VERFASSUNGSGERICHTSHOF
G 2/2013-17
01.10.2013

# IM NAMEN DER REPUBLIK!

Der Verfassungsgerichtshof hat unter dem Vorsitz des Präsidenten
Dr. Gerhart HOLZINGER,

in Anwesenheit der Vizepräsidentin
Dr. Brigitte BIERLEIN

und der Mitglieder
Dr. Markus ACHATZ,
Dr. Sieglinde GAHLEITNER,
DDr. Christoph GRABENWARTER,
Dr. Christoph HERBST,
Dr. Michael HOLOUBEK,
Dr. Helmut HÖRTENHUBER,
Dr. Claudia KAHR,
Dr. Georg LIENBACHER,
Dr. Rudolf MÜLLER,
Dr. Johannes SCHNIZER und
Dr. Ingrid SIESS-SCHERZ

als Stimmführer, im Beisein der Schriftführer
Mag. Dr. Florian GRATZL und
Dr. Valerie TROFAIER-LESKOVAR,

in dem von Amts wegen eingeleiteten Verfahren zur Prüfung der Verfassungsmäßigkeit des § 140 Abs. 3 StPO idF BGBl. I 19/2004 nach der am 12. Juni 2013 durchgeführten öffentlichen mündlichen Verhandlung, nach Anhörung des Vortrages der Berichterstatterin und der Ausführungen der Vertreter der Bundesregierung Mag. Philipp Cede sowie SC Mag. Christian Pilnacek, des Vertreters der Datenschutzkommission Mag. Michael Suda und des Vertreters der beteiligten Partei Rechtsanwalt Dr. Martin Riedl (für Rechtsanwalt Dr. Walter Riedl) gemäß Art. 140 B-VG zu Recht erkannt:

I. § 140 Abs. 3 der Strafprozeßordnung 1975, BGBl. Nr. 631, idF BGBl. I Nr. 19/2004, wird als verfassungswidrig aufgehoben.

II. Die Aufhebung tritt mit Ablauf des 31. Oktober 2014 in Kraft.

III. Frühere gesetzliche Bestimmungen treten nicht wieder in Kraft.

IV. Der Bundeskanzler ist zur unverzüglichen Kundmachung dieser Aussprüche im Bundesgesetzblatt I verpflichtet.

## Entscheidungsgründe

## I. Anlassverfahren, Prüfungsbeschluss und Vorverfahren

1. Beim Verfassungsgerichtshof ist zur Zahl B 1408/2011 eine auf Art. 144 B-VG gestützte Beschwerde anhängig, der zusammengefasst folgender Sachverhalt zugrunde liegt: 1

1.1. Der Beschwerdeführer war Polizeibeamter im Bereich des Landespolizeikommandos Wien (LPK Wien) und befindet sich seit 1. Jänner 2011 im Ruhestand. Im Jahr 2009 erstattete das LPK Wien gegen ihn wegen des Verdachts verschiedener Disziplinarvergehen Disziplinaranzeige. In diesem Zusammenhang wurde gegen den Beschwerdeführer wegen allfälliger gerichtlich strafbarer Handlungen auch ein kriminalpolizeiliches Ermittlungsverfahren geführt, in dem die Staatsanwaltschaft (nach gerichtlicher Bewilligung) eine auf die Mobilfunknummer des Beschwerdeführers bezogene Rufdaten- und Standortdaten- 2

rückerfassung anordnete. Die ermittelten Daten der Nachrichtenübermittlung wurden der Staatsanwaltschaft und dem LPK Wien zur Kenntnis gebracht.

Das Strafverfahren wurde – soweit es mit den angeführten verdeckten Ermittlungen im Zusammenhang stand – durch Einstellung (3. März 2010), im Übrigen durch Freispruch (17. August 2010) beendet. 3

1.2. Die in der Folge vom Beschwerdeführer wegen Verletzung im Recht auf Geheimhaltung durch Verwendung der für Zwecke des Strafverfahrens erhobenen Daten im Disziplinarverfahren bei der Datenschutzkommission eingebrachte Beschwerde wurde mit Bescheid vom 21. Oktober 2011 abgewiesen, weil die Daten im Strafverfahren rechtmäßig ermittelt worden seien und daher allenfalls von den Justizbehörden zu löschen wären. Die – parallel ermittelnde – Disziplinarkommission habe die strafrechtlichen Daten iSd Ermächtigung des § 140 Abs. 3 StPO weiterverwenden und als Beweismittel verwerten dürfen. 4

2. Bei Behandlung der gegen diesen Bescheid erhobenen Beschwerde sind beim Verfassungsgerichtshof Bedenken ob der Verfassungsmäßigkeit des § 140 Abs. 3 StPO entstanden. Es wurde daher am 12. Dezember 2012 beschlossen, diese Gesetzesbestimmung von Amts wegen auf ihre Verfassungsmäßigkeit zu prüfen. 5

3. Der Verfassungsgerichtshof legte die Bedenken, die ihn zur Einleitung des Gesetzesprüfungsverfahrens bestimmt haben, folgendermaßen dar: 6

"2.1. Vorangestellt sei, dass § 140 Abs. 3 StPO nach der vorläufigen Auffassung des Verfassungsgerichtshofes hinsichtlich der Verwendung von Daten, die in einem Strafverfahren legitimerweise ermittelt wurden, in anderen gerichtlichen und verwaltungsbehördlichen Verfahren eine abschließende Regelung darstellt, sodass die (insoweit verdrängte) Bestimmung des § 8 Abs. 4 Z 2 DSG 2000 auf derartige Fälle nicht anwendbar sein dürfte.

