Interkantonale bzw. interbehördliche Vereinbarung über den Datenaustausch zum Betrieb von Lage- und Analysesystemen im Bereich der seriellen Kriminalität

Erläuternder Bericht

1. Anlass

1.1. Ausgangslage

Für eine effiziente Kriminalitätsbekämpfung müssen die vorhandenen polizeilichen Mittel lagegerecht gesteuert werden können. Im Rahmen der Lageaufbereitung und -analyse besteht ein wachsendes Bedürfnis zum Austausch von Informationen zwischen den Kantonen, da die heutige Täterschaft eine sehr hohe Mobilität aufweist. Dies zeigt sich insbesondere im Bereich der Massenkriminalität mit einem ausgeprägt seriellen Charakter. Das Erkennen von hochaktiven Täterschaften ist ein wichtiger Teil der Bekämpfung dieser seriellen Kriminalität. Nicht minder wichtig sind das frühzeitige Erkennen einer Serie und das Ergreifen präventiver Massnahmen, auch wenn die Täterschaft (noch) nicht bekannt ist. Die Kriminalitätsräume, in denen sich diese Täterschaft bewegt, erstrecken sich dabei weit über die Kantonsgrenzen hinaus.

Da keine Rechtsgrundlage für die Verarbeitung und den Austausch sämtlicher lagerelevanter Daten zwischen den Kantonen besteht, sind die Polizeikorps im PKNW[1] - und in den meisten anderen Polizeikonkordaten - beim Monitoring und der Analyse der seriellen Kriminalität auf das eigene Kantonsgebiet beschränkt. Sie erhalten somit nur ein unvollständiges Bild der aktuellen Lage. Der Erkenntnisaustausch zwischen den Konkordatspartnern erfolgt auf konventionellem Weg[2], was langsam, ineffizient, vergangenheitszentriert, unvollständig, ressourcenintensiv sowie aus technologischer Sicht nicht mehr zeitgemäss ist.

Eine vertiefte Analyse mit dem Ziel, hochaktive Täter und Serien zu erkennen und die Grundlage für eine wirkungsvolle Bekämpfung zu schaffen, ist gegenwärtig nicht möglich. Dazu müssten die Konkordatspartner über gemeinsame Analysetools verfügen, welche den Datenaustausch im Abrufverfahren ermöglichen. Mitarbeitende der Lage- und Analysestellen der Polizei müssen so stark wie möglich durch automatisierbare Arbeitsschritte entlastet werden können, damit mehr Zeit für die eigentliche Analysetätigkeit bleibt.

Erlangte Erkenntnisse müssen in verschiedenen, dem Zielpublikum angepassten Formen (Berichte, interaktive Karten, graphische Darstellung von personellen/materiellen Zusammenhängen, etc.) bereitgestellt werden können, sei dies in Form von objektiven

[1] Konkordat über die polizeiliche Zusammenarbeit in der Nordwestschweiz vom 20.01.1995.
[2] Wöchentlicher Rapport im Regionalen Lagezentrum und Einzelfall-Informationsaustausch per Email und/oder Telefon.

Entscheidungsgrundlagen zur Planung von Massnahmen, als Ermittlungsansätze oder in Form von konkreten Informationen und Empfehlungen.

Obwohl solche Analysetools in einzelnen Kantonen durchaus erfolgreich angewendet werden, wird das volle Potential erst ausgeschöpft werden können, wenn diese Datenbanken vereinigt und interkantonal betrieben werden. Erst dann erhält man ein vollständiges Bild der Lage im Bereich der kantonsübergreifenden, seriellen Kriminalität und erkennt Tendenzen und Zusammenhänge, die zuvor nicht ersichtlich waren. Zusätzlich müssten Daten, die heute von Drittparteien geliefert werden und in jedem Kanton separat in die Analyse einfliessen (z.B. „Verbreitungen National" durch andere Polizeikorps), nur noch einmal erfasst werden, was wiederum mehr Zeit für die eigentliche Analysetätigkeit lässt.

Gemeinsame Datenbanken, welche das Bewirtschaften von interkantonalen Kriminalitätsräumen ermöglichen, existieren zurzeit noch nicht. Nur diese würden jedoch das Erstellen von Prognosen für regionale Kriminalitätsräume ermöglichen. Somit könnte die Bewirtschaftung von regionalen Brennpunkten koordiniert erfolgen, was zweifellos auch einen positiven Einfluss auf die Ressourcen hätte.

1.2. Tools

Die Entwicklung von Polizeiapplikationen hat sich in den vergangenen Jahren vervielfacht. Dieser Trend dürfte sich fortsetzen. Die vorliegende Vereinbarung nimmt darauf Rücksicht, indem sie nicht eine bestimmte Applikation vorsieht, sondern so abgefasst ist, dass mehrere bestehende und zukünftig zu entwickelnde Applikationen darunterfallen können. Somit wird die Gefahr, dass die gesetzliche Grundlage der technischen Entwicklung dauernd hinterherläuft, gemindert. Daten, welche erfasst werden dürfen, werden genau bezeichnet, um der Datenschutzgesetzgebung Rechnung zu tragen. Die Art der Verknüpfung und somit die Detailprozesse der Applikationen werden dagegen bewusst offengelassen. Deren Regelung erfolgt im jeweiligen Betriebsreglement.

Zwei Analysetools haben in den vergangenen Jahren eine grössere Verbreitung erlangt:

1.2.1. PICAR[3]

PICAR wird im CICOP[4] seit 2008 als gemeinsame Analyseplattform verwendet. Es handelt sich dabei um eine ereignisorientierte Datenbank, welche im Bereich der Kriminalanalyse Anwendung findet. Der Fokus dieses Analysetools ist auf die serielle Kriminalität im Bereich der Vermögens- (Einbruchdiebstahl, Ladendiebstahl, Trickdiebstahl, etc.), Gewalt- und Sexualdelikte ausgerichtet. Durch das zentrale Erfassen und Analysieren von Fällen und

[3] Plateforme d'Information du CICOP pour l'Analyse et le Renseignement.
[4] Concept Intercantonal de Coordination Opérationelle et Préventive, Polizeikonkordat der Westschweizer und des Tessiner Polizeikorps.

Fallzusammenhängen[5] können Serien und Tendenzen schnell, systematisch und zentralisiert erkannt werden. Dazu gehören das zeitnahe Darstellen und Analysieren der seriellen Kriminalität, das Koordinieren von erkannten Serien oder auch das Abgleichen von Bildern unbekannter Täterschaft.

Dank der Administration und Weiterentwicklung durch polizeiinterne Mitarbeitende[6] wird PICAR permanent und in hohem Ausmass an die Bedürfnisse der teilnehmenden Polizeikorps angepasst.

Im PKNW betreiben die Polizei Basel-Landschaft und die Kantonspolizei Aargau PICAR seit 2014/2015 in separaten, kantonalen Datenbanken. Diese werden mit Informationen aus anderen polizeilichen Systemen (z.B. Journal, ABI, Vulpus), die jeder/jedem Polizistin/Polizisten im Kanton zugänglich sind, gespeist. Erst der Zusammenzug dieser Informationen in einer gemeinsamen Datenbank wird jedoch zu einer für beide Kantone gültigen Lagedarstellung führen.

1.2.2. PRECOBS

PRECOBS[7] ist eine Software, welche vom Oberhausener Institut für musterbasierte Prognosetechnik[8] entwickelt wurde.

