die vielen kritischen Rückmeldung hinsichtlich den Betriebsverordnungen veranlassen die KKPKS dazu, diese vorgesehene Konzeption einer vertieften grund- und datenschutzrechtlichen Analyse zu unterziehen. Gleich an dieser Stelle soll jedoch darauf hingewiesen werden, dass die Betriebsverordnungen als kantonale Erlasse im Sinne von Art. 82 lit. b BGG mit der abstrakten Normenkontrolle anfechtbar sind, wie wenn sie durch die Gesamtregierung jedes Kantons erlassen würden.

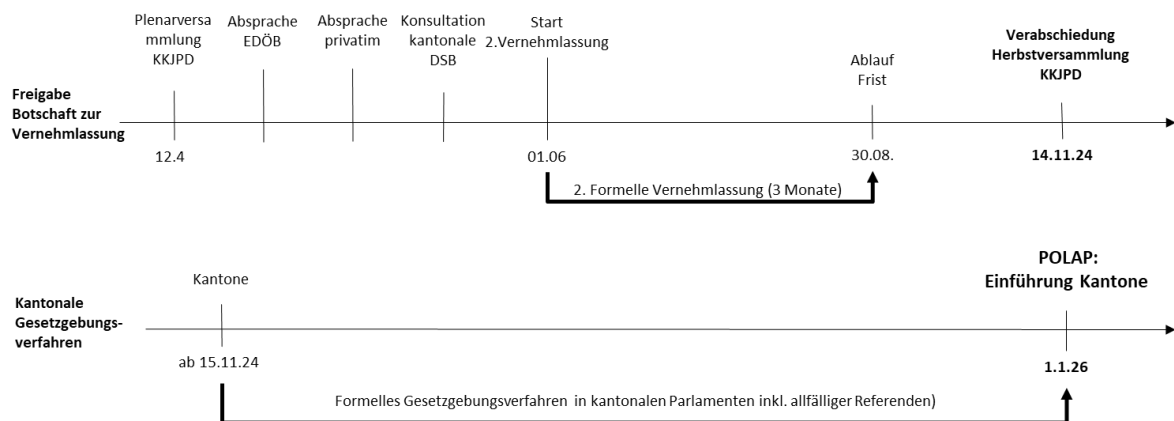
Im breiteren Rahmen werfen die zahlreichen Rückmeldungen zu diesem Thema auch wieder die Frage auf, welche Art von Informationssystemen mit der vorliegenden Vereinbarung errichtet werden sollen und können (siehe sogleich).

5. Weiteres Vorgehen

Die Rückmeldungen werden aufgenommen und der Konkordatstext überarbeitet. Dabei wird weiterhin an einem Konkordat für die Regelung der Abfrageplattform, wie zum Beispiel POLAP und den gemeinsamen Datenbanken festgehalten. Insbesondere werden folgende Punkte angepasst:

- a) Anpassung der Governance Struktur durch die Verantwortung von fedpol als Betreiber von POLAP sowie den dafür neu geschaffenen Rechtsgrundlagen im revidierten BPI.
- b) Überarbeitung der Deliktskataloge (auch in Anlehnung an aktuelle bestehende Deliktskataloge in verschiedenen Bundesgesetzen).
- c) Präzisierung der heute bereits bestehenden Systeme in einem eigenen Absatz (zum Beispiel Überführung ViCLAS und PICAR Konkordate mit analogem Bestimmtheitsgrad).
- d) Abstimmung der datenschutzrechtlichen Anforderungen mit dem EDÖB und Privativim. Einbezug aller kantonalen Datenschutzstellen anlässlich einer Konsultationsveranstaltung.

Die Verabschiedung des Konkordats ist auf die Plenarversammlung der KKJPD am 14. November 2024 vorgesehen, damit danach das Ratifizierungsverfahren in den Kantonen starten kann und der Betriebsstart von POLAP auf Anfang 2026 (gleichzeitig mit der Revision BPI) möglich wird. Der angepasste Zeitplan sieht wie folgt aus:



Um eine breite Abstützung des Vorhabens bei den Kantonen und den interessierten Stellen sicherzustellen, wird nach der Überarbeitung nochmals eine zweite formelle Vernehmlassung durchgeführt.