2.2. Der Verfassungsgerichtshof hegt das Bedenken, dass die in Prüfung genommene Vorschrift nicht nur ein Beweisverwertungsverbot in Bezug auf unrechtmäßig ermittelte Daten normiert, sondern darüber hinaus eine generelle Ermächtigung zur Verwendung von in einem Strafverfahren rite erhobenen Ergebnissen iSd § 134 Z 5 StPO – nämlich die Beschlagnahme von Briefen (§ 134 Z 1 StPO), die Auskunft über Daten einer Nachrichtenübermittlung (§ 134 Z 2 StPO), die Überwachung von Nachrichten (§ 134 Z 3 StPO), die optische und akustische Überwachung von Personen (§ 134 Z 4 StPO) – als Beweismittel in (allen) anderen gerichtlichen und verwaltungsbehördlichen Verfahren enthält und daher dem Grundrecht auf Datenschutz widerspricht.

2.3. Diesem – verfassungsgesetzlich gewährleisteten – Grundrecht (§ 1 Abs. 1 DSG 2000) zufolge hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf die Achtung seines Privat- und Familienlebens, hat.

2.3.1. Beschränkungen dieses Grundrechts sind nach dem Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 (abgesehen vom lebenswichtigen Interesse der Betroffenen an der Verwendung personenbezogener Daten oder ihrer Zustimmung dazu) nur zur Wahrung überwiegender berechtigter Interessen eines anderen, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen zulässig, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind. Besondere Schutzvorkehrungen gelten ferner für 'ihrer Art nach besonders schutzwürdig(e)', also sogenannte sensible Daten.

2.3.2. Gemäß Art. 8 Abs. 2 EMRK sind Eingriffe in das in diesem Artikel verbürgte Grundrecht nur statthaft, insoweit sie 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 notwendig ist. Auch im Fall zulässiger Beschränkungen darf gemäß dem letzten Satz des § 1 Abs. 2 DSG 2000 der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden (vgl. VfSlg. 18.975/2009). Der jeweilige Gesetzgeber muss daher eine diesen Anforderungen genügende materienspezifische Regelung vorsehen (VfSlg. 18.643/2008, 19.592/2011).

2.3.3. Zudem hat der Verfassungsgerichtshof in VfSlg. 18.146/2007 ausgesprochen, dass die Ermittlung und Verwendung personenbezogener Daten durch Eingriffe einer staatlichen Behörde wegen des Gesetzesvorbehalts des § 1 Abs. 2 DSG 2000 nur auf Grund von Gesetzen zulässig ist, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind und ausreichend präzise, also für jedermann vorhersehbar regeln, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig ist. Das DSG 2000 geht daher von einer strengen Zweckbindung der Ermittlung und der Verwendung von Daten aus, weshalb erhobene Daten ausschließlich für die im jeweiligen Materiengesetz definierten Zwecke verwendet werden dürfen (vgl. auch VfGH 29.6.2012, G 7/12).

2.4. Nun ist es dem Gesetzgeber durch das Grundrecht auf Datenschutz nicht von vornherein untersagt, die Zulässigkeit einer Datenverwendung als Beweismittel in anderen Verfahren als in jenem, in dem diese Daten rechtmäßig ermittelt wurden, vorzusehen, jedoch ist ein solcher Eingriff gemäß § 1 DSG 2000 iVm Art. 8 Abs. 2 EMRK auf das erforderliche, geeignete und verhältnismäßige Maß zu beschränken (vgl. VfSlg. 18.975/2009 mwN). Der Gesetzgeber darf daher die Verwertung von personenbezogenen Daten, die in einem Strafverfahren rite erhoben wurden, in sonstigen (gerichtlichen oder verwaltungsbehördlichen) Verfahren nur insoweit vorsehen, als der Zweck der Datenverwendung in diesen

Verfahren ein öffentliches Interesse verfolgt, welches das Interesse des Betroffenen an der Geheimhaltung (bzw. Löschung) der Daten übersteigt.

2.5. Diesen verfassungsrechtlich vorgegebenen Erfordernissen dürfte die Regelung des § 140 Abs. 3 StPO nicht genügen:

2.5.1. Scheint sie doch die Verwendung von Ergebnissen einer Datenermittlung aus einem Strafverfahren als Beweismittel in sonstigen gerichtlichen und verwaltungsbehördlichen Verfahren unter der einzigen Prämisse, dass die Datenverwendung im Bezug habenden Strafverfahren zulässig war oder wäre, im Übrigen aber unbeschränkt zu erlauben.

