

**Gericht**

Verfassungsgerichtshof

**Entscheidungsdatum**

16.12.2009

**Geschäftszahl**

B298/09

**Sammlungsnummer**

\*\*\*\*\*

**Leitsatz**

Keine Verletzung verfassungsgesetzlich gewährleisteter Rechte durch Abweisung des Antrags auf vorzeitige Löschung personenbezogener, für Zwecke der Strafverfolgung ermittelter Daten im Kopienakt und im EDV-System PAD nach Einstellung des Strafverfahrens wegen Sexualdelikten

**Spruch**

Der Beschwerdeführer ist durch den angefochtenen Bescheid weder in einem verfassungsgesetzlich gewährleisteten Recht noch wegen Anwendung einer rechtswidrigen generellen Norm in seinen Rechten verletzt worden.

Die Beschwerde wird abgewiesen.

**Begründung****Entscheidungsgründe:**

I. 1. Die Bundespolizeidirektion Wien erstattete im April 2007 gegen den Beschwerdeführer nach Durchführung von Ermittlungen im Dienste der Strafjustiz bei der Staatsanwaltschaft Wien Strafanzeige wegen des Verdachts der Vergehen der pornographischen Darstellung Minderjähriger nach §207a StGB (idF BGBl. I 15/2004) sowie des sexuellen Missbrauchs von Jugendlichen nach §207b StGB (idF BGBl. I 134/2002). Die Staatsanwaltschaft Wien legte die Anzeige nach veranlassten gerichtlichen Vorerhebungen im September 2007 ("aus Beweisgründen") gemäß §90 Abs1 StPO (in der damals geltenden Fassung) zurück, weshalb das Verfahren vom Untersuchungsrichter des Landesgerichtes für Strafsachen Wien eingestellt wurde.

Im März 2008 beehrte der Beschwerdeführer bei der Bundespolizeidirektion Wien die Löschung sämtlicher zu seiner Person im Zusammenhang mit den sicherheitsbehördlichen Ermittlungen (automationsunterstützt oder nicht automationsunterstützt) verarbeiteten Daten, insbesondere im kriminalpolizeilichen Akt, in den Allgemeinen Protokollen und in den entsprechenden Erhebungsakten, weil die Daten nicht mehr benötigt würden.

Mit Schreiben vom 8. Mai 2008 teilte die Bundespolizeidirektion Wien dem Beschwerdeführer mit, dass im so genannten Kriminalpolizeilichen Aktenindex (KPA) - zufolge umgehender Löschung nach Bekanntwerden der Verfahrenseinstellung von Amts wegen - keine ihn betreffenden Daten mehr verarbeitet würden; Daten, die im unstrukturierten Erhebungsakt enthalten sind, unterlägen nicht dem Löschungsrecht; die in der Datenanwendung "Allgemeine Protokolle" gespeicherten Daten würden zur Wiederauffindung des Kopienaktes sowie zur Dokumentation behördlichen Handelns "jedenfalls auf Dauer der Aufbewahrung einer Aktenkopie (fünf Jahre)" noch benötigt.

2. Die vom Beschwerdeführer gegen die Verweigerung der Löschung bei der Datenschutzkommission (DSK) gemäß §31 Abs2 Datenschutzgesetz 2000 (DSG 2000) erhobene Beschwerde vom 26. Mai 2008 wurde

mit Bescheid vom 21. Jänner 2009 abgewiesen. Begründend führte die DSK im Wesentlichen aus, dass sich der Antrag auf Löschung der Daten auf einen (nicht strukturierten) Papierakt (Kopienakt), einen inhaltlich teils identischen, im EDV-System mit der technischen Bezeichnung PAD ("Protokollieren-Anzeigen-Dateien") - Version 2.0 - gespeicherten Text (mit Bezug auf einen "Kurzschverhalt", der Rolle des Betroffenen, den Tatverdacht, die befassten Behörden und allenfalls den Verfahrensausgang) sowie auf die im Kanzleiindexteil des PAD enthaltenen (der Aktenauffindung dienenden) "äußeren" Verfahrensdaten (Identitäts-, Adress- und Kontaktdaten) beziehe.

Ein Lösungsanspruch bestehe hinsichtlich des Papieraktes nicht, weil diesem die Dateiqualität iSd §4 Z6 DSG 2000 fehle.

Im PAD würden zwar seit Umstellung der Software auf die Vollversion 2.0 im Dezember 2006 nicht mehr ausschließlich "äußere", sondern auch "innere" personenbezogene Verfahrensdaten (gescannte Dokumente, Textdokumente über Einvernahmen, Aktenvermerke etc.) gespeichert. Die vom Beschwerdeführer behauptete "Sensibilität" strafrechtsrelevanter Ermittlungsdaten gemäß §4 Z2 DSG 2000 im Zusammenhang mit den hier aktuellen Sexualdelikten könne im Fall einer Verfahrensbeendigung durch Einstellung allerdings nicht anders beurteilt werden als bei Straftatbeständen ohne Sexualbezug. Die vom Verfassungsgerichtshof zur Löschungspflicht iZm Daten betreffend den speziellen - wegen Verfassungswidrigkeit aufgehobenen (und in der Folge entfallenen) - Tatbestand des §209 StGB entwickelte Rechtsprechung lasse sich nicht verallgemeinernd auf andere, dem Rechtsbestand weiterhin angehörende Delikte (einschließlich solcher mit sexueller Relevanz) ausdehnen. Die (Weiter)Verarbeitung personenbezogener Daten im PAD nach Verfahrensbeendigung sei nach der Judikatur des Verfassungsgerichtshofes nicht dem inneren Dienst gemäß §13 Sicherheitspolizeigesetz (SPG) zuzurechnen, weil damit Rechtspositionen des Beschwerdeführers gestaltet würden; eine Lösungsverpflichtung hinsichtlich der in Rede stehenden Daten sei zum gegenwärtigen Zeitpunkt indes zu verneinen, weil sich der Bedarf an der Verfahrensdokumentation in Anbetracht der Möglichkeit einer Wiedereröffnung des Strafverfahrens, aber auch unter dem Aspekt der gesetzlichen Vorschriften über die nachprüfende Kontrolle des konkreten Verwaltungshandelns ergebe.

Im Einzelnen führte die belangte Behörde hiezu aus (Kursivtext im Original):

"Nach §6 Abs1 Z5 DSG 2000 dürfen 'Daten nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben'.