PRECOBS arbeitet auf Basis des sogenannten „Near-Repeat-Phänomens"[9]. Anhand von polizeilichen Daten wie Örtlichkeit, Modus Operandi, Tatwerkzeug, Deliktsgut und empirischen Erkenntnissen aus der Vergangenheit wird untersucht, wo es zu zeitlichen und räumlichen Deliktskonzentrationen kam. Es wird davon ausgegangen, dass dort die Wahrscheinlichkeit für das Vorkommen von solchen Deliktskonzentrationen auch in Zukunft am höchsten ist. Daher werden in diesen Gebieten Prognoseräume definiert. Ereignet sich nun ein Delikt in einem Prognoseraum, ist die Wahrscheinlichkeit, dass sich im besagten Prognoseraum in den folgenden sieben Tagen weitere Delikte ereignen, erhöht. Somit können präventive und repressive Massnahmen gezielt und ressourcenschonend eingesetzt werden.

Als erstes Polizeikorps führte 2014 die Stadtpolizei Zürich PRECOBS ein. Ende 2014 wurde das System auch in der Polizei Basel-Landschaft und kurz darauf in der Kantonspolizei Aargau eingeführt.

2. Vorgehen

---

[5] Situative und auf materiellen Spuren basierende Fallzusammenhänge. Es werden lediglich die Zusammenhänge, jedoch nicht die Spuren an sich, erfasst.
[6] In der Regel mit wissenschaftlichem Hintergrund (Master an der Universität Lausanne).
[7] Pre Crime Observation System.
[8] IfmPt; vgl. auch: https://www.ifmpt.de/
[9] Vgl. z.B. GLUBA, ALEXANDER: Predictive Policing – eine Bestandsaufnahme. Historie, theoretische Grundlagen, Anwendungsgebiete und Wirkung. – Hannover: LKA Niedersachsen, 2014. S. 3.

2.1. Auftrag

Die Konkordatsbehörde des PKNW beschloss am 9.12.2016, eine Arbeitsgruppe aus den Konkordatskantonen unter der Führung der Polizei Basel-Landschaft einzusetzen. Unter Einbezug der Vereinigung der schweizerischen Datenschutzbeauftragten sei zu prüfen, ob das bestehende Konkordat erweitert werden könne. Ziel wäre der mögliche gemeinsame Betrieb von Einsatzleit-, Lage- und Analysesystemen und der automatische Austausch der dazu benötigten Daten. Insbesondere sei zu prüfen, ob das bestehende Konkordat oder die kantonalen Polizeigesetze oder gegebenenfalls beide Regelungen anzupassen seien.

2.2. Arbeitsgruppe

Die Arbeitsgruppe setzte sich aus Vertreterinnen und Vertretern der Datenschutzstellen der Kantone Aargau (teilweise), Basel-Stadt, Basel-Landschaft, Bern und Solothurn, der Rechtsdienste der Kantonspolizeien Basel-Stadt, Bern und Solothurn, einem Betreiber von PICAR (Kantonspolizei Aargau) und den Chefs Kriminalpolizei der Kantone Basel-Stadt und Basel-Landschaft zusammen.

2.3. Zwischenberichte und Entscheide

Anlässlich der Behördensitzung vom 9.06.2017 wurde entschieden, auf eine Ausweitung des existierenden Polizeikonkordates zu verzichten und keine gesetzliche Grundlage für interkantonale Lage- und Analysesysteme gestützt auf (unterschiedliche) kantonale Polizeigesetze anzustreben. Stattdessen sollte eine gesetzliche Grundlage in Form einer neuen, eigenständigen, interkantonalen Vereinbarung entwickelt werden. In einer ersten Phase sollte angestrebt werden, die Vereinbarung zwischen den Kantonen der Nordwestschweiz abzuschliessen. Der Beitritt weiterer Kantone wäre aber grundsätzlich möglich. Ausserdem sollte angestrebt werden, das GWK, welches bereits heute als wichtiger Informationslieferant eingebunden ist, als Vereinbarungspartner zu gewinnen.

2.4. Vernehmlassung

Mit Schreiben vom 18. Dezember 2018 wurden die Regierungen der Kantone des PKNW eingeladen, zur Vereinbarung Stellung zu nehmen. Sämtliche Regierungen nahmen diese Gelegenheit wahr. Änderungsanträge konnten zum grössten Teil berücksichtigt werden. War dies in Einzelfällen nicht der Fall, wird in diesem Bericht besonders darauf hingewiesen.

3. Inhalt, Konzeption und Struktur der Vereinbarung

3.1. Grundsatz

Im Rahmen der vorliegenden interkantonalen Vereinbarung werden Lage- und Analysesysteme betrieben, die besonders schützenswerte Personendaten enthalten können (vgl. Artikel 8). Dazu ist ein Beschluss der zuständigen Legislative erforderlich.

Die Vereinbarung nennt die zur Aufgabenerfüllung nötigen Organe und definiert deren Zusammensetzung und Aufgaben. Ausserdem enthält sie die Grundzüge der für alle Applikationen gültigen Modalitäten und finanziellen Folgen eines Austritts aus dem gemeinsamen Betrieb der jeweiligen Applikation und der Haftung im Innenverhältnis.

Geregelt werden insbesondere:

- Zweck der Datenbank bzw. der Datenbearbeitung
- Inhalt der Datenbank, Datenkategorien
- Regeln zum Datenaustausch
- Zugriffsberechtigungen
- Aufbewahrungsdauer, Archivierung und Löschung der Daten
- Auskunftsrecht / Rechtsschutz
- Grundlegende organisatorische Fragen
- Grundprinzipien der Finanzierung

Die Vereinbarung schafft die nötige Rechtsgrundlage für den recht- und verhältnismässigen Betrieb von verschiedenen interkantonalen Lage- und Analysesystemen. Gegenwärtig stehen die Produkte PICAR und PRECOBS im Vordergrund. Es ist jedoch denkbar, dass - insbesondere im Rahmen der technologischen Weiterentwicklung - neue Softwareprodukte auf den Markt kommen, die den gleichen Zweck verfolgen, aber eine andere Architektur aufweisen. Die gesetzliche Grundlage ist bewusst so formuliert, dass solche Produkte - immer im Rahmen des Zwecks dieser Vereinbarung - damit ebenfalls über eine Rechtsgrundlage verfügen.

3.2. Zweistufigkeit der Vereinbarung

Entsprechend dem Ziel, unter Wahrung der Kompetenzen des kantonalen Gesetzgebers eine rechtsgenügende Grundlage für den Datenaustausch zu schaffen, die übersichtlich bleibt, wurde eine zweistufige Struktur der Vereinbarung gewählt:

3.2.1 Strategische Ebene / Vereinbarungsebene

Der Beitritt zur Vereinbarung an sich verpflichtet die Vereinbarungspartner nicht, eine einzelne Applikation gemeinsam zu betreiben. Mit dem Beitritt zur Vereinbarung wird der Kanton bzw. die geeignete Bundesstelle lediglich zu einem Vereinbarungspartner, welchem es fortan offensteht, sich am gemeinsamen Betrieb einer einzelnen Datenbank zu beteiligen oder davon abzusehen (vgl. Artikel 2 Absatz 1 Satz 2). Dieser Entscheid ist für jede einzelne Datenbank unter Abwägung der eigenen Bedürfnisse und des zu erwartenden Nutzens von der jeweils zuständigen Behörde zu treffen.

3.2.2 Operative Ebene / Datenbankebene

Innerhalb des Rahmens dieser Vereinbarung werden unterschiedliche Datenbanken in unterschiedlicher Zusammensetzung betrieben werden können.

