IIIIII KANTON solothurn

Regierungsratsbeschluss

vom 1. April 2003

Nr. 2003/608

Verordnung über die polizeiliche Datenerhebung, -bearbeitung und -speicherung (PolDaVO)

---

1. Erwägungen

1.1 Allgemeines

Der Rechtsstaat verlangt nach Transparenz und Berechenbarkeit in all seinen Tätigkeiten, so auch bezüglich der Arbeit der Polizei im Umgang mit Personendaten. Um diese Transparenz zu gewährleisten, rechtfertigt es sich, neben dem Informations- und Datenschutzgesetz vom 21. Februar 2001 (InfoDG; Amtsblatt vom 2. März 2001, S. 376; BGS 114.1) und der Informations- und Datenschutzverordnung vom 10. Dezember 2001 (InfoDV; BGS 114.2), die am 1.Januar 2003 in Kraft getreten sind und für die Bearbeitung von Personendaten der gesamten Verwaltung Gültigkeit beanspruchen, eine eigene Verordnung (nachfolgend PolDaVO genannt) zu erlassen.
Die PolDaVO bezweckt, die von der Kantonspolizei bearbeiteten Personendaten dem InfoDG und der InfoDV entsprechend zu schützen und die grundrechtsverträgliche Verwendung der gesammelten Daten zu gewährleisten. Sie vollzieht und ergänzt die in den erwähnten Erlassen geregelten Bestimmungen und berücksichtigt dementsprechend vollumfänglich die grundlegenden Datenbearbeitungsprinzipien der Erforderlichkeit (und damit zusammenhängend das Übermassverbot), der Wahrheit, Sicherheit und der Zweckbindung.

Indessen drängt sich wegen der Besonderheiten polizeilicher Daten, welche vom InfoDG ausdrücklich anerkannt werden (siehe z. B. § 18 Abs. 2 InfoDG i. V. m. § 41 Abs. 3 des Gesetzes über die Kantonspolizei vom 23. September 1990, KapoG; BGS 511.11) eine die erwähnten Erlasse ergänzende Verordnung auf. Diese gilt einzig für Personendaten der Kantonspolizei und behandelt verbindlich die Bearbeitung, Löschungsregel und Aufbewahrungsdauer dieser Daten.
Die Zweiteilung der Verordnung in einen Allgemeinen und einen Besonderen Teil wird als zweckmässig erachtet, da die Kantonspolizei verschiedene Datensammlungen mit Personendaten führt. Der Allgemeine Teil enthält Bestimmungen, die für sämtliche Datensammlungen der Kantonspolizei Gültigkeit beanspruchen, der Besondere Teil findet lediglich auf die wohl wichtigsten und umfassendsten Datensammlungen, das polizeiliche Informationssystem ABI, sowie auf die erkennungsdienstlichen Foto- und Fingerabdrucksammlungen Anwendung. Da die Konsultation dieser Systeme aus dem polizeilichen Alltag nicht mehr wegzudenken ist, wird ihre Regelung auf Verordnungsstufe aus rechtsstaatlichen Überlegungen als gerechtfertigt erachtet.
Damit der Bürger sämtliche relevanten Bestimmungen bezüglich Datenbearbeitung durch die Kantonspolizei in einem einzigen Erlass nachlesen kann, wird die Wiederholung gewisser wichtiger Regelungen aus dem InfoDG, auf die gesetzestechnisch verzichtet werden könnte, bewusst in Kauf genommen.

1.2 Erläuterung einzelner Bestimmungen

§ 1.

Die ausführliche Formulierung soll den Bürgern Gegenstand und Zweck der PolDaVO verdeutlichen. Die zur Bearbeitung besonders schützenswerter Personendaten notwendige Rechtsgrundlage findet sich in § 40 und 41 Absatz 2 und 3 KapoG.

§ 4.

Dadurch wird eine Segmentierung der Zugriffsberechtigung vorgenommen:
Nur diejenigen Personendaten, welche zur Erfüllung der gesetzlichen Aufgaben notwendig sind, sollen dem einzelnen Mitarbeitenden auch tatsächlich zugänglich gemacht werden.
Der Begriff „Mitarbeitende der Kantonspolizei" ist bewusst gewählt worden, um damit sprachlich mit § 18^{bis} des Gesetzes über die Kantonspolizei übereinzustimmen. Der erwähnte Paragraph ist noch nicht in Kraft, sondern soll im Rahmen der Reform der Strafverfolgung in das erwähnte Gesetz eingefügt werden.

§ 5.

Mit dieser Bestimmung wird für die betroffenen Bürger klar, an welche Instanz sie sich zwecks Ausübung der im InfoDG verankerten Rechte wenden können.
Die Kantonspolizei verfügt über drei Abteilungschefs. Die Delegationsbefugnis an diese ist zweckmässig.

§ 8.

Zum Zweck der Verhinderung und Aufklärung von Straftaten darf die Kantonspolizei Daten erheben. Aus taktischen und auch aus verwaltungsökonomischen Gründen kann sich die nicht erkennbare Datenerhebung im Rahmen der polizeilichen Tätigkeiten (v.a. im Zusammenhang mit repressiven Massnahmen) als unerlässlich erweisen. In diesen Fällen ist durch das allgemeine Auskunftsrecht gemäss § 26 InfoDG sowie durch das Akteneinsichtsrecht gemäss kantonaler Strafprozessordnung die Rechtmässigkeit gewährleistet.
Unrechtmässig hingegen wäre die Datenbeschaffung im Rahmen der sogenannten Rasterfahndung, d. h. der Überprüfung privater oder öffentlicher Dateien nach vorher festgelegten kriminalistischen Merkmalen.

§ 9.

Unter den genannten Bedingungen kann der Zugriff auf Personendaten nicht nur Korpsangehörigen gewährt werden, sondern auch gewissen Spezialisten und Spezialistinnen, die von der Kantonspolizei als zivile Mitarbeitende angestellt und z.T. sogar zur Vornahme gesetzlicher Amtshandlungen befugt sind. Selbstverständlich muss auch bei ihnen im Einzelfall abgeklärt werden, ob ein solcher Zugriff zur Erfüllung ihrer gesetzlichen Aufgaben tatsächlich erforderlich ist und auch sie unterstehen dem Amtsgeheimnis.
Ob den einzelnen Korpsangehörigen oder Spezialisten die Zugriffsberechtigung erteilt wird, entscheidet der Kommandant beziehungsweise die Kommandantin. Mit der notwendigen Visierung beabsichtigen wir, dass die Notwendigkeitsprüfung in der Praxis auch in jedem Einzelfall wirklich vorgenommen wird. Die Erteilung der Zugriffsberechtigung kann an die Abteilungschefs delegiert werden (§ 5 i. V. m. § 9 dieser Verordnung), denn nur diese haben Kenntnis vom genauen Tätigkeitsgebiet ihrer Mitarbeitenden und können demzufolge abschätzen, ob der Zugriff tatsächlich erforderlich ist, um die zugewiesenen Arbeiten effizient erfüllen zu können. Die Delegationsbefugnis in diesem Zusammen-

hang ist demnach gerade wegen der von uns praktizierten Einschränkung der Zugriffsberechtigung notwendig.
Dabei ist die Zugriffsberechtigung als Oberbegriff zu verstehen, der sowohl die Abfrage- als auch die Eingabeberechtigung umfasst.
Der Kommandant oder die Kommandantin beziehungsweise der zuständige Abteilungschef entscheidet somit, ob dem einzelnen Mitarbeitenden überhaupt Zugriff gewährt werden soll und falls ja, ob ihm bloss die Möglichkeit der passiven Kenntnisnahme oder auch der aktiven Eingabe und Abänderung der Daten gegeben wird. Diese Entscheidung wird entsprechend dem Grundsatz der Verhältnismässigkeit getroffen. Eine genaue Zuteilung der Abfrage- und Eingabeberechtigung für jeden einzelnen Mitarbeitenden würde den Rahmen einer Verordnung sprengen.
Die einzelne Zuteilung wird in einem Anhang geregelt. Ein solches Vorgehen entspricht auch der Praxis auf Bundesebene (vgl. beispielsweise die Verordnung über das informatisierte Personennachweis-, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei vom 21. November 2001, IPAS-Verordnung; SR 361.2 oder die Verordnung über die Ausweise für Schweizer Staatsangehörige vom 20. September 2002, Ausweisverordnung; AS 2002 S. 3151ff).