Die Datenschutzkommission ist der Ansicht, dass es im Sinne des §6 Abs1 Z5 DSG 2000 einer 'besonderen gesetzlichen Vorschrift' über die Aufbewahrungsdauer jedoch im vorliegenden Fall nicht bedarf, da schon 'die Erreichung der Zwecke, für die (die Daten) ermittelt wurden' eine Aufbewahrung der Verfahrensdokumentation über die Verfahrensdauer hinaus erfordert.

Entscheidend ist hiebei, dass auch Verfahren, die zur Einstellung oder zum Freispruch geführt haben, unter Umständen nach ihrem Abschluss wieder eröffnet werden können (vgl. insbes. das XX. Hauptstück der StPO 'Von der Wiederaufnahme und der Erneuerung des Strafverfahrens sowie der Wiedereinsetzung in den vorigen Stand' und auch das 10. Hauptstück über die 'Einstellung, Abbrechung und Fortführung des Ermittlungsverfahrens'). Schon dies setzt augenfällig voraus, dass eine Dokumentation über den bisherigen Verfahrensverlauf in jedem Fall auch nach dem Verfahrensabschluss noch vorhanden sein muss.

Auch würde die Behauptung des Beschwerdeführers, wonach das bloße Vorhandensein von Verfahrensdokumentation die Geltung der Unschuldsvermutung für ihn gefährde - konsequent durchdacht - dazu führen müssen, dass nicht nur die Akten über kriminalpolizeiliche Ermittlungen bei den Sicherheitsbehörden, sondern auch alle Akten nach Einstellungen oder Freisprüchen bei den Strafgerichten umgehend zu vernichten wären. Damit ginge aber auch jeder Nachweis eines erfolgten Freispruchs verloren, was nicht im Interesse des Betroffenen sein kann. Diese Nachweisbarkeit der 'Unschuld' ist vom Zweck des Strafverfahrens mitumfasst, da hiebei ja nicht nur alles zu berücksichtigen ist, was die Schuld des Verdächtigen nachweisen könnte, sondern auch alles, was seine Unschuld beweist. Tatsache ist jedenfalls, dass eine Vorgangsweise, wonach etwa Gerichtsakten im Falle eines Freispruchs des Angeklagten sofort zu vernichten wären, der österreichischen Rechtspraxis völlig fremd ist.

Vielmehr ist es - ganz abgesehen von einer möglicherweise notwendigen neuerlichen Verfahrensdurchführung - für einen Rechtsstaat unerlässlich, dass Dokumentation über staatliches Handeln in Aktenform mindestens so lange vorhanden ist, als die unterschiedlichen, zur Prüfung der Rechtmäßigkeit außerhalb von Rechtsmittel- und fristgebundenen Beschwerdeverfahren berufenen Institutionen ihre

Prüfkompetenz ausüben dürfen. Diese Aufbewahrung der Dokumentation über staatliches Handeln zum Zweck der Nachprüfbarkeit seiner Rechtmäßigkeit ist als vom 'Zweck der Ermittlung' mitgetragen anzusehen. Die Annahme einer Pflicht zur sofortigen Vernichtung der Verfahrensdokumentation nach Verfahrensbeendigung würde demgegenüber die Gefahr der Förderung von Rechtswillkür und Korruption in sich bergen, da Organwalter - und von ihnen begünstigte Außenstehende - die nachgängige Kontrolle von staatlichem Handeln auf seine Rechtmäßigkeit hin in weit geringerem Maße fürchten müssten als bisher. Gerade im Zusammenhang mit kriminalpolizeilichen Ermittlungen ist aber die nachgängige Überprüfbarkeit der Vorgangsweise der kriminalpolizeilichen Organwalter für die Effektivität eines Rechtsstaates von besonderer Bedeutung.

Dass eine Pflicht zur Aufbewahrung von Akten auch nach Verfahrensbeendigung in der österreichischen Rechtsordnung ganz generell als selbstverständliches Erfordernis in einem Rechtsstaat vorausgesetzt wird, ergibt sich im Übrigen auch aus zahlreichen gesetzlichen Bestimmungen. So wird etwa in den §§5 ff des Bundesarchivgesetzes, BGBl. I Nr. 162/1999 idGF, auf die Skartierung von Akten ausdrücklich Bezug genommen, d.h. auf die Praxis, dass Akten während einer gewissen, mehrere Jahre dauernden 'Skartierfrist' jedenfalls aufzubewahren sind, und erst dann darüber entschieden wird, ob sie vernichtet oder infolge Archivwürdigkeit dem Staatsarchiv zur dauernden Aufbewahrung übergeben werden. Auch sämtliche gesetzlichen Vorschriften über die nachprüfende Kontrolle des Verwaltungshandelns außerhalb von Rechtsmittel- oder fristgebundenen Beschwerdeverfahren, wie etwa die Tätigkeit der Volksanwaltschaft oder des Rechnungshofs - aber auch der Datenschutzkommission -, setzen voraus, dass Verfahrensdokumentation auch nach Abschluss von Verwaltungsverfahren für einen bestimmten Zeitraum noch vorhanden ist.

Zur Forderung des VfGH (vgl. z.B. Erk. B1581/03 v. 26.1.06 oder B 1590/03 v. 15.12.2005), dass speziell im Hinblick auf Akten-Suchhilfen zu begründen wäre, wieso nicht mit nichtpersonenbezogenen Dokumentationssuchhilfen das Auslangen gefunden werden könne (- und zumindest in den Suchbehelfen der Personenbezug 'gelöscht' werden könnte -), ist zu bemerken, dass gerade im Bereich der beschwerdegegenständlichen, d.h. auf §13 SPG gegründeten Dokumentationshilfen eine Beschränkung des Personenbezugs ohnehin verwirklicht ist, indem im PAD (- gleichgültig welcher Version -) die Möglichkeit eines Zugriffs nur mit Hilfe eines Namens nicht existiert. §13 Abs2 letzter Satz SPG verbietet ausdrücklich die Auswählbarkeit von Daten aus der Gesamtmenge der gespeicherten Daten nur nach dem Namen. Der PAD kann somit nicht in gleicher Weise wie etwa der kriminalpolizeiliche Aktenindex zur Überblicksgewinnung über frühere Fälle eines Verdachtes gegen eine bestimmte Person verwendet werden.

D. ...

Das Anliegen des Beschwerdeführers betrifft ... im Kern die Weiterverwendung von Verfahrensdaten für einen neuen - vom ursprünglichen Ermittlungszweck verschiedenen - Zweck, nämlich die Aufklärung anderer strafrelevanter Sachverhalte: Was der Beschwerdeführer unterbinden will, ist die Heranziehung der Dokumentation über bestimmte frühere Ermittlungsergebnisse zur Informationsgewinnung im Hinblick auf spätere, neue Vorfälle, die denselben Beschuldigten betreffen - eine Verwendung, die im Folgenden als 'Informationsrückgriff' bezeichnet werden soll.