2.5.2. Das dürfte bedeuten, dass in einem strafgerichtlichen oder staatsanwaltschaftlichen (Ermittlungs-)Verfahren auf legitime Weise erhobene personenbezogene Daten der genannten Art auch lange nach Beendigung des gerichtlichen Strafverfahrens sowie unabhängig von dessen Ausgang und ungeachtet einer dort allenfalls bereits erfolgten Löschung in jedem anderen (auch zivil-)gerichtlichen oder verwaltungsbehördlichen (Parallel-)Verfahren, in welchem die Behörde Kenntnis von diesen Daten hat, als Beweismittel benützt werden können; dies anscheinend ohne jede Einschränkung im Hinblick auf öffentliche Interessen bzw. auf die Bedeutung dieser Verfahren (somit auch in Bagatellsachen) sowie ohne die Notwendigkeit des Bestehens eines Zusammenhanges mit dem betreffenden Strafverfahren.

2.6. Nach den Gesetzesmaterialien war die angeführte vergleichbare Vorgängerbestimmung (§ 149h StPO idF BGBl. I 105/1997) vom Ziel getragen, die Beweisverwertung von Überwachungsergebnissen in anderen (nicht strafrechtlichen) Gerichtsverfahren und verwaltungsbehördlichen Verfahren zu verbieten, wenn die Verwertung dieser Ergebnisse im Strafverfahren unzulässig war oder unzulässig gewesen wäre. Die Erweiterung des strafrechtlichen Beweisverwertungsverbotes auf andere Verfahren wurde damit begründet, dass 'nur dadurch das Wesen und der rechtsstaatliche Wert einer Verfahrensordnung zum Ausdruck gebracht werden kann, die massive Eingriffe in die Privatsphäre nur unter dem Gesichtspunkt und im Ausmaß eines angestrebten Nachweises organisierter Kriminalität und schwerster Straftaten in Kauf nehmen will' (AB 812 BlgNR 20. GP, 10).

Dieser gesetzgeberischen Intention dürfte die in Prüfung genommene (mit der Vorgängerbestimmung nahezu wortidente) Regelung, die nach ihrem anscheinend klaren Wortlaut gerade nicht auf die Konnexität der angeführten Verfahren mit dem Bezug habenden Strafverfahren oder auf den Nachweis schwerer und organisierter Kriminalität abstellt, insoweit nicht entsprechen, als die Beweisverwertung in anderen Verfahren – so nimmt der Verfassungsgerichtshof vorerst an – selbst dann erlaubt ist, wenn die Verwendung der Daten im Strafverfahren – etwa zufolge Wegfalls der Berechtigung zur Weiterspeicherung – unzulässig geworden ist oder die Daten im Strafakt bereits gelöscht wurden.

2.7. Vor diesem Hintergrund vermag der Verfassungsgerichtshof vorderhand keinen sachlichen Grund zu erkennen, der die beweismäßige Nutzung von Daten über Ergebnisse iSd § 134 Z 5 StPO, darunter Daten einer geheimen Nachrichten-

übermittlung, in allen (anderen) gerichtlichen oder verwaltungsbehördlichen Verfahren schlechthin – unabhängig davon, ob bzw. welche öffentlichen Interessen mit diesen Verfahren verfolgt werden (also nicht nur in mit der Strafsache in Konnex stehenden Gerichts-, Disziplinar- und sonstigen Verwaltungsverfahren oder bei Verdacht schwerer bzw. organisierter Delinquenz, wie es § 75 Abs. 5 StPO vorsieht), gemäß § 1 DSG 2000 iVm Art. 8 Abs. 2 EMRK aus überwiegenden Interessen des Auftraggebers notwendig erscheinen ließe.

2.8. Auch hegt der Verfassungsgerichtshof Zweifel, dass die in Prüfung genommene gesetzliche Regelung auf den geringst möglichen Eingriff abstellt. Vielmehr dürfte die – wie schon dargelegt, ganz allgemein gehaltene und ohne jede Schranken normierte – Verwendungs- und Verwertungsermächtigung des § 140 Abs. 3 StPO mit Blick auf die Garantien des Datenschutzes überschießend und deshalb unverhältnismäßig sein.

2.9. Für eine allfällige verfassungskonforme Interpretation der in Rede stehenden Bestimmung in der Weise, dass für diese die Verwendungsbeschränkungen des (zum Teil auf identische Überwachungsmaßnahmen bezogenen) § 75 Abs. 5 StPO heranzuziehen sind (nämlich das Erfordernis eines inhaltlichen Zusammenhanges zwischen anderen Zivil- und Verwaltungsverfahren und jenem Strafverfahren, in dem die Ergebnisse nach §§ 135, 136 und 141 StPO rechtmäßig erzielt wurden, oder das Vorliegen bestimmter Fälle der Gefahrenabwehr – vgl. *Reindl-Krauskopf*, WK-StPO$^2$ [2011], § 75 Rz 15 f. und [2009] § 140 Rz 28 f.), sieht der Verfassungsgerichtshof angesichts des anscheinend keinen Auslegungsspielraum offen lassenden Wortlautes sowohl des § 140 Abs. 3 StPO als auch des § 75 Abs. 5 StPO (der als lex specialis gegenüber § 140 Abs. 3 StPO auf Daten, die durch eine Überwachung von Nachrichten [§ 134 Z 3 leg.cit.], eine optische oder akustische Überwachung [§ 134 Z 4 leg.cit.] oder einen automationsunterstützten Datenabgleich [§ 141 leg.cit.] ermittelt worden sind, Bezug nimmt) – jedenfalls vorerst – keine Möglichkeit. Auch scheint es dem Gesetzgeber nicht zusinnbar, mit der Übernahme der Vorgängerbestimmung des § 149h StPO in § 140 Abs. 3 [StPO idF] des Strafprozessreformgesetzes BGBl. I 19/2004 lediglich versehentlich die Festlegung der mit demselben Gesetz in § 75 Abs. 5 StPO ausdrücklich normierten Schranken unterlassen zu haben.