§ 10.
Zur Zeit gewährt die Kantonspolizei einzig der Stadtpolizei Solothurn Zugriff auf einige Informationssysteme, soweit diese Sicherheit für die strikte Einhaltung der vorliegenden Verordnung bietet. In begründeten Sonderfällen kann die Zugriffsberechtigung für Mitarbeitende der Stadtpolizeien auch umfangmässig durch den Kommandanten oder die Kommandantin eingeschränkt werden.

§ 11.
Bezüglich des Auskunftsrechts in hängigen Strafverfahren gelten die Bestimmungen der Strafprozessordnung. Wo noch kein solches Verfahren hängig ist, die Polizei dennoch präventiv tätig wird, müssen Bestimmungen des Datenschutzes die Grundrechte, insbesondere das Recht auf informationelle Selbstbestimmung, gewährleisten.
Gemäss des Vorentwurfs zu einer Schweizerischen Strafprozessordnung wird ein Vorverfahren u. a. durch die selbständige Ermittlungstätigkeit der Polizei eingeleitet. Bereits mit der Aufnahme polizeilicher Vorermittlungen, welche erst aufgenommen werden, sobald ein Anfangsverdacht vorliegt, muss das Strafverfahren im Sinne der Terminologie des § 2 InfoD als „hängig“ gelten. Nur eine solche Auslegung vermag den Zweck dieser Norm, nämlich den Vorrang der fallspezifischen Arbeit der Strafjustizbehörden gegenüber der institutionellen Aufsicht der Datenschutzorgane und somit die Unabhängigkeit der Justiz, zu garantieren. Zusammenfassend ist deshalb festzuhalten, dass die zur Verifizierung eines Anfangsverdachts stattfindenden einzelfallbezogenen Datenabgleiche der Gerichtspolizei nicht unter die Datenschutzgesetzgebung fallen.
Hingegen unterliegen sowohl die präventiven Tätigkeiten der Polizei, d.h. die Datenbearbeitung im Rahmen der Gefahrenabwehr, wie auch die Datenbearbeitung mittels des Informationssystems ABI, welches Daten aus hängigen und abgeschlossenen Verfahren umfasst, der Datenschutzgesetzgebung.

§ 12.
Mit dieser Bestimmung soll dem Grundsatz der Wahrheit und Aktualität der Personendaten Rechnung getragen werden.
Die Regelung, dass erst auf Gesuch der betroffenen Person hin die Nachführung der Einträge vorgenommen wird, ist notwendig, da die Kantonspolizei nicht sämtliche Urteile der Gerichtsbehörden systematisch zur Kenntnisnahme erhält. Ein Nachtrag von Amtes wegen ist deshalb aus praktischen Gründen nicht bzw. nur in denjenigen Fällen möglich, in denen die Kantonspolizei über diese Verfahrensbeendigung unterrichtet wird. Dies trifft auf Nichteintretens- und Einstellungsentscheide des

Kantonalen Untersuchungsrichteramtes, über die wir als Anzeiger gem. § 85 der Strafprozessordnung vom 7. Juni 1970 (BGS 321.1) unterrichtet werden, zu. In diesen Fällen wird bereits heute die Bemerkung „Nichteintreten“ bzw. „Verfahren eingestellt“ von Amtes wegen in das Informationssystem aufgenommen. Bei Nichteintreten auf die Strafanzeige oder den Strafantrag sowie bei der Verfahrenseinstellung oder bei einem Freispruch besteht ein Anspruch auf Vornahme des Nachtrags. Die Einreichung eines schriftlichen Gesuchs inkl. Kopie des entsprechenden Entscheids stellt für den einzelnen Bürger und die einzelne Bürgerin keinen allzu grossen Aufwand dar. Bezüglich der Auswirkungen des Nachtrags auf die Aufbewahrungsdauer verweisen wir auf die Erwägungen zu § 39.

§ 13.
Diese Bestimmung, die den Zugang zu amtlichen Dokumenten regelt, bezieht sich sowohl auf physische Dokumente als auch auf gespeicherte Daten. Gemäss § 4 lit. a InfoDG ist einzig ausschlaggebend, dass die Dokumente auf einem Informationsträger (Papier, Ton- oder Bildaufzeichnungen und dgl.) aufgezeichnet sind.

§ 15.
Unter einem genügenden Rechtsnachweis, der einem Dritten die Auskunftserteilung ermöglicht, verstehen wir das Vorliegen einer schriftlichen Vollmacht, in welcher der Betroffene den Dritten explizit zum Erhalt der Auskunft bezüglich ihn betreffender Berichte ermächtigt. Diese Bestimmung entspricht somit § 15 Abs. 1 lit. d InfoDG.
Dritte können insbesondere Versicherungsgesellschaften oder Rechtsanwälte sein.
Zu beachten ist, dass diese Regelung nicht in hängigen Verfahren zum Zug kommt, da dort die Strafprozessordnung gilt. Sie gilt einzig für Verfahren, die für die Kantonspolizei als abgeschlossen gelten, in denen z. B. versicherungstechnische Fragen mit Hilfe polizeilicher Akten gelöst werden sollen.

§ 16.
Der Grundsatz stimmt vollumfänglich mit § 19 InfoDG überein.
Absatz 2 präzisiert diesen Grundsatz und weist auf die in §§ 28- 40 PolDaVO für die jeweils verschiedenen Datenkategorien des polizeilichen Informationssystems ABI und der erkennungsdienstlichen Datensammlungen festgelegten Aufbewahrungsfristen.
Ausnahmen von diesen festgelegten maximalen Aufbewahrungsfristen sind nur gemäss § 35 PolDaVO möglich.

§ 18.
Die folgenden Paragraphen gelten lediglich für das polizeiliche Informationssystem ABI und die erkennungsdienstlichen Datensammlungen. Für diese Datensammlungen gilt der vorherige Allgemeine Teil grundsätzlich auch: Beispielsweise gilt § 9, der die Zugriffsberechtigung regelt, auch für das ABI. Der Besondere Teil hingegen regelt diejenigen Datensammlungen, die aus sachlichen Gründen des Datenschutzes in Abweichung zum Allgemeinen Teil einer detaillierten Regelung bedürfen.

§ 19.
Unter der Rubrik „Verbindungen“ werden Hinweise auf weitere an der Straftat beteiligte Personen aufgeführt.

§ 20.
Mit Absatz 1 wird sichergestellt, dass die Kantonspolizei erst bei Vorliegen eines konkreten Tatverdachts beginnt, Personendaten zu bearbeiten. Dieser Anfangsverdacht ist für die Aufnahme polizeili-

cher Vorermittlungen im Rahmen der Repression von Straftaten notwendige Voraussetzung. Grunddaten gemäss Absatz 1 werden demnach lediglich von Beschuldigten erfasst. Zudem ist die Bearbeitung dieser Daten erforderlich, wenn die betroffene Person in ein administratives Bewilligungsverfahren verwickelt ist.
Die Aufzählung der vier Fälle, bei denen die Polizeibehörden notwendigerweise die ermittelten Grunddaten bearbeiten müssen, um ihrem gesetzlichen Auftrag der Strafverfolgung bzw. des Verfahrens im Rahmen der Waffen- und Sprengstoffgesetzgebung überhaupt nachkommen zu können, ist abschliessend zu verstehen: Über Zeugen, Kontaktpersonen des mutmasslichen Täters oder der mutmasslichen Täterin sowie über andere Drittpersonen werden demnach keine Grunddaten registriert. Einzige Ausnahme ist der oder die Geschädigte, welche unter den Falldaten erscheinen.
Die Voraussetzungen einer erkennungsdienstlichen Behandlung finden sich in § 33 Absatz 2 lit. a bis d KapoG.
Bezüglich der Haftdaten ist zu präzisieren, dass eine Person, welche von der Kantonspolizei weder erkennungsdienstlich behandelt noch je in polizeiliche Ermittlungen involviert war, nicht unbedingt auch in das polizeiliche Informationssystem aufgenommen wird, da wir nicht von allen Häftlingen Kenntnis erhalten. Bei den Haftdaten handelt es sich somit nicht um eine vollständige Auflistung sämtlicher in einer Anstalt des Kantons Solothurn je inhaftierter Personen.
Indessen findet sich bei den Grunddaten all jener Personen, die von der Kantonspolizei Solothurn gem. § 31 Absatz 2 KapoG in Gewahrsam genommen werden, der Vermerk „Haft“. Näheres dazu siehe unten bei den Erläuterungen zu § 23 PolDaVO.
Zu den Falldaten siehe die Erläuterungen zu § 24 PolDaVO.
Zur Bearbeitung von Grunddaten im Zusammenhang mit Waffendaten ist die Kantonspolizei gemäss des Waffengesetzes vom 20. Juni 1997 (WG, SR 514.54) i. V. m. der Verordnung über den Vollzug des eidgenössischen Waffenrechts (KRB vom 11. Mai 1999; BGS 512.211) verpflichtet.
Die Rechtsgrundlage zur Bearbeitung von Sprengstoffdaten findet sich im Bundesgesetz über explosionsgefährliche Stoffe vom 25. März 1977 (SR 941.41).