Dass es tatsächlich notwendig sein sollte, zur Vermeidung eines derartigen Informationsrückgriffs die Dokumentation der Verfahrensdaten nach Verfahrensbeendigung umgehend zu löschen und dabei in Kauf zu nehmen, dass dadurch die Möglichkeit einer Wiedereröffnung oder der nachprüfenden Kontrolle der Rechtmäßigkeit eines Verfahrens vereitelt wird, wird von der Datenschutzkommission bestritten: Gerade seitdem das Handeln staatlicher Organe nahezu ausschließlich elektronisch dokumentiert wird, ist jeder Zugriff auf Verfahrensdokumentationsdaten kontrollierbar. Eine vom Gesetz nicht vorgesehene Weiterverwendung kann daher mit vernünftigen technischem und organisatorischem Aufwand unterbunden werden, sodass die Löschung generell nicht mehr als der einzige verlässliche Weg zur Vermeidung einer unerwünschten Weiterverwendung von Daten angesehen werden kann.

E. Im Übrigen hat auch der VfGH ausschließlich im Zusammenhang mit Verfahren betr. den wegen Grundrechtswidrigkeit aufgehobenen §209 StGB eine generelle Lösungsverpflichtung elektronischer Dokumentationsdaten ausgesprochen. Außerhalb des Problembereichs des aufgehobenen §209 StGB hat der VfGH die Zulässigkeit der Aufbewahrung strafrelevanter Daten für Zwecke des späteren Informationsrückgriffs bei neuerlichen strafrechtlichen Ermittlungen nicht generell verneint, sondern jeweils an eine vorhergehende Prüfung im Einzelfall unter Vornahme einer Interessensabwägung gebunden (vgl. etwa VfSlg. 16149).

..."

3. In der dagegen gemäß Art144 B-VG erhobenen Beschwerde wird die Verletzung in den verfassungsgesetzlich gewährleisteten Rechten auf Löschung unzulässigerweise verarbeiteter personenbezogener

Daten (§1 Abs3 Z2 DSG 2000), auf Achtung des Privatlebens (Art8 EMRK), auf Gleichbehandlung (Art2 StGG und Art7 B-VG) und auf eine wirksame Beschwerde (Art13 EMRK) geltend gemacht.

Der Beschwerdeführer bringt wörtlich vor (Hervorhebungen im Original):

"A. Allgemeine Protokolle (PAD)

...

Die den Bf betreffenden Daten werden nicht mehr benötigt.

Die Verfahrenseinstellung ist in Rechtskraft erwachsen. Es steht daher fest, daß der Bf niemals eine strafbare Handlung intendiert hatte, woran keine staatliche Behörde mehr Zweifel äußern darf (EGMR: Orr gg. Norwegen 2008; Asan Rushiti vs. A, 21.03.2000; Lamanna vs. A, 10.07.2001). Hat der Bf aber nie eine strafbare Handlung auch nur intendiert, so werden die Daten nicht mehr (weiter) benötigt (weder für sicherheitspolizeiliche noch für kriminalpolizeiliche Zwecke) (§63 SPG, §§74f StPO; §27 DSG 2000, §1 Abs3 Z. 2 DSG 2000), weshalb sie zu löschen sind.

Erfolgt diese Löschung nicht, so verletzt dies den Bf in seinen verfassungsgesetzlich gewährleisteten Rechten gem. §1 DSG und Art8 EMRK (EGMR: Amann vs. CH 16.02.2000, par. 78ff; Rotaru vs. ROM [GC], 04.05.2000; VfGH 16.03.2001, G94/00, B1117/99). In Fällen, in denen trotz Einstellung infolge erwiesener Unschuld eine kriminelle Energie und damit eine weitere Gefahr konstatiert werden kann (freiwilliger Rücktritt vom Versuch, absolut untauglicher Versuch, Unzurechnungsfähigkeit, Unmündigkeit u.ä.), werden die Daten weiter benötigt und ist eine weitere Speicherung gerechtfertigt. Das ist aber beim Bf, der niemals einen Straftatbestand (zu dem alle objektiven und subjektiven Tatmerkmale gehören) setzen wollte, nicht der Fall. Deshalb wurden seine Vormerkungen ja auch bspw. aus dem KPA entfernt.

Die Ansicht, daß die Weiterverarbeitung der Daten notwendig sei (wohl für allfällige künftige gerichtliche Vorerhebungen; wofür sonst?; Dokumentation ist ja kein Selbstzweck) ..., ist mit den verfassungsgesetzlich gewährleisteten Rechten des Bf unvereinbar (§1 DSG 2000, Art6 (2), 8, 14 EMRK; Art7 B-VG, Art2 StGG), darf der völlig unschuldige Bf doch nicht lediglich deshalb gegenüber anderen völlig unschuldigen Staatsbürgern, die ebenfalls niemals eine strafbare Handlung intendierten und niemals vertretbaren Verdacht auf sich zogen, (durch Vorrätighalten seiner Daten für allfällige künftige Strafverfahren, in denen diese Daten dann zu seinem Nachteil Verwendung finden) benachteiligt werden, weil er - anders als die anderen völlig unschuldigen Bürger - das Pech hatte, unschuldig in Verdacht zu geraten und unschuldig angezeigt zu werden (vgl. die obigen Judikaturnachweise).

Werden die Daten nicht mehr benötigt, so ... sind die Daten zu löschen:

'Über die Verpflichtung zur Aktualisierung der ... Daten hinaus besteht aber gemäß §63 Abs1 SPG auch eine Verpflichtung der Sicherheitsbehörden zur Löschung der entgegen den Bestimmungen des SPG ermittelten und gespeicherten Daten. ... §63 Abs1 SPG sieht vor, dass personenbezogene Daten zu löschen sind, sobald sie für die Erfüllung der Aufgabe, für die sie verwendet worden sind, nicht mehr benötigt werden, es sei denn, für ihre Löschung wäre eine besondere Regelung getroffen worden. ... Daher besteht ... dann die Verpflichtung zur Löschung der ... Daten, wenn die Speicherung als im Dienste der Strafrechtspflege nicht mehr erforderlich anzusehen ist.'