2.10. Schließlich geht der Verfassungsgerichtshof vorläufig davon aus, dass der dem Betroffenen durch § 27 Abs. 1 Z 2 DSG 2000 grundsätzlich – wohl auch in Bezug auf die (ebenfalls) als Auftraggeber iSd § 4 Z 4 DSG 2000 anzusehende Behörde im Parallelverfahren – eingeräumte Löschungsanspruch ebenfalls (zumindest, soweit es sich um die Weiterverwendung von Daten handelt, die im Strafakt schon gelöscht wurden) nicht geeignet sein dürfte, die Bedenken gegen die in Prüfung gezogene Ermächtigungsnorm zu entkräften, zumal dem Betroffenen damit anscheinend eine unverhältnismäßige einseitige Belastung in Bezug auf ein allenfalls rechtswidriges Vorgehen auferlegt würde.

[…]

Ob die Prozessvoraussetzungen gegeben sind und die angeführten Bedenken zutreffen, wird im Gesetzesprüfungsverfahren zu klären sein; ebenso wird zu beurteilen sein, ob die in Rede stehende Vorschrift einer einschränkenden verfassungskonformen Auslegung in der Richtung zugänglich ist, dass diese ein bloßes Beweisverwertungsverbot (ohne Ermächtigung zur Datenverwendung) beinhaltet."

4. Die Bundesregierung erstattete eine Äußerung, in der den im Prüfungsbeschluss dargelegten Bedenken wie folgt entgegengetreten wird (Zitat ohne die im Original enthaltenen Hervorhebungen): 7

"2. Zu den Anforderungen des Grundrechts auf Datenschutz

2.1. Der dem Beschwerdeverfahren zugrundeliegende Sachverhalt gehört zu einer Abfolge von Vorgängen, die sich wie folgt beschreiben lässt:

1. Ermittlung und Speicherung von personenbezogenen Daten durch eine Behörde (A) zur Erfüllung der von dieser Behörde wahrzunehmenden Aufgaben der Hoheitsverwaltung (Gerichtsbarkeit).
Hier: (zunächst) verdeckte Ermittlung von personenbezogenen Daten auf Grund besonderer Befugnisse der Strafverfolgungsbehörden (Rufdatenrückerfassung) nach Maßgabe strenger prozessualer Voraussetzungen und strenger Zweckbindung im gerichtlichen Strafverfahren.

2. Übermittlung der für den ursprünglichen Zweck ermittelten Daten an eine Behörde (B) zur Erfüllung eines anderen Zwecks, nämlich der Wahrnehmung der von der Behörde B zu erfüllenden Aufgabe der Hoheitsverwaltung.
Hier: Übermittlung von Daten aus der Rufdatenrückerfassung durch die Kriminalpolizei an die als Disziplinarbehörde zuständigen Organe des BMI.

3. Weiterverwendung der übermittelten personenbezogenen Daten für Zwecke der Erfüllung der der Behörde B zukommenden Aufgaben;
Hier: Beweiserhebung und -verwertung der Ergebnisse der Rufdatenrückerfassung durch die Disziplinarbehörde im BMI.

2.2. Beschwerdegegenstand im Verfahren, das mit dem dem Prüfungsbeschluss zugrunde liegenden Bescheid der Datenschutzkommission erledigt wurde, war - soweit ersichtlich - ausschließlich die Weiterverwendung von Daten, sodass die Frage der Rechtmäßigkeit der Ermittlung und Übermittlung in diesem Verfahren lediglich als Vorfrage bzw. allenfalls im Rahmen der Interessenabwägung relevant war.

2.3. Nach dem in § 1 Abs. 1 DSG 2000 normierten 'Grundrecht auf Datenschutz' hat 'jedermann [...], insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden Daten, soweit ein schutzwürdiges Interesse daran besteht'.
Aus der Sicht dieses Grundrechts ist jeder der drei unter Punkt II.2.1. umschriebenen Schritte gesondert als Eingriff zu qualifizieren und daher jeweils gesondert auf seine Zulässigkeit zu prüfen. Zur Eingriffsqualität der angeführten Schritte kann auf die einschlägige Rechtsprechung des Verfassungsgerichtshofes verwiesen werden (zu Maßnahmen der Ermittlung zB VfSlg. 18.975/2009, VfGH