Absatz 2 erklärt die Bearbeitung von Personendaten für zulässig, wenn zwar keine in Absatz 1 genannten Gründe vorliegen, eine Bearbeitung indessen aus anderen Gründen erforderlich ist.
Diese Aufzählung ist nicht abschliessend zu verstehen, da eine vollständige Auflistung kaum möglich ist. Die erwähnten Situationen sind allerdings diejenigen, die im polizeilichen Alltag am häufigsten auftreten: Rapporte im Zusammenhang mit aussergewöhnlichen Todesfällen und Leumunds- oder andere polizeiliche Berichte.
Die Prüfung des Leumunds ist z. B. gemäss Art. 32 Absatz 1 lit. d der Verordnung über Waffen, Waffenzubehör und Munition (WV; SR 514.541) und gemäss § 46 Absatz 1 KapoG im Zusammenhang mit der Bewilligungspflicht bestimmter Tätigkeiten als Privatdetektiv und als privates Sicherheitsunternehmen erforderlich. Ebenfalls kann die Kantonspolizei gem. § 5 Abs. 3 der Vollzugsverordnung zum Gesetz über das Kantons- und Gemeindebürgerrecht vom 28. September 1993 (Bürgerrechtsverordnung; BGS 112.12) auf Begehren der Bürgergemeinde oder des kantonalen Amtes Informationen über den Einbürgerungswilligen einholen und in Leumundsberichten weitergeben.

§ 21.
Diese Bestimmung soll der Kantonspolizei die Bearbeitung von Personendaten ermöglichen, obwohl noch kein Anfangsverdacht bezüglich einer konkret begangenen Straftat vorliegt, der die Polizei zur Vornahme von Ermittlungen verpflichten würde.
Indessen geht es um präventive Polizeiaufgaben, in concreto um Gefahrenabwehr und den Schutz der physischen Integrität gefährdeter Personen, zu deren Erfüllung die Kantonspolizei gemäss §§ 2 und 3 Absatz 1 KapoG verpflichtet ist.

Die Informationsbeschaffung und insbesondere deren Bearbeitung inkl. Aufbewahrung ohne Anfangsverdacht, welche der Sensibilisierung und der Verhinderung künftiger Straftaten dienen soll, darf u. E. nur unter Beachtung bestimmter Vorsichtsmassnahmen zulässig sein, damit eine ausufernde und quantitativ wie qualitativ masslose Beschaffung und Bearbeitung wirksam verhindert werden kann. Andererseits können Warnungen und konkrete Drohungen mit schweren Straftaten, beispielsweise im Zusammenhang mit häuslicher Gewalt, von der Polizei nicht einfach unbeachtet und schubladisiert werden. Erfahrungsgemäss drohen zahlreiche Amokläufer ihre Taten einer mehr oder weniger grossen Öffentlichkeit vorher an.
Es ist Aufgabe des Staates, sich um einen Ausgleich zwischen den Interessen des Einzelnen und der Allgemeinheit am Erhalt des liberalen Staates und dem Bedürfnis derselben Individuen nach präventiven Massnahmen, um Straftaten wenn möglichst zu verhindern, zu bemühen.
Mit der Bearbeitung solcher Daten soll, selbstverständlich unter Beachtung des Amtsgeheimnisses, in erster Linie die gezielte Beratung bedrohter Personen und das Ergreifen bestimmter Massnahmen im Rahmen der Prävention bezweckt werden. Andererseits dienen diese Daten bei Delikten gegen die körperliche Integrität bedrohter Personen als erste Ermittlungsansätze.
In diesem Sinne ist eine Bearbeitung nur zulässig, wenn der Betroffene durch sein Verhalten eine grosse Gewaltbereitschaft an den Tag legt, so dass die Behörden nach eingehender Prüfung der konkreten Umstände zur Überzeugung gelangen, dass mit gewalttätigen Handlungen ernsthaft gerechnet werden muss.
Blosses Querulieren oder auffällige Verhaltensweisen ohne jeglichen Bezug zu einer Straftat genügen nicht zur Rechtfertigung. Ebenso werden keine Daten über politische Tätigkeiten der Bürger gesammelt, sondern im Bereich des Staatsschutzes bleiben das Bundesgesetz über die Wahrung der inneren Sicherheit (BWIS; SR 120) sowie die Verordnung über das Staatsschutz-Informations-System (ISIS; SR 120.3) vorbehalten. Die massive verbale Drohung mit einer Straftat, gerichtet gegen eine bestimmte Person oder Personengruppe, die je nach Einzelfall gewichtet werden muss, vermag hingegen unter Umständen die Bearbeitung zu rechtfertigen.
Als weitere Sicherung zur Vermeidung allgemeiner und quasi flächendeckender Bearbeitungen bestimmter Bürger und Bürgerinnen wird verlangt, dass über die Bearbeitung solcher Daten in jedem Einzelfall der Polizeikommandant oder die Polizeikommandantin nach Vornahme einer Interessenabwägung zu entscheiden und die ausdrückliche und schriftliche Genehmigung zu erteilen hat. Der Kreis der potentiellen Störer, die eine Bearbeitung ihrer Daten hinnehmen müssen, wird dadurch eng gehalten.
Ferner wird auch die Zahl der Zugriffsberechtigten bewusst sehr klein gehalten und es wird eine spezielle Regelung hinsichtlich der Aufbewahrungsdauer statuiert (siehe dazu unten: Erwägungen zu § 27 bzw. § 31 Abs. 3 PolDaVO).

§ 22.
Zweck einer erkennungsdienstlichen Behandlung ist die Erlangung von sogenannten erkennungsdienstlichen Daten. Dazu sind alle Informationen über physische Merkmale und Tatortspuren zu zählen, die den Behörden zur gegenwärtigen und künftigen Identifizierung von Personen und Leichen dienen, siehe dazu auch § 33 Abs. 1 KapoG.
Die Datenbearbeitung durch den Erkennungsdienst richtet sich grundsätzlich nach der Datenschutzgesetzgebung, die speziellen Datenbearbeitungsvorschriften des Art. 351^{septies} des Schweizerischen Strafgesetzbuches vom 21. Dezember 1937 (StGB; SR 311.0), der Verordnung über die Bearbeitung erkennungsdienstlicher Daten vom 21. November 2001 (SR 361.3) und der Verordnung über das DNA-Profil-Informationssystem vom 31. Mai 2000 (EDNA-VO; SR 361.1) bleiben vorbehalten.

Unter dem Begriff Signalement hat man die folgenden, eine bestimmte Person kennzeichnenden Daten zu verstehen: Statur, Grösse, Gesichtsform, Haarfarbe, Haarhelligkeit, Hautfarbe, Augenfarbe sowie Sprachen, derer die betroffene Person mächtig ist.
Als besondere Merkmale werden, sofern vorhanden, vermerkt: Narben und Tätowierungen.
Als Daktyloskopie bezeichnet man die Abnahme der Finger- und allenfalls Handballenabdrücke des Betroffenen.
Anhand des Wangenschleimhaut-Abstrichs kann die DNA eines Individuums analysiert werden.
Unter dem Stichwort Behandlungsgrund wird die Straftat, welcher die betroffene Person verdächtigt wird, aufgeführt. Weitere erkennungsdienstliche Daten werden nicht bearbeitet.
Zu beachten ist, dass nicht nur die Kantonspolizei, sondern gemäss der erwähnten Bundesgesetzgebung auch das Bundesamt für Polizei Fotografien und daktyloskopische Daten aufbewahrt. Die mittels WSA erhaltenen DNA-Profile werden in der nationalen DNA-Datenbank am Institut für Rechtsmedizin der Universität Zürich aufbewahrt. Diesbezüglich bleibt die Bundesgesetzgebung vorbehalten.