(VfGH 16.03.2001, G94/00)

Diese Lösungsverpflichtung ist auch durch die Notwendigkeit der Auffindbarkeit des Kopienaktes der sicherheitsbehördlichen Ermittlungen ... nicht ausgeschlossen, weil der Kopienakt selbst nicht mehr benötigt wird und daher zu vernichten (oder zumindest zu anonymisieren) ist (§63 SPG; §§74f StPO; §27 DSG 2000, §1 Abs3 Z. 2 DSG 2000). Ist schon die weitere (unanonymisierte) Aufbewahrung des Kopienaktes über die sicherheitsbehördlichen Vorerhebungen unzulässig, so gilt dies umsomehr für die Protokoll Daten, die der Auffindung dieses Kopienaktes dienen ... sowie für den im PAD vorrätig gehaltenen (mit dem Papierakt identen, allerdings elektronisch durchsuchbaren) elektronischen Akt (BS 7), zumal berechtigten Belangen der Kriminalstatistik auch durch anonymisierte Dokumentation der (bezüglichen) Aktenvorgänge Genüge getan werden kann.

Für allfällige Wiederaufnahmeverfahren, genügt (ebenso wie für die 'Nachvollziehbarkeit der Rechtmäßigkeit behördlichen Handelns' oder den Schutz des Bf vor weiteren identen Vorwürfen) der Gerichtsakt völlig. Der beschwerdegegenständliche polizeiliche Papierakt ist ja nur ein bei der Sicherheitsbehörde verbliebenes Duplikat.

Eine Lösungsverpflichtung der Polizeibehörden indiziert im übrigen auch nicht, wie von der bB behauptet (BS 12), eine solche Lösungsverpflichtung der Staatsanwaltschaften und Gerichte. Letztere sind im Gegensatz zu den Polizeibehörden nicht mit proaktiven präventiven Aufgaben betraut, weshalb sich die Grundrechtsproblematik nicht im selben Ausmaß stellt. Zudem folgt schon rein denklösig aus der Vernichtung überflüssiger Duplikate nicht, dass auch die Originale zu vernichten sind. Für die von der bB ins Treffen geführten Zwecke (Wiederaufnahme, Nachvollziehbarkeit der Rechtmäßigkeit, Schutz vor identen Vorwürfen) genügen die Originale bei Gericht und StA völlig. Der zusätzlichen Aufbewahrung von Kopien bei den Polizeibehörden ist dazu nicht erforderlich.

Die Daten im PAD wären daher zu löschen gewesen, und zwar zur Gänze, weil durch eine nur teilweise Löschung immer noch ein Personenbezug durch Einsicht in den Papier-Kopienakt hergestellt werden kann ... . So wie die Achtung des Privatlebens und Freiheit von Diskriminierung im Falle des §209 stellt auch die Unschuldsvermutung ein fundamentales Grundrecht dar, zumal auch Daten über strafrechtliche Verfolgungen sensible Daten sind.

Der VfGH hat daher völlig zurecht in VfGH 11.06.2007 (B1737/06) (wo es nicht um §209 StGB und nicht um ein menschenrechtswidriges Strafverfahren ging) vollinhaltlich auf die Judikatur zu Vormerkungen nach §209 StGB verwiesen.

...

Zusätzlich beinhalten die verfahrensgegenständlichen Daten im PAD auch sensible Daten (über das Sexualleben des Bf). In ... (= VfGH B1703/08) (der do. Bf wurde ebenfalls auf Grund eines Sexualdeliktes in ein Strafverfahren gezogen und erwies sich seine Unschuld) hat die bB noch ganz anders entschieden als im vorliegenden Fall:

...

Dabei lag in diesem anderen Fall, im Gegensatz zu dem hier vorliegenden (BS 7), gar kein (mit dem Papierakt weitgehend identer) elektronischer Akt im PAD vor ... . Umsomehr muß die Lösungsverpflichtung also im Falle des Bf gelten, in dem die Polizei die gesamten Ermittlungsergebnisse in allen Details (aus dem Sexualleben des Bf) in einem (automationsunterstützt durchsuchbaren) elektronischen Akt verarbeitet.

Wenn die bB damit argumentiert, dass eine Abfrage nur nach Namen nicht zulässig sei (BS 13), so ändert dieser Umstand nichts daran, dass diese Daten nicht gelöscht und daher der Polizeibehörde zur Verfügung stehen ... . Zudem hat die bB auch gar keine Ermittlungen vorgenommen, ob tatsächlich keine Möglichkeit zur Namensabfrage besteht. ... Die bB trifft auch keine Feststellungen, dass Abfragen nach Namen unmöglich seien (BS 4). Auf BS 13f geht sie selbst davon aus, dass ein Rückgriff möglich (lediglich dokumentierbar) sei.

Was schließlich den Verweis der bB darauf betrifft, dass ein 'Informationsrückgriff' auch anders unterbunden werden könne als durch die Löschung der Daten (BS 14), so fehlen wieder jegliche Ermittlungen dazu, ob und allenfalls welche anderen Vorkehrungen die Polizei diesbezüglich getroffen hätte. Bloße Spekulationen über alternative Maßnahmen vermögen den Lösungsanspruch des Bf nicht zunichte zu machen, zumal die bB selbst nicht einmal angibt, welche Maßnahmen dies sein könnten.

...

Nur die Löschung der Daten vermag daher die Weiterverarbeitung der Daten für allfällige künftige kriminal- und sicherheitspolizeiliche Tätigkeit wirksam zu unterbinden. Ganz abgesehen davon, dass in die Rechte von Betroffenen stets nur im geringstmöglichen Umfang einzugreifen ist (§§1, 7 Abs3 DSG; §§5, 74f StPO, §§29, 51f SPG).

...

B. Kopienakt

1. Recht auf Löschung (§1 Abs3 Z. 2 DSG, Art8 EMRK)

...

Die in den Kopienakten und im Protokoll enthaltenen personenbezogenen Daten sind als Gesamtheit zu sehen. Die Protokolldaten dienen nach den regelmässigen Ausführungen der bB ja der Wiederauffindung der Kopienakten. Damit handelt es sich aber bei den personenbezogenen Daten (auch) in den Kopienakten um (Teile) eine(r) strukturierte(n) Sammlung, die (durch das Protokoll) nach mindestens einem Kriterium (hier etwa der Aktenzahl und dem Namen des Bf) zugänglich sind. (§4 Z. 6 DSG). Die von der bB vorgenommene Trennung der personenbezogenen Daten im Kopienakt einerseits und den Protokollen andererseits ist künstlich und entspricht nicht dem Schutzzweck des Gesetzes. Im übrigen kann die Verfassungsbestimmung des §1 Abs3 DSG nicht anhand der einfachgesetzlichen, niederrangigeren Bestimmung des §4 Z. 6 DSG ausgelegt werden, würde doch dann der einfache Gesetzgeber den Inhalt von Verfassungsnormen bestimmen. Der Begriff 'Datei' in §1 Abs3 DSG ist verfassungsautonom am Prinzip der Grundrechtseffektivität auszulegen und umfasst daher auch Kopienakte.