Erst nach erfolgter Genehmigung des Betriebsreglements einer konkreten Datenbank wird der jeweilige Kanton bzw. die jeweilige Bundesstelle zum Teilnehmer an der entsprechenden Datenbank[10]. Die jeweiligen konkreten Regelungen, für welche sich im Detail je nach Applikation eine unterschiedliche Regelung sinnvoll erweisen kann, sind im jeweiligen Betriebsreglement genau festzulegen. Erst mit Genehmigung des Betriebsreglements wird der Vereinbarungspartner auch zum Teilnehmer an der Datenbank mit den entsprechenden Rechten und Pflichten. Er entscheidet somit über jeden Beitritt in Kenntnis aller Auswirkungen.

Jede dieser Datenbanken wird der Vorabkontrolle der zuständigen Datenschutzstelle unterliegen, wofür das Betriebsreglement bzw. ein ISDS-Konzept vorliegen müssen.

Im Falle von PICAR sind die Projektarbeiten schon relativ weit gediehen. Es ist angedacht, dass die Polizei Basel-Landschaft die Zentralstelle[11] betreibt, während sich die Kantonspolizei Aargau als Aussenstelle konfiguriert. Weitere Kantonspolizeien haben bereits signalisiert, der Vereinbarung beizutreten, sobald diese gesetzliche Grundlage in Kraft ist.

3.3. Organe

Neben der gesetzlichen Grundlage an sich bedarf die Umsetzung der Vereinbarung einer gewissen organisatorischen Struktur (vgl. Artikel 3 bis 5)[12].

3.3.1. Interkantonales Aufsichtsorgan

Ein interkantonales Aufsichtsorgan übt die Aufsicht über die Vereinbarung aus (vgl. Artikel 3). Da in verschiedenen Kantonen das kantonale Recht ausserdem eine periodische Berichterstattung über Vereinbarungen der vorliegenden Art verlangt, wird diese Aufgabe dem Aufsichtsorgan zugewiesen.

Das Aufsichtsorgan setzt sich aus Vertreterinnen bzw. Vertretern der Kantonsregierungen bzw. der politischen Verantwortlichen der entsprechenden Bundesstellen zusammen. Die Ernennung dieser Personen erfolgt entsprechend dem anwendbaren kantonalen bzw. Bundesrecht.

---

[10] Begrifflich wird deshalb durchgehend zwischen „Vereinbarungspartner" und „Teilnehmer" unterschieden. Auseinanderzuhalten sind demnach Kantone oder Bundesstellen, die mit ihrem Beitritt keinerlei Verpflichtung eingehen, sondern sich damit vorerst einzig die Option sichern, zu einem späteren Zeitpunkt an einer tauglichen gemeinsam betriebenen Datenbank zum Zweck und nach den von der Vereinbarung festgelegten Grundsätzen allenfalls teilzunehmen und Kantone oder Bundesstellen, welche von dieser Option auch tatsächlich Gebrauch machen.

[11] Vgl. Ziff. 3.3.3.

[12] In dieser Hinsicht waren sich die an der Vernehmlassung beteiligten Kantone nicht einig. Mehrere Kantone hätten eine schlankere Struktur der Organe bevorzugt. Da aber das Fehlen eines Aufsichtsorgans für mehrere Kantone ein „Killerkriterium" gewesen wäre, wurde die vorliegende Struktur gewählt. Damit wird dem Bestreben, die Teilnahme an der Vereinbarung für alle Kantone zu ermöglichen, Rechnung getragen.

3.3.2. Lenkungsausschuss

Ein Lenkungsausschuss nimmt die strategische Führung und Umsetzung dieser Vereinbarung und die Streitbeilegung wahr (vgl. Artikel 4), wobei es sich dabei ausschliesslich um rechtsgeschäftliche[13] Tätigkeiten handelt.

Obwohl der Lenkungsausschuss sich selbst konstituieren wird, ist zu erwarten, dass in diesem Organ die Stufe Polizeikommandantin/Polizeikommandant oder Chefin/Chef Kriminalpolizei bzw. Kriminalabteilung vertreten sein werden.

3.3.3. Zentralstelle und Aussenstellen

Eine Zentralstelle wird zusammen mit Aussenstellen für den operativen Betrieb der Datenbanken zuständig sein (vgl. Artikel 5), wobei die Vereinbarung die allgemeinen organisatorischen und für alle Datenbanken gleichermassen geltenden Grundsätze festlegt. Die technischen, organisatorischen und finanziellen Details bzw. die Funktionsweise werden - immer innerhalb des Rahmens dieser Vereinbarung - in einem Betriebsreglement für jede einzelne Datenbank geregelt.

Aus Ressourcengründen ist nicht davon auszugehen, dass stets dasselbe Polizeikorps bereit bzw. dazu in der Lage ist, die mit der Zentralstelle verbundenen Aufgaben der Federführung des Betriebs zu übernehmen.

3.4. Übergeordnetes Recht

In Lage- und Analysedatenbanken finden sich unter anderem Daten, die aufgrund der Vorschriften der StPO[14] erhoben wurden.

Hängige Strafverfahren sind gemäss Artikel 2 Absatz 2 Buchstabe c DSG[15] aus dem Anwendungsbereich des allgemeinen Datenschutzrechtes ausgenommen. Die StPO enthält in den Artikeln 95 bis 99 eigene Grundsätze für die Datenbearbeitung. Artikel 96 Absatz 1 StPO lässt dabei eine „systematische Vernetzung verschiedener Fälle"[16] ausdrücklich zu. Die Artikel 95 bis 99 sind somit lex specialis während der Hängigkeit eines Strafverfahrens im engeren Sinn und keine abschliessende Regelung für die Bearbeitung von Daten, die zwar im Rahmen eines Strafverfahrens erhoben wurden, danach aber bis zu ihrer gesetzmässigen Löschung in den entsprechenden Datenbanken bestehen bleiben. Für diese kommen

[13] Der Erlass rechtsetzender Bestimmungen ist ausgeschlossen. Sollte der Betrieb einer (heute noch nicht bekannten) Applikation rechtsetzende Bestimmungen erforderlich machen, wäre die Vereinbarung im ordentlichen Gesetzgebungsverfahren entsprechend zu ergänzen.
[14] Schweizerische Strafprozessordnung, SR 312.0
[15] Bundesgesetz über den Datenschutz vom 19.6.1991 (SR 235.1).
[16] NIGGLI, MARCEL ALEXANDER / HERR MARIANNE / WIPRÄCHTIGER HANS (Hrsg.): Schweizerische Strafprozessordnung / Jugendstrafprozessordnung, 2. Aufl., Basel 2014, nachfolgend: BSK-StPO, GERHARD FIOLKA , Art. 96 N 1.

grundsätzlich die allgemeinen Datenschutzregeln des Bundes und der Kantone zur Anwendung[17].

4. Bestimmungen im Einzelnen

Titel

Auf die Bezeichnung „Konkordat" wird verzichtet, da ein Konkordat in der Regel nur zwischen Kantonen abgeschlossen wird, während der vorliegenden Vereinbarung auch „geeignete Bundesstellen" (Artikel 17) - gedacht wird an das Grenzwachtkorps als wichtiger Datenlieferant – beitreten können[18]. Da der Begriff „interkantonal" somit sprachlich unpräzis ist, wird von „interkantonal bzw. interbehördlich" gesprochen[19].