29.6.2012, B 1031/12, VfGH 29.9.2012, B 54/12; zur Eingriffsqualität der bloßen [weiteren] Speicherung zB VfSlg. 18.963/2009, VfGH 29.6.2012, G 7/12; zur Eingriffsqualität von Maßnahmen der Übermittlung an andere Auftraggeber siehe zB VfSlg. 17.940/2006, zur Eingriffsqualität der Unterkategorie einer Übermittlung in Form der Zweckänderung durch Überführung in ein anderes Aufgabengebiet desselben Auftraggebers - vgl. § 4 Z 12 DSG 2000 - siehe zB VfGH 11.10.2012, B 1369/11, sowie im Fall der Veröffentlichung VfSlg. 17.065/2003).
Bei den genannten Eingriffen handelt es sich jeweils nicht um Eingriffe Privater, sondern um Eingriffe durch eine 'staatliche Behörde' im Sinne des § 1 Abs. 2 DSG 2000.
Daraus folgt, dass sich die Beurteilung der Zulässigkeit dieser Eingriffe nach den in § 1 Abs. 2 DSG 2000 normierten Voraussetzungen richtet. Danach muss der Eingriff kumulativ die folgenden Voraussetzungen erfüllen:

1. Die Maßnahme muss (da es sich bei jedem der drei Schritte um einen 'Eingriff einer staatlichen Behörde' handelt) gesetzlich vorgesehen' sein, und zwar durch eine gesetzliche Regelung, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig ist.

2. Der Eingriff muss 'zur Wahrung überwiegender berechtigter Interessen' eines anderen stattfinden (§ 1 Abs. 2 DSG 2000 erster Satz).

Selbst wenn die Voraussetzungen 1. und 2. erfüllt sind, bedarf die Zulässigkeit noch der Erfüllung einer dritten Voraussetzung:

3. Die betreffende Maßnahme darf 'in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art' eingreifen (§ 1 Abs. 2 DSG 2000 letzter Satz).

Als nähere Konkretisierung der Voraussetzung 2. (Überwiegensprinzip) ist in erster Linie auf § 7 Abs. 1 sowie §§ 8 und 9 DSG 2000 zu verweisen. Als einfachgesetzliche Verankerung des bereits in § 1 Abs. 2 DSG 2000 normierten Verhältnismäßigkeitsgebots (Voraussetzung 3.) findet sich eine Regelung in § 7 Abs. 3 DSG 2000. Die Erfüllung der Voraussetzung 1., also der im öffentlichen Bereich zur Datenverwendung erforderlichen gesetzlichen 'Grundlage', wird nicht im einfachgesetzlichen Teil des DSG 2000 näher ausgeführt, sondern ist durch Auslegung des von der datenverarbeitenden Behörde zu vollziehenden materiellen und prozessualen Rechts zu ermitteln.

2.4. Der den Anlass des Gesetzesprüfungsverfahren bildende Bescheid der Datenschutzkommission enthält eine ausdrückliche Auseinandersetzung (nur) mit der ersten Voraussetzung: Er bejaht (1.) das Vorliegen einer gesetzlichen 'Ermächtigung', die er in § 140 Abs. 3 StPO lokalisiert. Zu den übrigen Eingriffsvoraussetzungen, nämlich ob der Eingriff (2.) zur Wahrung eines überwiegenden berechtigten Interesses erfolgt ist und ob der Eingriff auch (3.) auf die gelindeste zum Ziel führende Art erfolgt ist, enthält der Bescheid keine ausdrückliche Auseinandersetzung. Diese Vorgangsweise entspräche dann dem Gesetz, wenn die als 'Ermächtigung' herangezogene Gesetzesbestimmung als abschließende Regelung zu deuten wäre, die keinen Raum mehr für eine Interessenabwägung und eine Anwendung des Verhältnismäßigkeitsgrundsatzes beließe, wenn es sich also gleichsam um eine gesetzliche 'Datenverwendungspflicht jener Behörde handeln würde, die die Daten von der Strafverfolgungsbehörde erhalten hat und

wenn somit aufgrund dieser Bestimmung eine zusätzliche Prüfung anhand von §§ 7, 8 und 9 DSG 2000 gesetzlich ausgeschlossen wäre.

2.5. Wie im Folgenden zu zeigen ist, steht § 140 Abs. 3 StPO einer solchen Prüfung durch die Datenschutzkommission aber keineswegs entgegen, weil diese Vorschrift zur Verwertung von Daten in einem anderen Verfahren (zB Disziplinarverfahren) weder positiv 'ermächtigt' noch zwingt und weil sie auch keine Regelung darstellt, mit der der Gesetzgeber die Interessenabwägung bereits generell abschließend (also für die zur Verwertung in Betracht kommenden Organe der Vollziehung bindend) vorweggenommen hätte und sämtliche Kautelen des DSG 2000 vollständig verdrängt hätte.

3. Unterscheidung zwischen 'Ermächtigung' ('Grundlage') zur Datenverwendung und datenschutzrechtlichen Einschränkungen der Datenverwendung.