Darüber hinaus verleiht Art8 EMRK jedenfalls einen verfassungsgesetzlich gewährleisteten Anspruch auf Löschung (auch) unstrukturiert (konventionell) verarbeiteter Daten (vgl. EGMR: Amann vs. CH 16.02.2000, par. 78ff; Rotaru vs. ROM [GC], 04.05.2000). Auch die einfachgesetzlichen Bestimmungen des §63 SPG und der §§6 Abs1 Z. 2 und Z. 5 DSG sind nicht auf personenbezogene Daten in Dateien beschränkt.

Der Kopienakt wird nicht mehr benötigt (siehe oben A.).

...

2. Recht auf eine wirksame Beschwerde (Art13 EMRK)

Das rechtsstaatliche Prinzip verlangt, dass alle Akte staatlicher Organe im Gesetz und letzten Endes in der Verfassung begründet sein müssen und ein effizientes System von Rechtsschutzeinrichtungen Gewähr dafür bietet, dass nur solche Akte in ihrer rechtlichen Existenz als dauernd gesichert erscheinen, die in Übereinstimmung mit den sie bedingenden Akten höherer Stufe gesetzt werden (VfGH 12.12.2002, G151/02). Ein Rechtsschutzsuchender darf nicht generell einseitig mit den Folgen einer potentiell rechtswidrigen Entscheidung belastet werden (ebendort).

Genau das bewirkte aber die Rechtsansicht der bB.

..."

4. Die belangte Behörde legte die Verwaltungsakten vor und erstattete eine Gegenschrift, in der sie die Ablehnung, in eventu die Abweisung der Beschwerde beantragt. In der Gegenschrift wird der Entwicklungsstand des PAD als "Vorstufe" eines elektronisch geführten Aktensystems beschrieben; danach soll das PAD in Zukunft die vollständig automationsunterstützte Aktenführung ermöglichen und Papierakten mittelfristig (Zeithorizont fünf bis zehn Jahre) nur mehr die Rolle von Hilfs- oder Handakten zukommen.

II. Der Verfassungsgerichtshof hat über die - zulässige - Beschwerde erwogen:

1.1. Die hier maßgeblichen Vorschriften des DSG 2000 (BGBl. I 165/1999) samt Überschrift lauten auszugsweise:

**"Artikel 1  
(Verfassungsbestimmung)  
Grundrecht auf Datenschutz**

§1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer

allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art8 Abs2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. ...

2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs3 sind nur unter den in Abs2 genannten Voraussetzungen zulässig.

(5) ...

## **Artikel 2**

### **1. Abschnitt**

#### **Allgemeines**

#### **Definitionen**

§4. Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:

1. 'Daten' ('personenbezogene Daten'): Angaben über Betroffene (Z3), deren Identität bestimmt oder bestimmbar ist; 'nur indirekt personenbezogen' sind Daten für einen Auftraggeber (Z4), Dienstleister (Z5) oder Empfänger einer Übermittlung (Z12) dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;

2. 'sensible Daten' ('besonders schutzwürdige Daten'): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexuelleben;

3. 'Betroffener': jede vom Auftraggeber (Z4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z8) werden;

4. 'Auftraggeber': natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z9), und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hierzu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch dem Auftragnehmer anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder hat der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten, auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß §6 Abs4 eigenverantwortlich zu treffen, so gilt der mit der Herstellung des Werkes Betraute als datenschutzrechtlicher Auftraggeber;

5. 'Dienstleister': natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden (Z8);

6. 'Datei': strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;

7. 'Datenanwendung' (früher: 'Datenverarbeitung'): die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);

8. 'Verwenden von Daten': jede Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten (Z9) als auch das Übermitteln (Z12) von Daten;

9. 'Verarbeiten von Daten': das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittels (Z12) von Daten;

10. 'Ermitteln von Daten': das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden;

11. - 15. ...

## **2. Abschnitt**

### **Verwendung von Daten**

#### **Grundsätze**

§6. (1) Daten dürfen nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;

2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§46 und 47 zulässig;

3. - 4. ...

5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

(2) - (4) ...

#### **Zulässigkeit der Verwendung von Daten**

§7. (1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

(2) ...

(3) Die Zulässigkeit einer Datenverwendung setzt voraus, daß die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und daß die Grundsätze des §6 eingehalten werden.

#### **Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten**

§8. (1) - (3) ...

(4) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt - unbeschadet der Bestimmungen des Abs2 - nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht oder

2. die Verwendung derartiger Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder

3. sich sonst die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergibt und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach diesem Bundesgesetz gewährleistet.

### **Recht auf Richtigstellung oder Löschung**

§27. (1) Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete Daten richtigzustellen oder zu löschen, und zwar

1. aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder

2. auf begründeten Antrag des Betroffenen.

Der Pflicht zur Richtigstellung nach Z1 unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist. Die Unvollständigkeit verwendeter Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt. Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, daß ihre Archivierung rechtlich zulässig ist und daß der Zugang zu diesen Daten besonders geschützt ist. Die Weiterverwendung von Daten für einen anderen Zweck ist nur zulässig, wenn eine Übermittlung der Daten für diesen Zweck zulässig ist; die Zulässigkeit der Weiterverwendung für wissenschaftliche oder statistische Zwecke ergibt sich aus den §§46 und 47.

(2) - (9) ..."

1.2. Die §§13, 29, 51, 52, 57 und 58 SPG (BGBl. 566/1991 idF BGBl. I 114/2007) haben folgenden (teils auszugsweise wiedergegebenen) Wortlaut:

### **"Kanzleiordnung**

§13. (1) Die formale Behandlung der von den Sicherheitsdirektionen, den Bundespolizeidirektionen und den Polizeikommanden (§10) zu besorgenden Geschäfte ist vom Bundesminister für Inneres jeweils in einer einheitlichen Kanzleiordnung festzulegen. Für die Bundespolizeidirektion Wien können, soweit dies wegen der Größe dieser Behörde erforderlich ist, Abweichungen von der sonst für die Bundespolizeidirektionen geltenden Kanzleiordnung vorgesehen werden.