Ingress

Der Hinweis auf Artikel 56 BV erfolgt, da es denkbar - wenn auch gegenwärtig nicht geplant - ist, dass die deutsche Bundespolizei, die Landespolizei Baden-Württemberg, die französische Police Nationale oder Gendarmerie der Vereinbarung beitreten[20]. Mit diesen Organisationen besteht in der grenzüberschreitenden Kriminalitätsbekämpfung ein reger Informationsaustausch in traditionellem Rahmen. Da der Vereinbarung in der gegenwärtigen Fassung jedoch nur „Kantone oder geeignete Bundesstellen"[21] beitreten können, müsste dereinst die Vereinbarung im ordentlichen Gesetzgebungsverfahren angepasst werden. Im Rahmen der vorliegenden Vereinbarung werden diese Behörden lediglich als indirekte Informationslieferanten genutzt, ohne ihnen Zugriff auf die Datenbanken zu erlauben[22].

Artikel 1

Wichtigste Aufgabe der Polizei ist es, Straftaten zu verhindern, weshalb Serien zu erkennen und möglichst rasch zu stoppen sind. Ausserdem tragen die dadurch gewonnenen Informationen und Erkenntnisse dazu bei, die Täterschaft möglichst zu identifizieren und zur Rechenschaft zu ziehen.

Seriendelikte sind Straftaten, die wiederholt und/oder durch die gleiche Täterschaft verübt werden. Allerdings beginnt jede Serie zunächst mit einer ersten Straftat. Demzufolge muss insbesondere bei Delikten, die typischerweise in Serie verübt werden, auch bereits die Erfassung einer einzelnen, möglicherweise ersten Straftat zulässig sein.

---

[17] BSK-StPO-GERHARD FIOLKA, a.a.O., Vorbemerkungen zu Art. 95-99 N 3.
[18] Vgl. auch die Erläuterungen zu Art. 17.
[19] Vgl. Titel, Ingress und Art. 1 Abs. 1.
[20] Vgl. auch die Erläuterungen zu Art. 19.
[21] Art. 17 Abs. 1.
[22] Analog z.B. zu den kommunalen Polizeibehörden, deren Daten – wenn überhaupt – via die Kantonspolizeien in die Datenbanken gelangen.

Eine wissenschaftliche Definition der Seriendelikte fehlt. In der Praxis sind im Bereich der Vermögensdelikte (namentlich Einbruch- und Einschleichdiebstähle, Taschen-, Trick-, Entreiss-, Laden- und einfache Diebstähle, Aufbrüche von Automaten, Falschgeld, Fahrzeugdiebstähle und –aufbrüche, Kontrollschilderdiebstähle, Missbräuche von Datenverarbeitungsanlagen, Raubüberfälle, Sachbeschädigungen, Brände/Explosionen) anzahlmässig die grössten Serien feststellbar. Serien kommen aber auch im Bereich der Sexualdelikte (im nicht familiären/nicht bekannten Umfeld) und Gewaltdelikte (z.B. Tötungsdelikte) vor. Nicht zu den Seriendelikten gezählt werden in der Praxis insbesondere Verstösse gegen das Betäubungsmittelgesetz und Sexualdelikte, die im familiären Umfeld oder im näheren Bekanntenkreis begangen werden.

In Ermangelung einer wissenschaftlichen Definition der seriellen Kriminalität wird im Titel der Vereinbarung und in Artikel 1 Absatz 1 und Absatz 2 speziell erwähnt bzw. darauf hingewiesen, dass sich die Bestimmungen dieser Vereinbarung auf die serielle Kriminalität beschränken.

Datenbanken der vorliegenden Art enthalten sowohl ungesicherte, als auch gesicherte Daten. Typische Lagebilder weisen einen mehr oder minder grossen Anteil ungesicherter Informationen auf, welche demzufolge in einem Strafverfahren noch nicht verwendet werden können. Regelmässig kommt es im Laufe eines Strafverfahrens zu weiteren Erkenntnissen, welche zunächst ungesicherte Daten wahrscheinlicher erscheinen lassen und/oder bestätigen. Dann handelt es sich um gesicherte Daten, deren Verwertung nach StPO gegebenenfalls zulässig ist. Umgekehrt können sich ungesicherte Daten im Laufe eines Verfahrens auch als falsch erweisen. Diese Erkenntnis im Nachhinein macht die anfängliche Datenbearbeitung nicht unrechtmässig, kann jedoch eine Berichtigung und/oder Löschung zur Folge haben[23].

Artikel 2

Artikel 2 schreibt die Zweistufigkeit[24] fest, welche als zukunftsweisende Grundlage für den Datenaustausch und die Zusammenarbeit der Vereinbarungspartner dient. Es werden nicht Regelungen zu einzelnen Datenbanken erstellt, sondern Rahmenbedingungen geschaffen, welche als Grundlage für eine Vielzahl von Teilnehmern und Datenbanken dienen können. Die gewählte Struktur ermöglicht es einem Vereinbarungspartner, der Vereinbarung beizutreten, ohne gleichzeitig an allen Datenbanken partizipieren zu müssen. Entsprechend wurde eine zweistufige Struktur geschaffen, welche auf übergeordneter Ebene (Vereinbarung) die Grundlagen des Austausches und auf untergeordneter Ebene den konkreten Betrieb der Datenbank (Betriebsreglement) vorsieht.

[23] Vgl. Art. 12 und 13.
[24] Vgl. Ziff. 3.2.

Artikel 2 Absatz 1 ist als zentrale Bestimmung zu verstehen, welche die vorstehend genannten Überlegungen zur Zweistufigkeit verbindlich festhält. Durch die Formulierung "Für jede gemeinsame Datenbank (...) wird ein separates Betriebsreglement geschaffen" wird einerseits festgelegt, dass eine Vielzahl von Datenbanken unter der vorliegenden Vereinbarung betrieben werden kann, jede einzelne dieser Datenbanken andererseits aber über ein den übergeordneten Vorgaben entsprechendes Betriebsreglement verfügen muss. Letzteres bedeutet konkret, dass die gesamten technischen, organisatorischen und finanziellen Belange abschliessend und explizit im Betriebsreglement festgelegt werden müssen.

Durch Artikel 2 Absatz 1 Satz 2 wird schliesslich festgehalten, dass ein Beitritt zur Vereinbarung nicht gleichzeitig auch ein Beitritt zu allen unter dieser betriebenen Datenbanken bedeutet. Vielmehr wird den Vereinbarungspartnern dadurch die Möglichkeit eröffnet, nur jenen Datenbanken beizutreten, welche sie als sinnvoll erachten.

Artikel 3

Für mehrere Kantone ist es aufgrund ihres kantonalen Rechts zwingend, eine Aufsicht über die Einhaltung der Vereinbarung vorzusehen. Der Lenkungsausschuss (vgl. Artikel 4) muss somit einem übergeordneten Organ rechenschaftspflichtig sein.

Die Vereinbarung sieht deshalb ein interkantonales Aufsichtsorgan vor, das sich aus den politisch Verantwortlichen der Vereinbarungspartner zusammensetzt. Die Vereinbarungspartner sind dabei im Rahmen ihres jeweiligen Rechtes frei, welche Personen sie in dieses Organ delegieren.

Auf Regelungen zur Organisation und zur Periodizität der Berichterstattung wurde verzichtet, da dies von den Vereinbarungspartnern und ihrer jeweiligen Gesetzgebung abhängt. Erste Aufgabe des interkantonalen Aufsichtsorgans wird es deshalb sein, sich zweckmässig zu konstituieren und zu organisieren.