3.1. Das Grundrecht auf Datenschutz ist ein Grundrecht, das der Gesetzgeber durch verschiedene einfachgesetzliche Regelungen näher ausgestaltet. Bei der Beurteilung der Verfassungskonformität einer Gesetzesvorschrift am Maßstab dieses Grundrechts ist nach Auffassung der Bundesregierung zunächst zu untersuchen, ob es sich um eine Regelung zur näheren Ausgestaltung des Grundrechts handelt (also eine eingriffsbeschränkende Regelung) oder aber um eine Regelung, die zu einem Eingriff in das Grundrecht ermächtigt (zum Eingriff ermächtigende Regelungen).
Einfachgesetzliche Regelungen mit Relevanz für das Grundrecht auf Datenschutz existieren in mehrerlei Gestalt:

a. Dazu zählen etwa jene Regelungen, die näher definieren, wie die in § 1 Abs. 3 DSG 2000 geregelten Rechte (Auskunftsrecht, Löschungsrecht, etc) auszuüben sind, weiters auch Datensicherheits-, Protokollierungs-, Transparenzverpflichtungen und andere.

b. Weiters kann sich der (einfache) Gesetzgeber bei der Ausgestaltung des Grundrechts auch solcher Regelungen bedienen, die hinsichtlich der Zulässigkeit der Datenverwendung konkretere Determinanten dafür liefern, unter welchen Umständen bei der Abwägung zwischen dem Eingriffsinteresse und dem Geheimhaltungsinteresse von einem 'überwiegenden Interesse eines anderen' ausgegangen werden darf (vgl zB die §§ 8 und 9 DSG 2000; in der deutschen Literatur findet sich hierfür die Bezeichnung als allgemeine bzw. konkretisierte 'Interessenabwägungsklausel', vgl. *Tinnefeld/Buchner/Petri*, Einführung in das Datenschutzrecht, 5. Aufl, 367 f). Es handelt sich bei diesen Bestimmungen nicht um Ermächtigungen an eine staatliche Behörde im Sinne des § 1 Abs. 2 DSG 2000: Vielmehr handelt es sich um datenschutzrechtliche Regelungen, die (nicht nur im privaten Bereich, sondern – lege non distinguente –) auch bei Datenverwendungen einer staatlichen Behörde zu beachten sind, deren Anwendung die erforderliche Ermächtigung dieser Behörde aber nicht ersetzen kann (vgl. auch *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, in FS Schäffer, 335). Dies ergibt sich bereits aus den Materialien zum DSG 2000: Wenn dort ausgeführt wird, dass ein Eingriff durch eine staatliche Behörde einer 'besonderen' gesetzlichen Grundlage bedarf (1613 BlgNR 20. GP, 35), so kann nicht vom einfachgesetzlichen Teil des DSG 2000 die Rede gewesen sein. Dies findet auch Anerkennung in der Rechtsprechung des Verfassungsgerichtshofes, der den allgemeinen Regelungen des DSG 2000 die Eignung als 'Ermächtigung' abgespro-

chen hat, als er im Erkenntnis VfSlg. 1[8].643/2008 in Bezug auf eine Abstandsmessungsanlage der Straßenpolizei aussprach, dass sich 'auch aus den Regelungen der StVO betreffend die Zuständigkeit und Aufgaben der Straßenpolizeibehörden [...] in Verbindung mit den allgemeinen Grundsätzen über die Verwendung von Daten aus dem 2. Abschnitt des DSG 2000 (s. insb. §§ 6, 7, 8 DSG 2000) keine Ermächtigung zum Einsatz eines solchen [S]ystems ableiten' lässt.

c. Weiters finden sich im einfachen Gesetz stellenweise Regelungen, mit denen der Gesetzgeber die nach allgemeinem Datenschutzrecht gebotene Interessenabwägung (§ 1 Abs. 2, § 7 Abs. 3 DSG 2000) für bestimmte Falltypen und in bestimmter Hinsicht zwingend von vornherein zugunsten des Betroffenen festlegt, zB indem er bestimmte Datenverwendungsarten kategorisch verbietet oder beschränkt. Es ist freilich nicht haltbar, solche Regelungen in dem Sinn auszulegen, dass ihnen gleichsam im Umkehrschluss entnommen wird, dass sie die Anwendung aller sonstigen Kautelen, die sich sonst noch aus allgemeinen datenschutzrechtlichen Regelungen ergeben, 'verdrängen'. Ein Beispiel für diese Kategorie punktueller einfachgesetzlicher Ausgestaltungsregelungen ist zB d[a]s Verbot der Übermittlung von Daten, wenn sie aus einer unzulässigen Datenanwendung stammen (§ 7 Abs. 2 Z 1 DSG 2000) oder auch die in einzelnen Materiengesetzen enthaltenen Löschungsfristen, die die Löschung nach Ablauf einer festgelegten Frist zwingend vorsehen, während sie abgesehen von diesem Fall (also vor Fristablauf) die Pflicht zur Interessenabwägung unberührt lassen (so etwa § 58 Abs. 1 Z 6 SPG idF BGBl. 104/1997, dazu: VfSlg. 16.150/2001, beziehungsweise § 75 Abs. 3 StPO, dazu VfGH 29.6.2012, G 7/12).

d. Von den genannten Ausgestaltungsregelungen des einfachgesetzlichen Teils des DSG 2000 (und sonstiger Gesetze) streng zu unterscheiden sind jene gesetzlichen Regelungen, durch die Organe der Vollziehung zu einem Eingriff in das Grundrecht ermächtigt (bzw. verpflichtet) werden (§ 1 Abs. 2 DSG 2000 spricht hier von 'Eingriffe[n] einer staatlichen Behörde […] auf Grund von Gesetzen').