§ 23.

Als mögliche Haft-Arten kommen Ausschaffungshaft (Vorbereitungshaft wird davon offenbar nicht unterschieden), Untersuchungshaft, polizeiliche Sicherheitshaft oder Strafvollzug in Frage.
Mögliche Austrittsgründe sind die ordentliche Entlassung, die Einweisung in eine andere Strafanstalt oder die Ausschaffung.
Mit Bekanntgabe der für die Inhaftierung zuständigen Behörde wird ersichtlich, bei welcher Behörde allenfalls weitere Informationen erhältlich sind.

§ 24.

Nach Kenntnis eines konkreten und strafrechtlich relevanten Ereignisses werden die entsprechenden Falldaten registriert. Auch Spurenfotografien und anderes Bildmaterial, obwohl auf den ersten Blick nicht unbedingt als Personendaten erkennbar, werden als Falldaten registriert, da beispielsweise anhand eines Schuhsohlenabdrucks durchaus eine Zuordnung zu einer bestimmten Person erfolgen kann.
Unter der Angabe „Ereignis“ wird auf den in Frage stehenden Tatverdacht bzw. auf dasjenige Gesetz, gegen welches eine Widerhandlung vermutet wird, hingewiesen.

§ 25.
Zur Registrierung dieser Personendaten ist die Kantonspolizei aufgrund des Waffen- bzw. des Sprengstoffgesetzes verpflichtet. Bezüglich Waffendaten bleibt anzumerken, dass die Registrierung nicht bereits mit der Ausstellung des Waffenerwerbsscheins erfolgt, sondern erst, wenn der Betroffene von dieser Bewilligung auch tatsächlich Gebrauch gemacht und eine Waffe erworben hat.

§ 26.
Die Kantonspolizei führt ein Journal über Ereignisse, Vorkommnisse und eingegangene Meldungen. Dieses System automatisiert die Protokollierung der polizeilichen Aktivitäten sowie die Dokumentation von Anordnungen, Massnahmen und Meldungen. Zweck dieser Aufzeichnungen ist es, den internen Informationsaustausch sicherzustellen.

§ 27.
Mittels Weiterbearbeitung können anhand bestimmter Suchkriterien Verknüpfungen mit bereits vorhandenen Daten hergestellt werden. Diese Möglichkeit stellt für die Kantonspolizei ein äusserst nützliches Arbeitsinstrument dar. Beispielsweise kann mittels Eingabe des Aliasnamens oder des Signalements die gewünschte Person im Informationssystem aufgefunden werden.
Nicht sämtliche Mitarbeitende, die Zugriff zum Informationssystem haben, sind auch zur Weiterbearbeitung berechtigt. Die Berechtigung wird je nach den dienstlichen Bedürfnissen vom Kommandanten oder der Kommandantin einzelnen Mitarbeitenden erteilt. Die Berechtigung zur Weiterbearbeitung hängt von der Datenkategorie ab:
Grunddaten können lediglich von den Angehörigen dreier Fachdienste der Kommando- und Kriminalabteilung weiterbearbeitet werden. Da die Person, welche gemäss § 21 PolDaVO registriert wird, lediglich mit ihren Grunddaten im ABI-Modul „Person“ zu finden ist, unter ihrem Namen jedoch nicht unbedingt auch ein Fall eröffnet wird, kann sichergestellt werden, dass diese Grunddaten nur von einem begrenzten Kreis Berechtigter abgerufen werden kann: Dies sind lediglich diejenigen Mitarbeitenden, welche den Namen der betroffenen Person bereits kennen, weil sie in einer konkreten Angelegenheit eine diese Person betreffende Amtshandlung vornehmen müssen sowie die wenigen Angehörigen, welche zur Weiterbearbeitung berechtigt sind.
Die Berechtigung zur Weiterbearbeitung erkennungsdienstlicher Daten steht lediglich den Angehörigen des kriminaltechnischen Dienstes zu.
Zur Weiterbearbeitung fallbezogener Daten sind lediglich diejenigen Mitarbeitenden der Kantonspolizei befugt, welche an das Amtsgeheimnis gebunden sind und diese Daten zur Erfüllung ihrer gesetzlichen Aufgaben benötigen. Mittels Eingabe eines Straftatbestandes kann auf die Personendaten derjenigen Betroffenen zugegriffen werden, welche im Zusammenhang mit diesem Delikt im Informationssystem verzeichnet sind.
Zur Weiterbearbeitung der Waffen- und Sprengstoffdaten ist lediglich der für Waffen und für Sprengstoff zuständige Sachbearbeiter befugt. Das Wissen um vorhandene Waffen kann für die Kantonspolizei bei der Planung und Vorbereitung allenfalls notwendiger Zwangsmassnahmen von grösster Wichtigkeit sein. Zu denken ist beispielsweise an Personenkontrollen und Hausdurchsuchungen.
Journal-Daten können lediglich von den Angehörigen des Informationsdienstes und der Kriminalanalyse weiterbearbeitet werden.
Jede Weiterbearbeitung der erfassten Personendaten wird § 13 InfoDV und § 43 Abs. 2 PolDaVO entsprechend protokolliert.

§ 28.
Um dem Grundrecht der persönlichen Freiheit Geltung zu verschaffen, darf der Staat Personendaten nicht unbeschränkt lange Zeit aufbewahren, selbst wenn diese nicht öffentlich zugänglich sind. Eine

zeitliche Limitierung ist aus rechtsstaatlichen Gründen demnach unabdingbar. Die Terminierung hat sich grundsätzlich nach der Datenschutzgesetzgebung zu richten, als lex specialis können datenbankspezifische Bearbeitungsvorschriften zum Zug kommen.
Diese Bestimmung konkretisiert bezüglich der im ABI aufbewahrten Grunddaten den Grundsatz des Paragraphen 16 und geht diesem somit vor.
Die ordentlichen Aufbewahrungsfristen des Absatzes 2 richten sich analog den Bestimmungen des Strafgesetzbuches bezüglich der Verjährungsfristen nach der Schwere der begangenen Straftat.

§ 29.
In den genannten Ausnahmefällen (Tod der betroffenen natürlichen Person bzw. Auflösung der betroffenen juristischen Person) gilt die in diesem Paragraphen genannte Ausnahmeregelung zum Paragraphen 28: Die entsprechenden Daten werden unverzüglich gelöscht. Vom Amt für Finanzen, Abteilung Finanzausgleich und Statistik, wird die Kantonspolizei von Amtes wegen vierteljährlich über den Tod aller im Kanton Solothurn wohnenden natürlichen Personen orientiert.

§ 30.
Bei mehrmaliger Registrierung gelten nicht die für die einzelnen Delikte geltenden Fristen, sondern die Frist sämtlicher Einträge richtet sich nach der am längsten dauernden Aufbewahrungsdauer. Mit dieser Regelung wird der statistisch belegbaren erhöhten Wahrscheinlichkeit eines Rückfalls Rechnung getragen (BGE 120 Ia 147 Erw. 2e).

§ 31.
Diese Aufbewahrungsdauer bezieht sich vorwiegend auf Bewilligungen zur gewerbsmässigen Ausübung von Tätigkeiten als Privatdetektiv oder privates Sicherheitsunternehmen gemäss §§ 45ff KapoG.
Absatz 3 trägt der Besonderheit dieser Datenkategorie hinsichtlich der Aufbewahrungsdauer gebührend Rechnung: Für diejenigen Personendaten, welche die Kantonspolizei im Rahmen ihrer präventiven Aufgaben bearbeitet, gilt eine vom konkreten Einzelfall abhängende Aufbewahrungsdauer. Es liegt in der Natur dieser Daten, dass für sie, im Gegensatz zu denjenigen Daten, welche sich auf eine bereits begangene Straftat beziehen, vernünftigerweise keine schematisch und von vornherein festgelegte Aufbewahrungsdauer bestimmt werden kann.