Artikel 4

Der Lenkungsausschuss[25] konstituiert sich selber und setzt sich aus je einer Vertreterin bzw. einem Vertreter der Vereinbarungspartner zusammen. Es obliegt den Vereinbarungspartnern festzuhalten, wer ihre Interessen im Lenkungsausschuss vertreten soll. Sinnvollerweise sollte hierbei eine Person berücksichtigt werden, welche über gute Kenntnisse der Materie und der Polizeilandschaft besitzt. Es ist zu erwarten, dass die Stufe Polizeikommandantin/Polizeikommandant oder Chefin/Chef Kriminalpolizei bzw. Kriminalabteilung im Lenkungsausschuss vertreten sein werden.

[25] Vgl. Ziff. 3.3.2

Der Lenkungsausschuss hat verschiedene Aufgaben, welche nicht abschliessend aufgeführt sind. Einerseits zeichnet er für die strategische Führung und Umsetzung der Vereinbarung verantwortlich. Dies umfasst insbesondere den grundlegenden Entscheid, welche Datenbanken unter der Vereinbarung betrieben werden sollen. Weiter nimmt der Lenkungsausschuss Beitrittsgesuche und Kündigungen zur Vereinbarung[26] entgegen und sorgt für die Streitbeilegung[27]. Zur Streitbeilegung kann er in besonderen Fällen, welche über die Anwendung und Auslegung der Vereinbarung hinausgehen, ein unabhängiges Schiedsgericht einsetzen. Gegen den Entscheid des Schiedsgerichts ist die Klageerhebung beim Bundesgericht möglich (Artikel 189 Absatz 2 Schweizerische Bundesverfassung[28]).

Als zentrale Aufgabe erlässt der Lenkungsausschuss das Betriebsreglement einer Datenbank[29]. In dieser Funktion sorgt er für die gleichmässige Einhaltung und Anwendung der Bestimmungen der Vereinbarung[30]. Die Kostenverteilung einer Datenbank wird allerdings ausschliesslich unter den Teilnehmern geregelt. Der Lenkungsausschuss stellt lediglich sicher, dass der Verteilschlüssel mit Artikel 14 in Einklang steht.

Artikel 5

Obliegen die strategischen Entscheide dem Lenkungsausschuss, ist die Zentralstelle in Zusammenarbeit mit den Aussenstellen für die operative Umsetzung der Vereinbarung auf Stufe Datenbank verantwortlich. Die Zentralstelle agiert ebenfalls als Vertreterin gegenüber Dritten und schliesst, sofern nötig, Lizenzverträge (inkl. Service und Support) ab. Insbesondere obliegt der Zentralstelle der Betrieb der Datenbank, was die Einhaltung der übergeordneten Vorgaben und die Umsetzung der vorliegenden Vereinbarung und des Betriebsreglements beinhaltet.

Die Zentralstelle kann von Aussenstellen unterstützt werden. Wie sich die konkrete Organisation und die Aufgabenteilung darstellt, ist im Betriebsreglement festzuhalten. Die Zentral- wie die Aussenstellen haben sich im Hinblick auf die Bearbeitung der Daten an die einschlägigen gesetzlichen Vorgaben zu halten.

Absatz 4 hält schliesslich die Meldepflicht der Teilnehmer fest. Damit eine genügende Kontrolle betreffend Datenbearbeitung und Nachvollziehbarkeit erreicht werden kann, muss bekannt sein, welche Mitarbeitenden in der Zentral- wie in den Aussenstellen zur Bearbeitung von Daten zugelassen sind.

---

[26] Vgl. Art. 17.
[27] Vgl. Art. 20.
[28] SR 101.
[29] In der Praxis wird der Lenkungsausschuss die detaillierte Ausarbeitung des Betriebsreglements der Zentralstelle der betreffenden Datenbank in Auftrag geben, falls nicht der Vorschlag dazu direkt aus einem Polizeikorps erfolgt.
[30] Der Erlass rechtssetzender Bestimmungen ist ausgeschlossen (vgl. Fn 13).

Artikel 6

Selbstverständlich sind Polizeikommandantinnen und Polizeikommandanten für den Datenschutz und die Datensicherheit in ihrem Betrieb verantwortlich, unabhängig davon, ob sie diese Daten selbst erfassen oder von extern geliefert erhalten. Damit sie diese Verantwortung jedoch wahrnehmen können, sind sie darauf angewiesen, dass die Datenlieferanten („Aussenstellen") ihre Verantwortung ebenfalls wahrnehmen und zur Meldung verpflichtet werden, wenn ihre Daten nicht mehr rechtmässig verwendet werden können oder nicht mehr richtig sind[31].

Artikel 7

Das Betriebsreglement bildet das zentrale Regelwerk auf Stufe der Datenbank. Erst mit der Genehmigung des Betriebsreglements wird ein Vereinbarungspartner zum Teilnehmer an einer Datenbank mit den entsprechenden Rechten und Pflichten.

Die Abschlusskompetenz richtet sich nach dem Recht der Teilnehmer. Es liegt somit in der Verantwortung der Teilnehmer, vor der Genehmigung des Betriebsreglements allfällig notwendige Genehmigungen bzw. Delegationen einzuholen.

Absatz 2 Buchstabe g: Die Lösch*fristen* sind in den Artikeln 13 und 16 geregelt. Im Betriebsreglement sind die entsprechenden, detaillierten Modalitäten bzw. Prozesse der Datenlöschung zu definieren.

Artikel 8

Absatz 1: Inhalt der Datenbanken sind polizeiliche Daten. Dabei wird auf einen funktionalen Begriff abgestellt. Entscheidend ist, dass die Daten zu polizeilichen Zwecken erhoben sind und nicht, dass sie formell von einer Polizei erfasst werden. Die Bestimmung ist so ausgelegt, dass z.B. auch Daten kommunaler Polizeien erfasst werden können. Andererseits soll insbesondere das GWK, das formell keine Polizei ist, Partner werden und seine Daten in die Datenbanken liefern können. Nicht-polizeiliche Daten, z.B. Daten von Nachrichtendiensten im In- und Ausland, sind dagegen ausgeschlossen.

Absatz 2: Die Eckdaten eines Ereignisses sind in der Regel klar und relativ schnell gesichert vorhanden. Häufig sind zur Täterschaft und zu Zusammenhängen nur Bruchstücke bekannt. Die Auflistung der einzelnen Daten stellt sicher, dass diese Bruchstücke gesammelt werden dürfen und zu gegebener Zeit im Sinne eines Puzzles zusammengefügt werden können.

Absatz 2 Buchstabe b: Unter Tatmittel sind im Fall von sog. Cybercrime-Delikten insbesondere auch Hardware, Software und Malware zu verstehen.

[31] Vgl. auch die Erläuterungen zu Art. 10 und 16.

Absatz 2 Buchstabe c: Die Täterschaft steht im Zentrum des Interesses. Bruchstückhafte Informationen müssen zusammengefügt werden können. Neben den üblichen Personalien können auch Identifikationsnummern von Ausweisen, Pass- und Personalnummern erfasst werden. Diese bleiben jeweils unverändert, während Namen in zahlreichen Ländern völlig legal geändert werden können. Neben klassischen Wohnadressen werden elektronische Adressen wie IP-Adressen, URI[32], E-Mail-Adressen, Namensbezeichnungen in sozialen Medien oder Zugangsdaten (inkl. biometrische Daten) zur Identifikation immer wichtiger. Unter biometrischen Zugangsdaten werden dabei Augen, Ohren, Fingerabdrücke, Gesichtserkennungsdaten und die Weiterentwicklung dieser Technologien verstanden.