3.2. Ordnet man § 140 Abs. 3 StPO in die vorstehende Typologie von Normen mit datenschutzrechtlichem Bezug ein, so ergibt sich aus Sicht der Bundesregierung klar, dass hierbei für die Verwendung durch Behörden/Gerichte 'in anderen gerichtlichen oder verwaltungsbehördlichen Verfahren' keine 'Ermächtigung' (Typ d.) vorliegt, sondern eine Regelung, die ausschließlich zum Schutz des Betroffenen (also ausschließlich verwendungsbeschränkend) wirken soll (Typ c.) und darüber hinaus gehenden Einschränkungen (insbesondere jenen des DSG 2000) zudem nicht entgegensteht.

4. Zu Inhalt und Wirkungsweise des § 140 Abs. 3 StPO

4.1. Mit der ihrem Bescheid zugrundeliegenden Annahme, dass § 140 Abs. 3 StPO als eine 'gesetzliche Ermächtigung' der Disziplinarbehörde zur Datenverwendung zu verstehen sei, setzt sich die Datenschutzkommission in einen gewissen Widerspruch zu ihrer früheren Rechtsprechung (Bescheid vom 16.12.2005, K121.105/0004-DSK/2005), in der sie bezüglich der Ermittlung von Daten durch die Disziplinarbehörde in einem Disziplinarverfahren gegen einen Beamten des

BMI noch davon ausgegangen ist, dass 'gemäß § 105 Z 1 BDG 1979 iVm. § 38 Abs. 2 AVG [...] im Disziplinarverfahren gegen Beamte von Amts wegen vorzugehen und der Sachverhalt wahrheitsgemäß zu ermitteln [ist]'.

4.2. Auch sonst hat eine Ermächtigung der Ermittlung und Verwendung von Daten in der Form, dass Beweise erhoben werden und den Feststellungen bei Erlassung einer behördlichen Entscheidung zugrunde gelegt werden, ihren Sitz gewöhnlicherweise immer in jenen Bestimmungen, die die von dieser Behörde zu vollziehende Materie, das dafür anzuwendende Verfahren und die Organisation dieser Behörde regeln.
Auch die StPO selbst geht von dieser Systematik aus:
Die im 5. Hauptstück der StPO ('Gemeinsame Bestimmungen') enthaltene Bestimmung des § 76 Abs. 4 leg.cit. regelt, dass eine Übermittlung der im Zuge der Strafrechtspflege verarbeiteten Daten 'an andere Behörden' nur zulässig ist, 'wenn hierfür eine ausdrückliche gesetzliche Ermächtigung besteht'. Den Sitz einer solchen 'Ermächtigung' verortet der Gesetzgeber in diesem Zusammenhang naturgemäß nicht in der StPO selbst. Der Gesetzgeber meint dabei vielmehr eine Ermächtigung, die diesen anderen Behörden im jeweiligen - dh. in dem von diesen Behörden zu vollziehenden - Materiengesetz erteilt wurde (vgl. die Erläuterungen zur RV für das Strafprozessreformgesetz, BGBl. I Nr. 19/2004, 25 BlgNR, 22. GP; so auch *Pilnacek/Pleischl*, Das neue Vorverfahren, Rz 319; ebenso *Lendl*, WK-StPO [2012], § 76 Rz 22).
Wenn aber der StPO-Gesetzgeber schon im Zusammenhang mit der Übermittlung (§ 76 Abs. 4 StPO) die Ermächtigung zur außerstrafprozessualen Datenverwendung im jeweiligen Materiengesetz voraussetzt, so muss ihm dies erst recht im Kontext von § 140 Abs. 3 StPO unterstellt werden, also bei einer Bestimmung, die die (Schranken der) Weiterverwertung betrifft. Denn die Regelung der Ermächtigung einer Behörde, die ihr zuvor von anderen Behörden übermittelten oder von ihr unmittelbar selbst ermittelten Beweise bei Erlassung der behördlichen oder gerichtlichen Entscheidung zur Feststellung des Sachverhalts zu verwerten, muss in jenen Gesetzen enthalten sein, die die von dieser Behörde zu vollziehende Materie und das dazugehörige Verfahrensrecht regelt: Die grundsätzliche Erlaubnis zur Erhebung und Verwertung von Beweisen wäre also im jeweiligen Materiengesetz (verbunden mit dem entsprechenden Verfahrensgesetz) der 'anderen Behörde' zu suchen. Es ist dagegen nicht Zweck der StPO für das Ermittlungs- und Beweisverfahren vor anderen Behörden die 'Grundlage' zu bieten.