§ 32.
Damit soll der allgemein formulierte § 33 Abs. 3 KapoG präzisiert werden.
Unter dem Begriff der erkennungsdienstlichen Daten sind die im polizeilichen Informationssystem direkt abrufbaren Informationen zu verstehen.
Als erkennungsdienstliches Material werden die anlässlich einer erkennungsdienstlichen Behandlung erstellten physischen Akten (abgelegte Fotos und Fingerabdruckbögen) bezeichnet.
Die Aufbewahrung erkennungsdienstlichen Materials über den Abschluss eines Strafverfahrens hinaus ist von grossem öffentlichen Interesse und wird vom Bundesgericht nicht als schwerer Eingriff in die persönliche Freiheit betrachtet. Für die Polizeibehörden hingegen stellt dieses Material ein unerlässliches Mittel zur Aufklärung von Straftaten dar und erleichtert die Bekämpfung zukünftiger Verbrechen und Vergehen im Interesse eines wirksamen Schutzes der Allgemeinheit.
Zudem hat es das Bundesgericht in BGE 120 Ia 147 ausdrücklich für verhältnismässig befunden, dass in erkennungsdienstlichen Datenbanken nicht nur das erkennungsdienstliche Material derjenigen Betroffenen, die rechtskräftig verurteilt worden sind, sondern auch derjenigen erkennungsdienstlich behandelter Personen, gegen die es in der Folge zu keinem Schuldspruch gekommen ist, aufbewahrt werden.

Bei Personen, die sich eines strafrechtlichen Delikts schuldig gemacht haben, besteht gegenüber dem Durchschnittsbürger die leicht erhöhte Wahrscheinlichkeit, sie könnten auch in Zukunft in ein Delikt verwickelt werden (Erw. 2e des erwähnten BGE). Aus diesem Grund rechtfertigt sich die Aufbewahrung des erkennungsdienstlichen Materials, wenn das Verfahren bloss vorläufig eingestellt worden ist, weil der Sachverhalt nicht genügend abgeklärt werden konnte und sogar bei einem Freispruch, sofern dieser lediglich wegen eines Mangels an Beweisen erfolgte.
In diesem Zusammenhang ist ferner zu beachten, dass die Aufbewahrung von erkennungsdienstlichem Material im Unterschied zur Registrierung im zentralen Strafregister lediglich bedeutet, dass gegenüber dem Betroffenen einmal der Verdacht einer strafbaren Handlung bestanden hat. Auch wenn dasselbe Material in einem späteren Verfahren wieder verwendet werden sollte, liegt darin nur eine Verdachtsäusserung, welche die Unschuldsvermutung nicht verletzt (Erw. 3a des erwähnten BGE).
Konkret wird vom bereits zitierten BGE für „leichte Fälle“ eine maximale Aufbewahrungsfrist von 5 Jahren als vernünftig betrachtet.
Die Buchstaben a, c und d entsprechen Art. 15 der eidgenössischen Verordnung über die Bearbeitung erkennungsdienstlicher Daten vom 21.11. 2001, welche dem zitierten Grundsatzentscheid des Bundesgerichts entsprechend differenzierte Regelungen anstrebt. Buchstabe b richtet sich nach Art. 14 lit. b der Verordnung über das automatisierte Strafregister vom 1. Dezember 1999 (SR 331) und erscheint in Analogie zu § 31 Abs. 1 Satz 3 der PolDaVO sinnvoll.
Die Löschung dieser Daten erst nach Ablauf der deliktsspezifischen Aufbewahrungsfrist gem. § 28 PolDaVO muss als zu wenig ausdifferenziert zurückgewiesen werden. Auch nimmt die Eignung etlicher erkennungsdienstlicher Daten im Lauf der Zeit ab. In diesem Sinn erfüllt auch diese Bestimmung das Gebot der Notwendigkeit: Weil beispielsweise Fotos nach einer gewissen Zeit an Aussagekraft verlieren und somit von der Polizei nicht mehr sinnvoll verwendet werden können, sollen sie auch nicht uneingeschränkt aufbewahrt werden.

§ 34.
Die genannten Fristen berechnen sich jeweils ab Datum der Tatbegehung.

§ 36.
Die Kantonspolizei prüft verschiedene Gesuche um Bewilligungen im Zusammenhang mit explosionsgefährlichen Stoffen: Zu unterscheiden sind Verkaufsbewilligungen (von Schiesspulver, pyrotechnischen Gegenständen und von Sprengmitteln), Verwendungsbewilligungen und Erwerbsscheinbewilligungen (für Sprengmittel oder für pyrotechnische Gegenstände).
Da die Erwerbsscheine zum Erwerb während eines Jahres berechtigen, der gekaufte explosionsgefährliche Stoffe allerdings nicht während dieser Frist verbraucht werden muss, sondern auch nach Ablauf der Bewilligung gelagert und verwendet werden kann, ist die Regelung in Absatz 3 sachgerecht.

§ 37.
Die genannte Frist berechnet sich ab Meldedatum.

§ 38.
Damit soll sichergestellt werden, dass die Aufbewahrungsdauer gemäss § 28 PolDaVO nicht aus sachfremden Gründen verlängert wird.

§ 39.

Die Kürzung der ordentlichen Aufbewahrungsdauer um einen Drittel ist in den genannten Fällen die einzig sinnvolle Lösung, die Sinn und Zweck des polizeilichen Informationssystems gebührend berücksichtigt: Dieses will nämlich nicht Auskunft über die rechtskräftig ergangenen Schuldsprüche erteilen, wie dies vom zentralen Strafregister bezweckt wird, sondern lediglich Daten über möglichst sämtliche Personen und Fälle umfassen, gegen die einst polizeiliche Ermittlungen geführt worden sind. Selbst ein Freispruch vermag demnach unter Umständen keine sofortige Löschung aus dieser Datensammlung zu rechtfertigen.

§ 40.
Die Absätze 2 und 3 rechtfertigen sich, weil der Untersuchungsrichter gem. § 80 Abs. 1 und Art. 85 Abs. 3 StPO wegen der gleichen Sache erneut ein Strafverfahren eröffnen kann. Die bereits erfassten Daten können demnach in einem späteren Verfahren zur Aufklärung von Straftaten geeignet und erforderlich sein. Diese Regelungen tragen dem zweifellos bestehenden überwiegenden Fahndungsinteresse Rechnung: Bei einem Freispruch hinsichtlich verschiedener schwerer Sittlichkeitsdelikte, der beispielsweise bloss wegen Zurechnungsunfähigkeit oder Verjährung erfolgte, oder bei einer Nichteintretens- oder Einstellungsverfügung, die erfolgen musste, weil das Verhalten in der Phase der straflosen Vorbereitung stehen geblieben war, ist die weitere Bearbeitungsmöglichkeit dieser Daten geboten. Da der Zugang auf diese Daten auf die Kantonspolizei beschränkt ist, die Zugriffsberechtigung limitiert und das Amtsgeheimnis zudem strikte beachtet wird, werden die Interessen der Betroffenen gebührend berücksichtigt.

§ 43.
Sowohl die organisatorischen und technischen Massnahmen als auch die einzuführende Protokollierung sind gemäss § 22 InfoDV innert zweier Jahre nach Inkrafttreten der InfoDV zu treffen bzw. einzuführen.

2. Beschluss

(Siehe nächste Seite)

Verordnung über die polizeiliche Datenerhebung, -bearbeitung und -speicherung (PolDaVO)

RRB Nr. 2003/608 vom 1. April 2003

Der Regierungsrat des Kantons Solothurn
gestützt auf Artikel 8 Absatz 2 und Artikel 11 Absatz 3 der Kantonsverfassung vom 8. Juni 1986[1]), §§ 33, 40 und 41 des Gesetzes über die Kantonspolizei vom 23. September 1990[2]) und auf das Informations- und Datenschutzgesetz vom 21. Februar 2001[3])

beschliesst:

I. Allgemeiner Teil

A. Gegenstand, Zweck, Geltungsbereich und Zuständigkeit

§ 1. Gegenstand und Zweck

[1] Diese Verordnung regelt
a) die Bearbeitung und Speicherung
b) den Zugriff und Anspruch auf Berichtigung, Ergänzung und Nachführung
c) die Aufbewahrung und Löschung
von Personendaten und besonders schützenswerten Personendaten in den Datensammlungen der Kantonspolizei, einschliesslich der dazugehörigen Dokumente.
[2] Sie bezweckt, diese Daten dem Informations- und Datenschutzgesetz[4]) entsprechend zu schützen und zu sichern.