Absatz 2 Buchstabe d: Angaben zu Geschädigten sind auf die aufgeführten Informationen beschränkt. Weitergehende kantonale oder Bundesdaten dürfen gestützt auf diese Vereinbarung nicht verknüpft werden.

Absatz 2 Buchstabe h: Unter Ereignisbildern werden auch Radarfotos, Bilder von speziellen Tatwerkzeugen, Symbolbilder, Bilder von Deliktsgut und Phantombilder verstanden.

Absatz 2 Buchstabe j: Das DNA-Profil selbst ist für eine Ereignisverbindung nicht von Bedeutung. Ereignisse müssen jedoch anhand von Prozesskontrollnummern, die in anonymisierter Form auf das in den Systemen gespeicherte DNA-Profil verweisen, verbunden werden können.

Absatz 2 Buchstabe k: Darunter können gegenwärtig IBAN, Bitcoin-Adressen, Seeds, Wallets etc. verstanden werden. Auf eine Aufzählung dieser Bezeichnungen wird jedoch bewusst verzichtet, da die detaillierte, exakte Bezeichnung einem ausserordentlich schnellen Wandel unterworfen ist.

Artikel 9

Gegenüber der traditionellen Auswertung durch Analysten stellt die „elektronische", automatische Auswertung von Daten einen wesentlich grösseren Eingriff in die Datenhoheit dar und bedarf deshalb nach den Grundsätzen des Datenschutzes der ausdrücklichen Ermächtigung in dieser Vereinbarung.

[32] Ein Uniform Resource Identifier (Abk. URI) ist ein Identifikator und besteht aus einer Zeichenfolge, die zur Identifizierung einer abstrakten oder physischen Ressource dient. URIs werden zur Bezeichnung von Ressourcen (wie Webseiten, sonstigen Dateien, Aufruf von Webservices, aber auch z. B. E-Mail-Empfängern) im Internet eingesetzt. Unterarten von URIs sind die URL (Uniform Resource Locator) und der URN (Uniform Resource Name). Wobei vereinfacht gesagt eine URI anzeigt wo etwas ist (und wie man dorthin kommt) und URN beschreibt, was etwas ist. URLs waren ursprünglich die einzige Art von URIs, weshalb der Begriff URL oft gleichbedeutend mit URI verwendet wird.

Diese Bestimmung konkretisiert Artikel 8 Absatz 1 in dem Sinne, dass unter „Datenbearbeitung" insbesondere auch der Austausch, die Speicherung, die Verknüpfung und damit die Auswertung von Daten verstanden wird.

Die Vorgaben der RL 2016/680 müssen von jedem Vereinbarungspartner individuell auf seine Daten angewendet werden, weshalb sich eine spezielle Regelung in dieser Vereinbarung erübrigt.

Die Formulierung von Absatz 2 wurde so gewählt, dass grundsätzlich auch ein Outsourcing, wie es gegenwärtig für eine Anzahl von Polizei-Applikationen betrieben wird, möglich wäre. Das kantonale Recht des jeweiligen Sitzkantons bzw. das Bundesrecht, falls die Zentralstelle beim Bund betrieben werden sollte, bestimmt dabei, ob und unter welchen Voraussetzungen ein Outsourcing möglich ist[33] oder ob dazu eine Anpassung der Vereinbarung nötig wäre. Im Rahmen der laufenden PICAR-Projektarbeiten[34] ist ein Outsourcing jedoch kein Thema.

Artikel 10

Diese Bestimmung konkretisiert, dass der volle Zugriff zur jeweiligen Datenbank nur einem kleinen Kreis von Benutzern gewährt wird.

Erst die Produkte (Auswertungen, Berichte), welche mit Hilfe einer Datenbank erstellt werden, sind einem weiteren Kreis von Personen zugänglich, der jedoch auf Mitarbeitende der beteiligten Polizeikorps bzw. des GWK oder anderer geeigneter Bundesstellen (vgl. Ausführungen zu Artikel 17 Absatz 1) beschränkt ist.

Die in eine (neue) Datenbank gelieferten, gesicherten Daten bleiben selbstverständlich in der originären Datenbank bestehen. Eine Mutation[35] in dieser hat durch den Lieferanten zu erfolgen, ist er doch dafür verantwortlich (Artikel 6 Absatz 2), dass die Daten „rechtmässig und richtig" sind. Der umgekehrte Weg bzw. eine Mutation durch eine andere Stelle ist nicht zulässig. Daten sind so zu kennzeichnen, dass der Datenlieferant jederzeit klar ist.

In der Datenbank können diese Daten durch die Zentralstelle und die Aussenstellen ergänzt, verknüpft und verbunden werden, wobei diese Tätigkeiten mit einem Hinweis auf die handelnde Stelle ergänzt werden müssen.

Mutationsprozesse bzw. das Loggen von Mutationen sind technisch operative Aspekte und deshalb in den jeweiligen Betriebsreglementen und ISDS-Konzepten zu regeln.

Artikel 11

Absatz 1: Um keine Unsicherheiten in Bezug auf das anwendbare Recht aufkommen zu lassen und um die Abläufe zu vereinfachen, soll nur ein Recht in Bezug auf die neuen

[33] Z.B. unter der Bedingung, dass der Datenserver seinen Standort in der Schweiz hat.
[34] Vgl. Ziff. 3.2.2.
[35] Auch eine Löschung ist eine Mutation.

Datenbanken zur Anwendung kommen. Anwendbar soll das Recht des Sitzes der Zentralstelle sein. Dies gilt sowohl in Bezug auf das Datenschutzrecht, als auch in Bezug auf das zugehörige Verfahrens- oder auch Haftungsrecht. Mit dem anwendbaren Recht ist auch die Zuständigkeit der Datenschutzaufsicht verbunden. Auf die in den kantonalen Polizeisystemen bzw. den Bundessystemen verbleibenden Informationen, bleibt selbstverständlich weiterhin das jeweilige Recht anwendbar.

Absatz 2: Die Rechtmässigkeit der Datenerfassung bestimmt sich nach dem Recht des liefernden Teilnehmers. Die jeweiligen Polizeigesetze können voneinander abweichen. Geht es darum, die Rechtmässigkeit einer Datenerfassung zu prüfen, muss das jeweils einschlägige Recht berücksichtigt werden und nicht das Recht der Zentralstelle.

Artikel 12

Absatz 1: Je nach Zeitpunkt, in dem ein Gesuch gestellt wird, richtet sich das Verfahren entweder nach der StPO oder dem Datenschutzrecht. Richtet sich das Verfahren nach der Datenschutzgesetzgebung, ist das Datenschutzrecht des Sitzes der Zentralstelle anwendbar.

Absatz 2: Für die Bearbeitung der Gesuche ist die Zentralstelle zuständig. Die Zentralstelle bearbeitet die Gesuche in Rücksprache mit den liefernden Teilnehmern, da sie unter Umständen nicht alle Gründe für eine Einschränkung, ein Aufschieben oder ein Verweigern eines Gesuches kennt (z.B. ermittlungstaktische Gründe).

Inwiefern die Zentralstelle eine Löschung oder Berichtigung selbst vornehmen kann oder beim liefernden Teilnehmer veranlassen muss, hängt von der jeweiligen Datenbank ab und wird im Betriebsreglement festgelegt. Die Verantwortung für die Umsetzung liegt jedoch bei der Zentralstelle.