(2) Der Bundesminister für Inneres, die Sicherheitsdirektionen, Bundespolizeidirektionen und Polizeikommanden sind ermächtigt, sich bei der Wahrnehmung gesetzlich übertragener Aufgaben für die Dokumentation von Amtshandlungen und die Verwaltung von Dienststücken der automationsunterstützten Datenverarbeitung zu bedienen. Zu diesen Zwecken dürfen sie Daten über natürliche und juristische Personen sowie Sachen verwenden, auf die sich der zu protokollierende Vorgang bezieht, wie insbesondere Datum, Zeit und Ort, Fahrzeugdaten, Betreff und Aktenzeichen samt Bearbeitungs- und Ablagevermerken sowie Namen, Rolle des Betroffenen, Geschlecht, frühere Namen, Aliasdaten, Staatsangehörigkeit, Geburtsdatum, Geburtsort, Wohnanschrift und andere zur Erreichbarkeit des Menschen dienende Daten. Soweit es erforderlich ist, dürfen

auch sensible Daten (§4 Z2 DSG 2000) sowie Daten im Sinne des §8 Abs4 DSG 2000 verwendet werden. Die Auswählbarkeit von Daten aus der Gesamtmenge der gespeicherten Daten nur nach dem Namen und nach sensiblen Daten darf nicht vorgesehen sein, vielmehr ist für die Auswahl ein auf den protokollierten Sachverhalt bezogenes weiteres Datum anzugeben.

### **Verhältnismäßigkeit**

§29. (1) Erweist sich ein Eingriff in Rechte von Menschen als erforderlich (§28a Abs3), so darf er dennoch nur geschehen, soweit er die Verhältnismäßigkeit zum Anlaß und zum angestrebten Erfolg wahrt.

(2) Insbesondere haben die Sicherheitsbehörden und die Organe des öffentlichen Sicherheitsdienstes

1. von mehreren zielführenden Befugnissen jene auszuwählen, die voraussichtlich die Betroffenen am wenigsten beeinträchtigt;

2. darauf Bedacht zu nehmen, ob sich die Maßnahme gegen einen Unbeteiligten oder gegen denjenigen richtet, von dem die Gefahr ausgeht oder dem sie zuzurechnen ist;

3. darauf Bedacht zu nehmen, daß der angestrebte Erfolg in einem vertretbaren Verhältnis zu den voraussichtlich bewirkten Schäden und Gefährdungen steht;

4. - 5. ...

## **4. Teil**

### **Verwenden personenbezogener Daten im Rahmen der Sicherheitspolizei**

#### **1. Hauptstück**

##### **Allgemeines**

§51. (1) Die Sicherheitsbehörden haben beim Verwenden (Verarbeiten und Übermitteln) personenbezogener Daten die Verhältnismäßigkeit (§29) zu beachten. Beim Verwenden sensibler und strafrechtlich relevanter Daten haben sie angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen.

(2) Sofern nicht ausdrücklich Anderes angeordnet wird, finden auf das Verwenden personenbezogener Daten die Bestimmungen des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999, Anwendung.

#### **2. Hauptstück**

##### **Ermittlungsdienst**

##### **Aufgabenbezogenheit**

§52. Personenbezogene Daten dürfen von den Sicherheitsbehörden gemäß diesem Hauptstück nur verwendet werden, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Ermächtigungen nach anderen Bundesgesetzen bleiben unberührt.

### **Zentrale Informationssammlung; Zulässigkeit der Ermittlung, Verarbeitung und Übermittlung**

§57. (1) Die Sicherheitsbehörden dürfen Namen, Geschlecht, frühere Namen, Staatsangehörigkeit, Geburtsdatum, Geburtsort und Wohnanschrift, Namen der Eltern und Aliasdaten eines Menschen ermitteln und im Rahmen einer Zentralen Informationssammlung samt dem für die Speicherung maßgeblichen Grund, einer allenfalls vorhandenen Beschreibung des Aussehens eines Menschen und seiner Kleidung und einem allenfalls erforderlichen Hinweis auf das gebotene Einschreiten für Auskünfte auch an andere Behörden verarbeiten, wenn

1. gegen den Betroffenen ein inländischer richterlicher Befehl oder eine Anordnung des Vorsitzenden eines finanzbehördlichen Spruchsenates zur Ermittlung des Aufenthaltes oder zur Festnahme besteht;

2. gegen den Betroffenen ein sicherheitsbehördlicher Befehl zur Festnahme gemäß §171 Abs2 StPO besteht;

3. gegen den Betroffenen ein Vorführbefehl nach dem Strafvollzugsgesetz, BGBl. Nr. 144/1969, besteht;

4. ...

5. gegen den Betroffenen im Zusammenhang mit der Abwehr oder Aufklärung gefährlicher Angriffe oder mit der Abwehr krimineller Verbindungen ermittelt wird;

6. gegen den Betroffenen Ermittlungen im Dienste der Strafrechtspflege eingeleitet worden sind;

7. - 12. ...

(2) - (3) ...

### **Zentrale Informationssammlung; Sperren des Zugriffes und Löschen**

§58. (1) Personenbezogene Daten, die gemäß §57 Abs1 evident gehalten werden, sind für Zugriffe der Sicherheitsbehörden als Auftraggeber zu sperren

1. in den Fällen der Z1 zwei Jahre nach Widerruf des richterlichen Befehles oder der finanzbehördlichen Anordnung;

2. in den Fällen der Z2 nach Widerruf des sicherheitsbehördlichen Befehles, spätestens jedoch 24 Stunden nach Aufnahme in die Zentrale Informationssammlung;

3. in den Fällen der Z3 nach Widerruf des Vorführbefehles;

4. ...

5. in den Fällen der Z5, wenn der Angriff abgewehrt oder aufgeklärt worden ist oder wenn der Betroffene sonst für die allgemeine Gefahr nicht mehr maßgeblich ist;

6. in den Fällen der Z6, wenn gegen den Betroffenen kein Verdacht mehr besteht, eine strafbare Handlung begangen zu haben, spätestens jedoch fünf Jahre nach der Aufnahme in die Zentrale Informationssammlung, im Falle mehrerer Speicherungen gemäß Z6 fünf Jahre nach der letzten;

7. - 11. ...

Nach Ablauf von zwei weiteren Jahren sind die Daten auch physisch zu löschen. Während dieser Zeit kann die Sperre für Zwecke der Kontrolle der Richtigkeit einer beabsichtigten anderen Speicherung gemäß Abs1 aufgehoben werden.

(2) ..."