§ 2. Definitionen

[1] Für die Begriffe Personendaten und besonders schützenswerte Personendaten gelten die Definitionen gemäss Informations- und Datenschutzgesetz[5]).
[2] Der Begriff Daten in dieser Verordnung umfasst sowohl die Personendaten wie die besonders schützenswerten Personendaten.

§ 3. Sachlicher Geltungsbereich

[1] Diese Verordnung gilt für sämtliche von der Kantonspolizei geführten Datensammlungen.
[2] Die Bestimmungen des Informations- und Datenschutzgesetzes[6]) bleiben vorbehalten.

§ 4. Persönlicher Geltungsbereich

Dieser Verordnung unterstehen alle Mitarbeitenden der Kantonspolizei und allfällige Mitarbeitende anderer Polizeien, die ermächtigt sind, auf Daten im Sinne dieser Verordnung zu zugreifen.

§ 5. Zuständigkeit

[1]) BGS 111.1.
[2]) BSG 511.11.
[3]) BGS 114.1.
[4]) BGS 114.1.
[5]) BGS 114.1.
[6]) BGS 114.1.

[1] Der Kommandant oder die Kommandantin ist für die Aufgaben gemäss § 24, §§ 26–29 und §§ 34 ff. des Informations- und Datenschutzgesetzes[1]) zuständig.

[2] Er oder sie kann diese und die weiteren ihm gemäss dieser Verordnung zugewiesenen Aufgaben an die Abteilungschefs delegieren.

[1]) BGS 114.1.

§ 6. Schutz vor Missbrauch

[1] Die Daten sind durch Regelung der Zugriffs-, Abfrage- und Eingabeberechtigung zu schützen, insbesondere vor unbefugter Kenntnisnahme, Bearbeitung, Verwendung, Löschung und Entwendung.
[2] Der Kommandant oder die Kommandantin erlässt bezüglich der Einzelheiten Weisungen.

§ 7. Bauliche Sicherheit

Der Kommandant oder die Kommandantin sorgt dafür, dass Terminals, worin Daten gespeichert sind, samt zugehörigen Registraturen und Akten in Räumen untergebracht werden, die gegen den Zutritt Unbefugter gesichert sind.

B. Grundsätze der Datenbearbeitung und Zugriffsberechtigung

§ 8. Qualität der Daten

Es dürfen nur Daten aufbewahrt werden, die zur Verhinderung oder Aufklärung von Straftaten oder für administrative Bewilligungsverfahren erheblich, notwendig und geeignet sind.

§ 9. Zugriffsberechtigung

[1] Der Kommandant oder die Kommandantin erteilt die Zugriffsberechtigungen und muss sie visieren.
[2] Die Zugriffsberechtigung wird Mitarbeitenden der Kantonspolizei erteilt, die dem Amtsgeheimnis unterstehen und zur Erfüllung ihrer gesetzlichen Aufgaben auf die aufbewahrten Daten angewiesen sind.
[3] Unter den gleichen Voraussetzungen kann der Kommandant oder die Kommandantin Mitarbeitenden anderer Polizeien die Zugriffsberechtigung erteilen.

§ 10. Zugriffsberechtigung der Stadtpolizeien

[1] Die Kantonspolizei kann den städtischen Polizeikorps den Zugriff auf kantonale Informationssysteme genehmigen, sofern diese für die Einhaltung der in dieser Verordnung festgelegten Bestimmungen Gewähr bieten.
[2] Die Zugriffsberechtigung wird nur denjenigen Mitarbeitenden städtischer Polizeikorps erteilt, die dem Amtsgeheimnis unterstehen und zur Erfüllung ihrer gesetzlichen Aufgaben auf die aufbewahrten Daten angewiesen sind.
[3] In jedem Fall beschränkt sich ihre Zugriffsberechtigung auf Grund- und Haftdaten sowie auf fallbezogene Daten.
[4] Der Kommandant oder die Kommandantin kann den Zugriff im Einzelfall weiter einschränken.

C. Rechte der betroffenen Personen

§ 11. Auskunfts- und Einsichtsrecht

Das Auskunfts- und Einsichtsverfahren sowie die diesbezügliche Ausnahmeregelung richtet sich nach § 26 des Informations- und Datenschutzgesetzes[1]).

§ 12. Nachführung der Einträge

[1] Wer in einer Datensammlung der Kantonspolizei registriert ist, kann schriftlich das Gesuch stellen, dass im System die Bemerkung „Nichteintreten“, „Verfahren eingestellt“ oder „Freispruch“ aufgenommen wird. Die Kantonspolizei teilt den Entscheid darüber schriftlich mit.

[1]) BGS 114.1.

[2] Dem Gesuch wird stattgegeben, wenn ein entsprechender Entscheid der zuständigen Stelle vorgelegt wird.

[3] Nichteintretensentscheide und Verfahrenseinstellungen des kantonalen Untersuchungsrichteramtes werden von Amtes wegen eingetragen.

D. Zugang zu amtlichen Dokumenten

§ 13. Zugang zu amtlichen Dokumenten

Der Zugang zu amtlichen Dokumenten und die entsprechenden Ausnahmeregelungen richten sich nach §§ 12ff., §§ 34ff. und 40 des Informations- und Datenschutzgesetzes[1]).

§ 14. Amtshilfe

Für die Bekanntgabe von Daten bei Amtshilfe gilt § 42 des Gesetzes über die Kantonspolizei[2]).

§ 15. Auskünfte an Dritte

Auskünfte werden nur an Dritte erteilt, die einen genügenden Rechtsnachweis erbringen.

E. Allgemeine Löschungsregel

§ 16. Grundsatz

[1] Daten werden nur solange aufbewahrt, wie die Kantonspolizei diese zur Erfüllung ihrer Aufgaben, insbesondere zu Sicherungs- oder Beweiszwecken, benötigt.

[2] Vorbehalten bleibt die in dieser Verordnung oder in den entsprechenden Dienstbefehlen festgelegte Aufbewahrungsdauer.

§ 17. Löschung der Daten

Nach Ablauf der in dieser Verordnung beziehungsweise im entsprechenden Dienstbefehl festgelegten Aufbewahrungsdauer werden die Daten gelöscht.

II. Besonderer Teil: Das polizeiliche Informationssystem ABI und erkennungsdienstliche Datensammlungen

A. Gespeicherte Daten

§ 18. Die gespeicherten Daten

Im Informationssystem der Kantonspolizei werden insbesondere folgende Daten aufbewahrt:

a) Grunddaten;

b) Erkennungsdienstliche Daten, inkl. Arrestantenfotografien;

c) Haftdaten;

d) Fallbezogene Daten;

e) Waffen- und Sprengstoffdaten;

f) Journal-Daten.

§ 19. Grunddaten

[1] Als Grunddaten einer natürlichen Person werden erfasst:

a) Name und Vorname;

b) Aliasname(n) und Spitzname(n);

c) Geburtsdatum und Geburtsort;

[1]) BGS 114.1.
[2]) BGS 511.11.

d) Heimatorte/Staatsangehörigkeit(en);
e) Status bei ausländischer Staatsangehörigkeit;
f) Geschlecht;
g) Adresse;
h) Namen und Vornamen der Eltern;
i) Zivilstand sowie Name und Vorname des Ehegatten bzw. des geschiedenen Ehegatten;
j) Beruf;
k) Verbindungen.
[2] Grunddaten juristischer Personen sind sämtliche Daten, welche die juristische Person gemäss der obligationenrechtlichen Bestimmungen kennzeichnen.

§ 20. Voraussetzungen zur Bearbeitung von Grunddaten

[1] Grunddaten dürfen nur im Zusammenhang mit erkennungsdienstlichen Daten, Haftdaten, fallbezogenen Daten oder Waffen- bzw. Sprengstoffdaten bearbeitet werden.
[2] Ebenso ist eine Bearbeitung von Grunddaten nur zulässig, wenn Leumundsberichte oder andere polizeiliche Rapporte über die betroffene Person, insbesondere im Zusammenhang mit aussergewöhnlichen Todesfällen, verfasst worden sind.