Absatz 3: Die Einschränkungsgründe ergeben sich aus dem kantonalen Datenschutzrecht oder dem Datenschutzrecht des Bundes. Auch hier ist wieder das Recht des Sitzes der Zentralstelle anwendbar. Obwohl die Datenschutzgesetze sehr ähnlich formuliert sind, ist es theoretisch denkbar, dass die Einsicht aufgrund unterschiedlicher gesetzlicher Formulierungen nicht in allen Kantonen bzw. im Bund gleich gewährt wird. In der Praxis werden diese Abweichungen jedoch selten vorkommen und inhaltlich kaum wesentlich sein.

Weitere Einschränkungsgründe können sich aus dem Bundesrecht ergeben.

Artikel 13

Die Regelung der Löschfristen ist einerseits aufgrund des Datenschutzes notwendig, dient andererseits auch der Pflege der Datenbank und damit dem sinnvollen Betrieb der Lage- und Analysesysteme.

Absatz 1 Buchstabe a: Sobald die Daten dem Bearbeitungszweck nicht mehr dienen, sollen sie gelöscht werden. Zudem ist eine absolute Maximalfrist von 10 Jahren vorgesehen, nach der die Daten zu löschen sind.

Absatz 1 Buchstabe b: Handelt es sich um eindeutig verknüpfte Ereignisse, soll für den Beginn des Fristenlaufs der letzte Zuwachs zum Gesamtbild ausschlaggebend sein. So kann vermieden werden, dass einzelne Ereignisse frühzeitig aus der Datenbank entfernt werden, die zur späteren Beurteilung bzw. Aufklärung notwendig wären. Im Übrigen ist es möglich, einzelne Ereignisse - falls sie bei einem Teilnehmer immer noch in Bearbeitung sind - bei erheblicher Relevanz erneut einzutragen, da die Löschfristen der kantonalen Polizeisysteme bzw. der Bundessysteme von dieser Bestimmung nicht tangiert werden.

Absatz 1 Buchstabe c: Kann der Verdacht gegen eine Person ausgeräumt werden, gibt es keinen Grund mehr, diese weiter in der Datenbank zu führen. Eine weitere Aufbewahrung wäre unverhältnismässig.

Absatz 2: Im Sinne des Opferschutzes sind Daten zu geschädigten Personen bereits dann aus den Datenbanken zu entfernen, wenn der Bearbeitungszweck es erlaubt. D.h. einerseits, dass dort, wo mit anonymisierten Daten gearbeitet werden kann, der Personenbezug von Amtes wegen zu löschen ist und andererseits, dass alle Angaben zu den geschädigten Personen zu löschen sind, sobald der Bearbeitungszweck dies erlaubt.

Artikel 14

Die Vereinbarung legt die Grundsätze der Finanzierung fest, welche für alle dereinst betriebenen Lage- und Analysesysteme gleichermassen gelten[36]:

Der Betrieb solcher Systeme hat jeweils Infrastruktur-, Betriebs- und Lizenzkosten zur Folge. Diese sind von jedem Teilnehmer, der das jeweilige System nutzt, selber zu tragen (Absatz 1)[37]. Absatz 2 regelt die Verteilung der Kosten für den Betrieb der jeweiligen Zentral- und Datenschutzaufsichtsstelle[38]. Jeder Teilnehmer hat einen Anteil dieser Kosten zu tragen. Welcher konkrete Verteilschlüssel sich als sachgerecht erweist, hängt vom jeweiligen Lage- und Analysesystem ab. Zur Verfügung stehen die vier genannten Verteilschlüssel, gegebenenfalls ergänzt durch einen Sockelbeitrag, der gleichmässig verteilt wird und verhindern soll, dass ein grosser Teilnehmer unverhältnismässig hohe Kosten zu tragen hat (Absatz 3). Ausdrücklich wird die Aufzählung als abschliessend bezeichnet. Die Anwendung

[36] Vgl. auch Ziff. 3.
[37] Für PICAR entstehen den beteiligten Teilnehmern im Übrigen keine Lizenzkosten. Die Universität Lausanne und die Kantonspolizei VD, welche PICAR entwickelt haben, stellen ihnen das System kostenfrei zur Verfügung.
[38] Um die Kosten der Datenschutzaufsichtsstelle aber überhaupt überwälzen zu können, müsste eine ausdrückliche gesetzliche Grundlage im Kanton dieser Datenschutzaufsichtsstelle vorhanden sein. Dies ist gegenwärtig, soweit ersichtlich, in keinem Kanton der Fall.

eines nicht genannten Verteilschlüssels setzt demnach eine Änderung der Vereinbarung voraus.

Die Kosten können erstens (Buchstabe a) analog zu den Artikeln 11 und 12 der Vereinbarung zwischen dem Bund und den Kantonen zur Harmonisierung der Polizeiinformatik in der Schweiz (HPI) vom 10. November 2011 zwischen den jeweils beteiligten kantonalen Teilnehmern einerseits und den jeweils beteiligten Teilnehmern des Bundes (beziehungsweise allenfalls des Auslands) andererseits im Verhältnis 70:30 aufgeteilt werden. Die beteiligten kantonalen Teilnehmer teilen sich ihren Beitrag nach Massgabe der im Zeitpunkt der Rechnungstellung aktuell bekannten ständigen Wohnbevölkerung.

Zweitens kann sich die Anzahl Teilnehmer als sachgerechter Verteilschlüssel erweisen (Buchstabe b). Drittens kann der bewährte KKJPD-Schlüssel zur Anwendung kommen, welcher sich auf die im Zeitpunkt des Inkrafttretens der Vereinbarung bekannte ständige Wohnbevölkerung des Teilnehmers stützt (Buchstabe c). Viertens können die Kosten aufgrund der Grösse der von den Teilnehmern bearbeiteten Datenmenge berechnet werden (Buchstabe d).

Es ist Aufgabe der Teilnehmer, den konkret anwendbaren Verteilschlüssel für das Lage- und Analysesystem in dessen Betriebsreglement verbindlich festzulegen. Die Entscheidung hat sich danach zu richten, welcher der genannten Verteilschlüssel sich für das konkrete Lage- und Analysesystem als am sachgerechtesten erweist.

Die Kompetenz der Teilnehmer, dem gewählten Verteilschlüssel zuzustimmen und die geschuldeten Beträge auch tatsächlich zu zahlen, richtet sich selbstverständlich nach der jeweiligen Gesetzgebung[39].

Artikel 15

Absatz 1 hält fest, dass ein Austritt aus einer Datenbank möglich ist. Der Austritt soll in geordneten Bahnen ablaufen. Es soll genügend Zeit eingeräumt werden, damit die Ablösung aus der Datenbank vorgenommen werden kann. Sechs Monate werden als genügend angesehen.

Absätze 2 und 3 halten fest, dass mit dem Eintritt der Kündigungswirkung Rechte (z.B. das Recht, die Datenbank zu nutzen) und Pflichten (z.B. die Kostentragungspflicht) entfallen. Ein Austritt eines Teilnehmers kann finanzielle Folgen haben. Die Vereinbarung hält aber fest, dass grundsätzlich keine Rückerstattung für geleisteten Sach- und Personalaufwand zu erfolgen hat.

[39] Vgl. auch die Erläuterungen zu Art. 7.

Bei Unstimmigkeiten in Zusammenhang mit einem Austritt ist die Streitbeilegungsbestimmung des Artikels 20 i.V.m. Artikel 4 Absatz 1 anwendbar.