2. Unter Berücksichtigung dieser Rechtslage ergibt sich für den vorliegenden Fall Folgendes:

2.1. Der Verfassungsgerichtshof geht (ebenso wie der Verwaltungsgerichtshof) in seiner Rechtsprechung davon aus, dass Kopienakten (Papierakten) zufolge ihres Aufbaues und ihrer Struktur nicht als Datei iSd §4 Z6 DSG 2000 zu qualifizieren sind, weshalb insoweit kein Lösungsanspruch besteht (vgl. zB VfSlg. 17.745/2005, 18.092/2007; VwSlg. 16.477 A/2004, VwGH 2.11.2008, 2005/6/0301 uva.). In diesem Konnex hat der Verfassungsgerichtshof zudem festgehalten, dass aus den Garantien der Art8 und 13 EMRK grundsätzlich keine weiter reichenden Ansprüche abgeleitet werden können als aus der Verfassungsbestimmung des §1 Abs3 DSG 2000 (VfSlg. 18.092/2007, 18.300/2007).

2.2. Darüber hinaus hat der Verfassungsgerichtshof bereits in VfSlg. 16.149/2001 (Anlassfall zu VfSlg. 16.150/2001 betreffend die Prüfung der - für nicht verfassungswidrig erkannten - §§57 Abs1 Z6, 58 Abs1 Z6 litb

SPG) zu automationsunterstützt verarbeiteten personenbezogenen Daten, die von der Kriminalpolizei für Zwecke der Strafrechtspflege ermittelt wurden, ausgesprochen, dass "dann, wenn die weitere Speicherung der Anzeigedaten zum Zweck der Strafrechtspflege nicht mehr erforderlich ist", eine umgehende Löschung in Betracht kommt. "Ob die Voraussetzungen für die Löschung (vor Ablauf der Frist des §58 SPG) vorliegen, ist im Einzelfall unter Vornahme einer (ausreichenden) Interessenabwägung zu beurteilen". Dieser Rechtsstandpunkt wurde in der Folge va. iZm Beschwerden des auch hier einschreitenden Rechtsvertreters zu Daten betreffend den (vom Verfassungsgerichtshof mit VfSlg. 16.565/2002 aufgehobenen und mit dem StrafrechtsänderungsG 2002, BGBl. I 134, entfallenen) §209 StGB mehrfach wiederholt und ist inzwischen ständige Rechtsprechung (vgl. zB VfSlg. 17.716/2005, 17.745/2005, 18.091/2007 und 18.300/2007).

2.2.1. In den Bezug habenden Erkenntnissen hat der Verfassungsgerichtshof ferner klargestellt, dass derartige Daten nicht gemäß §13 SPG dem inneren Dienst zugerechnet werden dürfen, wenn damit (wie bei Aufnahme eines bestimmten Namens mit weiteren Angaben) subjektive Rechtspositionen der Betroffenen geschaffen wurden; eine Zurechnung dieser Daten zum inneren Dienst bewirkt in solchen Fällen ein in die Verfassungssphäre reichendes Verkennen der Rechtslage (vgl. auch VfSlg. 17.746/2006, 17.747/2006, 17.748/2006, 18.457/2008 und VfGH 26.1.2006, B764/04).

3. Bedenken gegen die dem angefochtenen Bescheid zugrunde liegenden Rechtsvorschriften werden in der Beschwerde nicht vorgebracht und sind beim Verfassungsgerichtshof aus Anlass der Beschwerde in Ansehung der von ihm anzuwendenden Bestimmungen (nach dem DSG 2000 und nach dem SPG) auch nicht entstanden (vgl. zB VfSlg. 16.150/2001, 17.745/2005, 18.091/2007, 18.324/2007). Es ist daher ausgeschlossen, dass der Beschwerdeführer in seinen Rechten wegen Anwendung einer rechtswidrigen generellen Norm verletzt wurde.

3.1. Der belangten Behörde ist aber auch (va. mit Blick auf den Gewährleistungsumfang des Grundrechts auf Datenschutz iVm jenem auf Achtung des Privatlebens) kein in die Verfassungssphäre reichender Fehler unterlaufen:

3.1.1. Beschränkungen des gemäß §1 Abs3 Z2 DSG 2000 nach Maßgabe gesetzlicher Bestimmungen garantierten Grundrechts auf Löschung unzulässigerweise verarbeiteter Daten sind lediglich unter den in §1 Abs2 DSG 2000 genannten Voraussetzungen zulässig. Diese Vorschrift erlaubt (abgesehen von hier nicht in Betracht kommenden Ausnahmefällen) Eingriffe in das in Rede stehende Grundrecht durch staatliche Behörden nur auf Grund von Gesetzen, die aus den in Art8 Abs2 EMRK genannten Gründen notwendig sind.

Art 8 Abs2 EMRK gestattet Beschränkungen des in Abs1 verbürgten Grundrechts nur, wenn diese eine Maßnahme darstellen, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer erforderlich ist.

3.2. Es gibt keinen Anhaltspunkt dafür, dass die belangte Behörde den angewendeten Rechtsvorschriften fälschlicherweise einen verfassungswidrigen, insbesondere dem §1 Abs3 DSG 2000 oder dem Art8 EMRK zuwiderlaufenden Inhalt unterstellt hat.

3.3. Zum vorliegenden Kopienakt ist festzuhalten:

3.3.1. Die darin enthaltenen, auf den Beschwerdeführer bezogenen personenbezogenen Daten wurden in Kongruenz mit der dargelegten (vorwiegend zu Beschwerden des hier einschreitenden Rechtsvertreters mit weitgehend identischem Vorbringen zur Speicherung von Anzeigedaten nach §209 StGB ergangenen) Rechtsprechung des Verfassungsgerichtshofs (oben Pkt. 2.1.) - von der abzugehen vor dem Hintergrund des vorliegenden Falles kein Anlass besteht - zutreffend nicht dem Begriff einer Datei iSd DSG 2000 unterstellt.

Der Umstand, dass die Eintragungen im PAD nunmehr - im Unterschied zur früheren Praxis - auch hinsichtlich "innerer" Daten (wie in Bezug auf Vernehmungsprotokolle) automationsunterstützt erfolgen, ist iS der Auffassung der belangten Behörde aus verfassungsrechtlicher Sicht für die Beurteilung der Frage der Verknüpfbarkeit des unstrukturierten Papieraktes mit den PAD-Eintragungen und damit für die datenschutzrechtliche Qualifikation eines Kopienaktes ohne entscheidende Bedeutung, weil auch die schon bisher enthaltenen "äußeren" Daten (wie Name des Angezeigten und Delikt) die Herstellung einer Verbindung zum Kopienakt ermöglichten und die gesonderte Auswählbarkeit aus der Gesamtmenge der gespeicherten Daten nur nach dem Namen ohne zusätzliches Kriterium unzulässig ist (§13 Abs2 SPG).