§ 21. Erfassen und Bearbeiten von Grunddaten von Personen mit grosser Gewaltbereitschaft

[1] Die Kantonspolizei ist berechtigt, Grunddaten über Personen zu erfassen und zu bearbeiten, bei denen infolge ihres Verhaltens oder ihrer Aeusserungen eine hohe Gewaltbereitschaft anzunehmen ist.
[2] Die Erfassung der Grunddaten und deren Bearbeitung bedarf der ausdrücklichen Bewilligung des Kommandanten oder der Kommandantin.

§ 22. Erkennungsdienstliche Daten

Als erkennungsdienstliche Daten werden erfasst:
a) Behandlungsstelle, Behandlungsdatum;
b) Ausweisdaten;
c) Foto der betroffenen Person inkl. Nummer und Aufnahmedatum;
d) Identität (Signalement, besondere Merkmale, Daktyloskopie und Wangenschleimhaut-Abstrich);
e) Behandlungsgrund.

§ 23. Haftdaten

[1] Haftdaten sind Angaben über Personen, die verhaftet oder vorläufig festgenommen sind oder sich in einer kantonalen Vollzugsanstalt befinden. Sie werden erfasst, sofern die Kantonspolizei davon Kenntnis erhält.
[2] Als Haftdaten werden erfasst:
a) Eintrittsort und Eintrittsdatum;
b) Haft-Art;
c) Austrittsdatum und Austrittsgrund;
d) Die für die Einweisung zuständige Behörde;
e) Delikt.

§ 24. Fallbezogene Daten

[1] Fallbezogene Daten sind Angaben über eine versuchte oder begangene Straftat oder über strafbare Vorbereitungshandlungen gemäss Art. 260[bis] StGB[1]) und weitere Angaben aus Strafanzeigen und Rapporten der Polizei.

[2] Als fallbezogene Daten werden erfasst:

a) Ereignis;

b) Ort und Zeit;

c) Sachverhalt;

d) Tatvorgehen;

e) Geschädigte;

f) Spuren;

g) Deliktsgut und Sachschaden;

h) Verbindungen zu artgleichen Ereignissen;

i) Fahrzeuge.

[1]) Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB; SR 311.0).

§ 25. Waffen- und Sprengstoffdaten

[1] Daten über Inhaber und Inhaberinnen einer Bewilligung von Waffen- und Waffentragscheinen sowie einer Bewilligung gemäss des Bundesgesetzes über explosionsgefährliche Stoffe werden[1]) werden im ABI-Modul „Waffen" bearbeitet.

[2] Falls eine erfasste Person auch in einem anderen ABI-Modul (Personen- oder Fallmodul) verzeichnet ist, wird darauf mit der Bemerkung „Waffe" bzw. „Sprengstoff" hingewiesen.

§ 26. Journal-Daten

[1] Journal-Daten sind Angaben über Ereignisse, die der Kantonspolizei gemeldet werden oder ihr in Ausübung ihrer Tätigkeit zur Kenntnis gelangen.

[2] Als Journal-Daten werden erfasst:

a) Empfänger oder Empfängerin einer Meldung;
b) Meldedatum und -zeit;
c) Sachbearbeiter oder Sachbearbeiterin der Kantonspolizei;
d) Ereignis;
e) Ereignisdatum/-zeit;
f) Ereignisort;
g) Sachverhalt;
h) Massnahmen / Anordnungen;
i) Personendaten des Melders oder der Melderin, des oder der Geschädigten, des oder der Beschuldigten sowie des Finders oder der Finderin;
j) Fahrzeuge.

B. Berechtigung zur Weiterbearbeitung

§ 27. Berechtigung zur Weiterbearbeitung

Der Kommandant oder die Kommandantin bezeichnet einzelne Mitarbeitende der Kantonspolizei, die zur Weiterbearbeitung der aufbewahrten Daten berechtigt sind.

C. Aufbewahrungsdauer und Löschungsregel

1. Abschnitt: Ordentliche Aufbewahrungsdauer

§ 28. Ordentliche Aufbewahrungsdauer der Grunddaten: Grundsatz

[1] Grunddaten, die mit einem Fall in Beziehung stehen, bleiben bis zum Ablauf der deliktspezifischen Aufbewahrungsdauer gemäss Absatz 2 im polizeilichen Informationssystem.

[2] Die deliktsspezifische Aufbewahrungsdauer beträgt:

a) 80 Jahre für unverjährbare Verbrechen gemäss Art. 75^{bis} StGB[2]);
b) 30 Jahre für Taten, die mit lebenslänglichem Zuchthaus bedroht sind;
c) 15 Jahre für Taten, die mit Zuchthaus bedroht sind;
d) 10 Jahre für Taten, die mit Gefängnis bedroht sind;
e) 4 Jahre für Taten, die mit Haft oder Busse bedroht sind.

[1]) Bundesgesetz über explosionsgefährliche Stoffe vom 25. März 1997 (Sprengstoffgesetz; SR 941.41).
[2]) Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB; SR 311.0).

[3] Vorbehalten bleibt die Verkürzung der ordentlichen Aufbewahrungsdauer gemäss § 39 dieser Verordnung.

§ 29. Ordentliche Aufbewahrungsdauer der Grunddaten: Ausnahmen

[1] Die Grunddaten natürlicher Personen werden spätestens mit dem Tod der betroffenen Person gelöscht.

[2] Die Grunddaten juristischer Personen werden spätestens mit deren Auflösung bzw. mit Löschung des Handelsregistereintrags gelöscht, soweit die Kantonspolizei davon Kenntnis erhält.

§ 30. Bei mehrmaliger Registrierung

Ist eine Person mit mehreren Delikten erfasst, so bleiben die Einträge zu allen Delikten so lange im polizeilichen Informationssystem aufbewahrt, bis die Aufbewahrungsdauer für dasjenige Delikt, das am längsten registriert bleibt, abgelaufen ist.

§ 31. Grunddaten, die keinen Bezug zu einem Fall haben

[1] Beziehen sich Daten auf Berichte, die im Zusammenhang mit einem administrativen Bewilligungsverfahren erstellt worden sind, werden sie nach 5 Jahren gelöscht.
Falls die betroffene Person in diesem Zeitpunkt noch im Besitz einer entsprechenden Bewilligung ist, bleiben die Daten um weitere 5 Jahre registriert.
Sie werden spätestens 5 Jahre nach Ablauf der Bewilligung oder nach Erreichen des 80. Altersjahres bzw. nach dem Tod der betroffenen Person gelöscht.
[2] Bei aussergewöhnlichen Todesfällen werden die Grunddaten nach Ablauf von 20 Jahren ab Todesdatum gelöscht.
[3] Grunddaten von Personen, die gemäss § 21 dieser Verordnung bearbeitet worden sind, werden unverzüglich gelöscht, wenn die Gründe der Bearbeitung weggefallen sind. Sie werden spätestens mit dem Tod der betroffenen Person gelöscht.

§ 32. Aufbewahrungsdauer der erkennungsdienstlichen Daten und des erkennungsdienstlichen Materials

[1] Erkennungsdienstliche Daten über eine Person werden gelöscht und das entsprechende erkennungsdienstliche Material wird vernichtet:
a) sobald sie im Laufe des Verfahrens als Täter oder als Täterin ausgeschlossen werden kann;
b) wenn sie das 80. Altersjahr erreicht hat;
c) nach ihrem Tod;
d) nach 30 Jahren, ausser wenn sie während dieser Zeit erneut wegen eines Verbrechens oder eines Vergehens verzeigt worden ist. In diesem Fall werden sie spätestens nach 50 Jahren gelöscht.

[2] Vorbehalten bleibt die Verkürzung der ordentlichen Aufbewahrungsdauer gemäss § 40.
[3] Die Löschung der erkennungsdienstlichen Daten, welche den Wangenschleimhaut-Abstrich betreffen, richtet sich nach der Bundesgesetzgebung[1]).
[4] Die Löschung erkennungsdienstlichen Materials, welches in Datensammlungen des Bundes aufbewahrt wird, richtet sich nach der Bundesgesetzgebung[2]).

§ 33. Aufbewahrungsdauer der Haftdaten

Haftdaten werden zusammen mit den Grunddaten gelöscht.