Artikel 16

Absatz 1: Mit dem Austritt eines Teilnehmers werden dessen eingegebene Daten aus der Datenbank gelöscht. Die Teilnehmer tragen die Verantwortung dafür, dass die von ihnen eingegebenen Daten rechtmässig und richtig sind[40]. Tritt ein Teilnehmer aus, hat er keinen Zugriff mehr auf seine eingegebenen Daten und kann sie nicht mehr korrigieren, wenn sich zeigt, dass die Daten nicht mehr richtig sind. Somit ist nicht mehr gewährleistet, dass die eingegebenen Daten rechtmässig und richtig sind. Deshalb ist es folgerichtig, dass eingegebene Daten, die vom austretenden Teilnehmer stammen, mit dem Austritt des Teilnehmers gelöscht werden, sofern sie nicht in Verbindung stehen zu einem Ereignis, das von einem anderen Teilnehmer erfasst wurde.

Diese Bestimmung hat zur Folge, dass Datenbanken technisch so konfiguriert sein müssen, dass die Löschung von Daten eines Teilnehmers möglich ist. Bei der Datenbank PICAR ist diese Anforderung erfüllt.

Absatz 2: Wird eine Datenbank ganz aufgelöst, werden sämtliche Datenbestände gelöscht. Diese Löschung ist technisch so zu gestalten, dass die Daten definitiv gelöscht werden und nicht wiederhergestellt werden können. Nur so ist der Schutz der Personendaten vor unrechtmässiger Bearbeitung gewährleistet. Allfällige Löschkosten sind nach dem für die Datenbank festgelegten Verteilschlüssel zu tragen. Das Betriebsreglement enthält die entsprechenden Detailregelungen (vgl. Artikel 7 Absatz 2 Buchstabe e).

Artikel 17

Absatz 1 regelt, wer dieser Vereinbarung beitreten kann. Dies sind sämtliche Kantone sowie geeignete Bundesstellen. Da diese Vereinbarung vor allem der Zusammenarbeit der Kantone auf polizeilicher Ebene zum umschriebenen Zweck (Artikel 1 der Vereinbarung) dient, ist es konsequent und im Sinne dieser Vereinbarung, dass sämtliche Kantone der Vereinbarung beitreten können.

Es gibt aber weitere, nicht-kantonale Organisationen, die sich mit der effizienten Bekämpfung der Serienkriminalität beschäftigen. Auch diese Organisationen sollen sich an dieser Vereinbarung beteiligen können. Die Bestimmung schränkt aber die mögliche Beteiligung von weiteren Organisationen auf geeignete Bundesstellen ein. Damit wird klargestellt, dass sich ausschliesslich Stellen des Bundes an der Vereinbarung beteiligen können[41]. Es soll sich aber nicht jede Bundesstelle an der Vereinbarung beteiligen können,

[40] Vgl. die Ausführungen zu Art. 6.
[41] Die Möglichkeit der Beteiligung des Bundes an einem Konkordat ist in Art. 48 Abs. 2 BV vorgesehen.

sondern nur die geeigneten. Im Sinne dieser Bestimmung bedeutet geeignet, dass die Bundesstelle zur effizienten Bekämpfung der Serienkriminalität einen Beitrag leisten kann bzw. muss. Als Beispiele können das Grenzwachtkorps oder die Bundeskriminalpolizei angeführt werden.

Dass der Beitritt sofort wirksam wird, ist so zu verstehen, dass vor dem Beitritt jeder Vereinbarungspartner die notwendigen kantonalen bzw. Bundes-Prozesse bzw. Erfordernisse (z.B. Beschluss der Legislative, Publikation) zu durchlaufen hat.

Ein Vereinbarungspartner kann nicht nur aus einer einzelnen Datenbank ausscheiden (Artikel 15), sondern auch aus der Vereinbarung. Auch dafür ist eine Frist von sechs Monaten auf das Ende eines Kalenderjahrs vorgesehen.

Artikel 18

Die Vereinbarung tritt in Kraft, wenn mindestens zwei Vereinbarungspartner entsprechend dem für sie massgebenden Recht den Beitritt formell rechtskräftig erklärt haben. Die hierfür erforderlichen Bedingungen bestimmt das jeweilige kantonale bzw. Bundes-Recht.

Materielle Anpassungen bzw. Änderungen der Vereinbarung bedürfen der Zustimmung sämtlicher Vertragspartner (Absatz 2). Das jeweilig anwendbare Recht des Vertragspartners bestimmt, wie diese Zustimmung zustande kommt.

Artikel 19

Nach Artikel 48 Absatz 1 BV können Kantone miteinander Verträge abschliessen sowie gemeinsame Organisationen und Einrichtungen schaffen. Sie können namentlich Aufgaben von regionalem Interesse gemeinsam wahrnehmen. Gemäss Absatz 2 von Artikel 48 BV kann sich der Bund im Rahmen seiner Zuständigkeiten beteiligen. Verträge zwischen Kantonen dürfen dem Recht und den Interessen des Bundes sowie den Rechten anderer Kantone nicht zuwiderlaufen. Sie sind dem Bund zur Kenntnis zu bringen (Artikel 48 Absatz 3 BV).

Nach Artikel 56 Absatz 2 BV dürfen Verträge der Kantone mit dem Ausland dem Recht und den Interessen des Bundes sowie den Rechten anderer Kantone nicht zuwiderlaufen. Ebenso sind sie dem Bund vor Abschluss zur Kenntnis zu bringen. Gemäss Artikel 56 Absatz 3 BV dürfen die Kantone mit untergeordneten ausländischen Behörden direkt verkehren; in den übrigen Fällen hat der Verkehr der Kantone mit dem Ausland durch Vermittlung des Bundes zu erfolgen. Artikel 172 BV hält in Absatz 3 fest, dass die Bundesversammlung die Verträge der Kantone unter sich und mit dem Ausland (nur dann) genehmigen muss, wenn der Bundesrat oder ein Kanton Einsprache erhebt.

Artikel 19 der Vereinbarung hält die verfassungsrechtliche Vorgabe, welche sowohl das Inkrafttreten der Vereinbarung wie auch sämtliche nach dessen Inkrafttreten darin vorgenommenen Änderungen betrifft, deklaratorisch nochmals explizit fest.

Artikel 20

Zwar ist davon auszugehen, dass kaum Streitigkeiten aus der Vereinbarung entstehen werden und dass – sollten sich doch solche ergeben – in der Regel eine einvernehmliche Lösung gefunden werden kann. Die im Rahmen der vorliegenden Vereinbarung vorgeschlagene Regelung sieht den Lenkungsausschuss für die Streitschlichtung/-beilegung unter den Vereinbarungspartnern vor (mit Möglichkeit des Weiterzugs an das Bundesgericht; vgl. oben, Ausführungen zu Artikel 4).

Artikel 21

Da die Haftungsregeln Vereinbarungsbestandteile mit Gesetzescharakter darstellen, werden sie auf Stufe der Vereinbarung festgelegt. Sie sind grundsätzlich den Haftungsregeln des PKNW nachempfunden. Durch die ausdrückliche Erwähnung in der Vereinbarung gelten sie für alle Vereinbarungspartner.

Absatz 2 stellt sicher, dass sich für den betroffenen Bürger bzw. die betroffene Bürgerin kein Nachteil daraus ergibt, dass mit der Vereinbarung eine besondere Organisation zur Datenbearbeitung geschaffen wird.

Polizeikonkordat Nordwestschweiz

Basel, 14. Juni 2019