3.3.2. Die elektronische Datensammlung im EDV-System PAD kann sich auf die Bestimmung des §13 Abs2 SPG stützen.

Die Evidenthaltung der in diesem System dokumentierten ("äußeren" und "inneren") Daten ist allerdings nur dann verfassungsrechtlich zulässig, wenn sie sich im Rahmen der grundrechtlichen Garantien hält.

Aus den Grundrechtsverbürgungen des §1 Abs3 DSG 2000 iZm Art8 Abs2 EMRK (oben Pkt. 3.1.1.) folgt, dass im Falle eines Eingriffs in das Grundrecht auf Datenschutz, so auch bei der Weiterverarbeitung strafrechtsrelevanter Daten nach Einstellung des Bezug habenden Strafverfahrens, eine Interessenabwägung vorzunehmen ist (vgl. auch §§8, 29, 51 und 58 SPG; 6 ff., 8, 27 DSG 2000).

Dabei sind die Interessen des Betroffenen an der Löschung der Daten dem öffentlichen Interesse an der weiteren Dokumentation - einzelfallbezogen - gegenüberzustellen und zu gewichten (vgl. zB VfSlg. 16.149/2001, 17.745/2006, 17.746/2006, VfGH 26.1.2006, B764/04).

3.3.3. Die hier maßgeblichen Daten wurden von der belangten Behörde (im Unterschied zur Konstellation in dem vom Beschwerdeführer ins Treffen geführten Erkenntnis VfGH 11.6.2007, B1737/06) zu Recht nicht dem inneren Dienst (als bloß behördeninterner Dokumentationszweck) iSd §13 SPG zugerechnet, sondern zutreffend als dem Löschungsrecht unterfallend eingestuft (vgl. oben Pkt. 2.2.1.).

Davon ausgehend hat die belangte Behörde das Lösungsbegehren anhand der datenschutzrechtlichen Kriterien geprüft und eine Interessenabwägung vorgenommen, in der sie zum Ergebnis gelangte, dass die öffentlichen Interessen an der Fortsetzung der Speicherung den Lösungsanspruch des Beschwerdeführers - jedenfalls zum maßgeblichen Zeitpunkt (der Mitteilung über das Unterbleiben der Löschung durch die Bundespolizeidirektion Wien) - an Gewicht übersteigen.

3.3.4. Diese Beurteilung ist unter den Umständen des vorliegenden Falles nicht zu beanstanden:

In Anbetracht der von der belangten Behörde erwogenen Möglichkeit des Hervorkommens von Gründen, die Anlass für eine Wiedereröffnung des Verfahrens bieten, aber auch angesichts der näheren Erörterung denkbarer nachträglicher Kontrollvorgänge, kann der belangten Behörde aus verfassungsrechtlicher Sicht nicht entgegengetreten werden, wenn sie den öffentlichen Interessen an der Auffindbarkeit der Ermittlungsakten höheres Gewicht beimisst als dem (evidenten) Lösungsinteresse des Beschwerdeführers. Dies u.a. auch deshalb, weil - zumindest im aktuellen Zeitraum (ca. sechs Monate nach Verfahrensbeendigung) - nicht von der Hand zu weisen ist, dass die in Rede stehenden Dateien nicht nur für die Nachvollziehbarkeit innerbehördlicher Vorgänge, sondern auch für andere, mit den konkreten Ermittlungen im Zusammenhang stehende sicherheitspolizeiliche Belange noch Bedeutung haben können.

Das Resultat dieser Interessenabwägung ist insbesondere auch vor dem Hintergrund der gesetzlichen Verpflichtung zur Sperre einer Datenspeicherung für Zugriffe der Polizeibehörden spätestens nach Ablauf von fünf Jahren (§58 Abs1 Z6 SPG) sowie zur physischen Löschung spätestens nach zwei weiteren Jahren (§58 Abs1 leg.cit. vorletzter Satz) - und mit Blick auf den eingeschränkten Kreis von zugriffsberechtigten Amtsträgern (deren rechtskonformes Verhalten durch dienst-, disziplinar- und strafrechtliche Vorschriften abgesichert ist) sowie auf die gerade bei elektronischer Aktenführung gegebene Nachvollziehbarkeit eines Datenzuganges (samt Ausforschbarkeit des Anwenders aufgrund zuordenbarer Zugangsdaten) als verfassungsrechtlich vertretbar anzusehen, zumal - wie erwähnt - die Auswählbarkeit von Daten einer bestimmten Person nur nach dem Namen unzulässig ist (§13 Abs2 SPG).

Der Umstand, dass die Daten zusätzlich im Bereich der Staatsanwaltschaft bzw. des Gerichtes aufgefunden werden können, vermag an der Vertretbarkeit der (Gesamt)Beurteilung durch die belangte Behörde aus verfassungsrechtlicher Sicht nichts zu ändern. In besonderen Konstellationen (wie im denkbaren Fall einer neuerlichen Anzeige wegen desselben Sachverhaltes) kann die Speicherung der Daten im Übrigen (auch) im Interesse des Betroffenen liegen.

Auch ein willkürliches Verhalten kann der belangten Behörde nicht zum Vorwurf gemacht werden.

3.4. Ein Verstoß gegen das in Art13 EMRK gewährleistete Grundrecht kommt mit Blick auf dessen Beschränkung auf Konventionsrechte und die vorstehenden Ausführungen zu Art8 EMRK nicht in Betracht (vgl. im Übrigen oben Pkt. 2.1.).

4. Die behaupteten Rechtsverletzungen haben somit nicht stattgefunden. Das Verfahren hat auch nicht ergeben, dass der Beschwerdeführer durch den angefochtenen Bescheid in einem anderen, von ihm nicht geltend gemachten verfassungsgesetzlich gewährleisteten Recht verletzt worden wäre.

Der Beschwerdeführer ist somit durch den bekämpften Bescheid weder in einem verfassungsgesetzlich gewährleisteten Recht noch wegen Anwendung einer rechtswidrigen generellen Norm in seinen Rechten verletzt worden.

5. Die Beschwerde war daher als unbegründet abzuweisen.

6. Diese Entscheidung konnte gemäß §19 Abs4 erster Satz VfGG ohne mündliche Verhandlung in nichtöffentlicher Sitzung getroffen werden.