§ 34. Aufbewahrungsdauer der fallbezogenen Daten

[1] Beziehen sich die Daten auf einen Fall, bei dem die Täterschaft ermittelt werden konnte, so werden sie nach 10 Jahren gelöscht. Falldaten bezüglich Straftaten, die mit Haft oder Busse bedroht sind, werden nach 4 Jahren gelöscht.
[2] Beziehen sich die Daten auf einen Fall, bei dem die Täterschaft nicht ermittelt werden konnte, so werden sie nach 15 Jahren gelöscht. Falldaten bezüglich Straftaten, die mit Haft oder Busse bedroht sind, werden nach 10 Jahren gelöscht.

[1]) Verordnung über das DNA-Profil-Informationssystem vom 31. Mai 2000 (EDNA-Verordnung; SR 361.1).
[2]) Verordnung über die Bearbeitung erkennungsdienstlicher Daten vom 21. November 2001 (SR 361.3).

[3] Bei schweren Straftaten können die Daten mit Zustimmung des Kommandanten oder der Kommandantin um weitere 10 Jahre aufbewahrt werden, insbesondere wenn für eine längere Registrierung wichtige öffentliche Interessen vorliegen.

§ 35. Sonderfälle

Zu Schulungszwecken dürfen geeignete Fälle wie beispielsweise Flugzeugunfälle und Mordfälle in anonymisierter Form und mit Zustimmung des Kommandanten oder der Kommandantin auf unbestimmte Zeit aufbewahrt werden.

§ 36. Aufbewahrungsdauer der Waffen- und Sprengstoffdaten

[1] Die Daten der Waffen- und Waffentragscheinbesitzer und – besitzerinnen werden bis zu deren Tod oder bis zur Weiterveräusserung bzw. Weitergabe der Waffe aufbewahrt, sofern die Kantonspolizei davon Kenntnis erhält. Im Zeitpunkt der Löschung muss auch die Bemerkung „Waffe“ in den anderen Modulen gelöscht werden.

[2] Die Daten des Inhabers oder der Inhaberin einer Verkaufsbewilligung von Sprengmitteln oder pyrotechnischen Gegenständen werden bis zum Erlöschen der Bewilligung beziehungsweise bis zu deren Tod aufbewahrt. Im Zeitpunkt der Löschung wird auch die Bemerkung „Sprengstoff“ in den anderen Modulen gelöscht.

[3] Die Daten des Inhabers oder der Inhaberin eines Sprengmittelerwerbsscheins bleiben während 10 Jahren nach Ablauf dieser Bewilligung aufbewahrt, es sei denn, der Inhaber oder die Inhaberin erbringe den Nachweis, dass sämtliche einst erworbenen Sprengmittel vollständig verbraucht sind. Spätestens mit dem Tod des Inhabers oder der Inhaberin werden die Daten gelöscht. Im Zeitpunkt der Löschung muss auch die Bemerkung „Sprengstoff“ in den anderen Modulen gelöscht werden.

§ 37. Aufbewahrungsdauer der Journal-Daten

Die Journal-Daten werden nach 10 Jahren gelöscht.

§ 38. Verbot der Kumulation

Ist eine Person im Zusammenhang mit einer Straftat im polizeilichen Informationssystem verzeichnet und gleichzeitig auch, weil sie um eine Bewilligung ersucht hat, so dürfen die jeweils geltenden Aufbewahrungsfristen nicht kumuliert werden.

2. Abschnitt: Verkürzung der ordentlichen Aufbewahrungsdauer

§ 39. Grunddaten, Haftdaten und fallbezogene Daten

Die ordentliche Aufbewahrungsfrist der Grunddaten sowie der Haft- und der fallbezogenen Daten wird um einen Drittel gekürzt, wenn einem Gesuch um Nachführung nach § 11 dieser Verordnung entsprochen wurde.

§ 40. Erkennungsdienstliche Daten und erkennungsdienstliches Material

[1] Auf Gesuch hin werden erkennungsdienstliche Daten gelöscht und das erkennungsdienstliche Material vernichtet, wenn:

a) das Nichteintreten verfügt wird;
b) das betreffende Verfahren mit einem rechtskräftigen Freispruch abgeschlossen ist;
c) 5 Jahre nach Einstellung des Verfahrens;
d) 10 Jahre nach Ablauf der Probezeit bei bedingtem Strafvollzug;
e) 20 Jahre nach der Entlassung aus einer Freiheitsstrafe oder Verwahrung oder nach dem Vollzug einer therapeutischen Massnahme.

[2] In den Fällen nach Absatz 1 Buchstabe a, b und c werden die Daten nicht gelöscht und können noch während höchstens 10 Jahren bearbeitet werden, wenn der Freispruch oder die Verfahrenseinstellung wegen Schuldunfähigkeit des Täters oder der Täterin erfolgte oder wenn zu erwarten ist, dass die Daten der Aufdeckung künftiger Straftaten dienen könnten.

[3] In den Fällen nach Absatz 1 Buchstabe d und e werden die Daten nicht gelöscht, wenn der konkrete Verdacht auf ein nicht verjährtes Verbrechen oder Vergehen nicht ausgeräumt oder eine Wiederholungstat zu befürchten ist.

[4] Das Verfahren richtet sich nach §§ 11 und 12 dieser Verordnung.

[5] Für die Löschung der Daten, welche den Wangenschleimhaut-Abstrich und das erkennungsdienstliche Material des Bundes betreffen, ist die Bundesgesetzgebung verbindlich[1)] [2)].

D. Folgen der Datenlöschung

§ 41. Vernichtung der Akten

[1] Spätestens mit der Löschung der Grunddaten müssen auch sämtliche Akten vernichtet werden. Bezüglich der Vernichtung des erkennungsdienstlichen Materials bleiben die §§ 32 und 40 vorbehalten.
[2] Der Kommandant oder die Kommandantin kann in Absprache mit dem oder der Beauftragten für Information und Datenschutz Ausnahmen bewilligen, wenn stichhaltige Gründe vorliegen, dass sich die Akten zu einem späteren Zeitpunkt als wesentlich für die Verfolgung wichtiger öffentlicher Interessen erweisen könnten.
[3] Die Weisungen für das Staatsarchiv bleiben vorbehalten[3)].

§ 42. Bescheinigung

Auf Antrag hin wird sowohl die Datenlöschung als auch die Vernichtung der entsprechenden Akten schriftlich bestätigt.

E. Datensicherheit

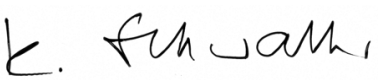
§ 43. Datensicherheit

[1] Der Kommandant oder die Kommandantin trifft die für die Gewährleistung der Datensicherheit technischen und organisatorischen Massnahmen im Sinne von § 16 Abs. 1 lit. c des Informations- und Datenschutzgesetzes[4)] und § 12f der Informations- und Datenschutzverordnung[5)].
[2] Jede Bearbeitung von Daten im polizeilichen Informationssystem ABI ist in einem Protokoll festzuhalten.

III. Inkrafttreten

§ 44. Inkrafttreten

[1] Der Regierungsrat bestimmt das Inkrafttreten.
[2] Vorbehalten bleibt das Einspruchsrecht des Kantonsrates.



Dr. Konrad Schwaller
Staatsschreiber

[1)] Verordnung über das DNA-Profil-Informationssystem vom 31. Mai 2000 (EDNA-Verordnung; SR 361.1).
[2)] Verordnung über die Bearbeitung erkennungsdienstlicher Daten vom 21. November 2001 (SR 361.3).
[3)] Weisungen für das Staatsarchiv (RRB vom 11. August 1992; BGS 122. 581).
[4)] BGS 114.1.
[5)] BGS 114.2.

Verteiler RRB

Staatskanzlei (SAN, Einleitung Einspruchsverfahren)
GS
BGS
Parlamentsdienste
Fraktionspräsidenten (4)
Amt für Justiz, Kant. Datenschutzbeauftragter
Amt für Informatik
Kantonspolizei
Stadtpolizeien von Solothurn, Olten und Grenchen
Präsidien der Einwohnergemeinden

Veto Nr. 5 Ablauf der Einspruchsfrist: 26. Juni 2003.

Verteiler Verordnung

Kantonaler Datenschutzbeauftragter (10)
Kantonspolizei (40)