4.3. Es handelt sich daher bei § 140 Abs. 3 StPO um keine den Behörden und Gerichten erteilte 'Ermächtigung' zur Verwendung von Daten, sondern um eine Regelung, die das Vorhandensein einer solchen Ermächtigung überhaupt nicht berührt (eine solche Ermächtigung also voraussetzt) und ausschließlich die Wirkung hat, eine Datenweiterverwendung für den Fall, dass der Gesetzgeber zur Datenverwendung (im Materiengesetz) ermächtigt haben sollte, punktuell unter einem datenschutzrechtlichen Gesichtspunkt einzuschränken (nämlich unter dem Gesichtspunkt, dass die Daten aus einer zulässigen Ermittlung stammen müssen: vgl. die ähnlich wirkende Norm des § 7 Abs. 2 Z 1 DSG 2000 hinsichtlich der Zulässigkeit von Übermittlungen).

4.4. Anhaltspunkte dafür, dass die Regelung dadurch gleichzeitig auch die Anwendung aller sonstigen relevanten datenschutzrechtlichen Gesichtspunkte (wie insbesondere das Überwiegensprinzip, das Erforderlichkeitsprinzip und den Verhältnismäßigkeitsgrundsatz [§ 7 Abs. 3 DSG 2000] verdrängen und die weiterverwendende Behörde von der Beachtung dieser Regeln entbinden wollte, sind für die Bundesregierung nicht erkennbar. Der Inhalt der Regelung nimmt keineswegs sämtliche Gesichtspunkte der durch § 1 Abs. 2 DSG 2000 gebotenen Interessenabwägung vorweg. Er regelt nur eine Voraussetzung (von mehreren). § 140 Abs. 3 StPO ist daher keine abschließende Regelung und verdrängt insbesondere auch nicht die Beschränkungen, die sich im Anlassfall für die Disziplinarbehörde aus dem Überwiegensprinzip des § 1 Abs. 2 DSG 2000 (§ 7 Abs. 1, § 8 Abs. 1 Z 4 DSG 2000), aus dem Übermaßverbot des § 7 Abs. 3 DSG 2000 und den sonstigen datenschutzrechtlichen Prinzipien wie dem Erforderlichkeits- und Zweckbindungsgrundsatz ergeben hätten.

4.5. Es wäre im Übrigen auch kaum möglich, bereits in der StPO eine abschließende Regelung zu treffen, die sämtliche Fälle einer Datenweiterverwendung in umfassender Weise so regeln könnte, dass sämtliche Aspekte der Interessenabwägung generell-abstrakt schon vom StPO-Gesetzgeber 'abgehandelt' wären und eine weitere Abwägung durch den (für die Weiterverwendung zuständigen) Materiengesetzgeber ausgeschlossen (oder 'verdrängt') wäre. Auch aus diesem Grund kann § 140 Abs. 3 StPO nicht in dieser Weise verstanden werden.
Es kann für den Zweck dieses - auf § 140 Abs. 3 StPO beschränkten - Gesetzesprüfungsverfahrens offen bleiben, ob die gesetzliche Grundlage für das Beweisverfahren vor Disziplinarbehörden aufgrund des BDG 1979 (iVm dem AVG) auch die Weiterverwendung von Ergebnissen aus dem Einsatz der vergleichsweise eingriffsintensiven Ermittlungsbefugnisse der StPO erlauben würde. Ob die von den Disziplinarbehörden anzuwendenden Regelungen des BDG 1979 in Verbindung mit dem AVG über das Beweisverfahren (Ermittlung und Verwertung von Beweisen von Amts wegen, Unbeschränktheit der Beweismittel, etc) eine ausreichende gesetzliche Grundlage für den von der Datenschutzkommission zu beurteilenden Informationseingriff darstellen konnten, wäre im Wege der Auslegung dieser Bestimmungen zu beurteilen gewesen. Sollte eine entsprechende gesetzliche Grundlage fehlen (oder nicht ausreichen), so führt dies nach der bisherigen Rechtsprechung des Verfassungsgerichtshofes nicht zur Verfassungswidrigkeit des betreffenden Gesetzes (hier: des BDG), sondern bloß zur Unzulässigkeit des in Rede stehenden Informationseingriffs (VfSlg. 18.643/2008, 18.922/2009, 18.987/2010). Auch § 140 Abs. 3 StPO wäre in diesem Fall nicht verfassungswidrig, sondern lediglich inoperativ, weil für eine Datenverwendung, auf die er anwendbar wäre, schon auf vorgelagerter Stufe die Grundlage fehlte. (Was freilich nicht bedeutet dass § 140 Abs. 3 StPO immer inoperativ wäre, zumal ja das Vorhandensein einer spezifischen Ermächtigung für andere Zwecke als für Disziplinarverfahren und in anderen Materiengesetzen als dem BDG 1979 denkbar wäre).
Es handelt sich bei dieser Problematik im Übrigen um keine Besonderheit von personenbezogenen Daten, die ursprünglich im gerichtlichen Strafprozess ermittelt worden sind, sondern um eine allgemeine Frage der Auslegung und Anwendung von § 46 AVG in Situationen, in denen die Beweisverwertung eine gesetz-

lich oder auch (zB) grundrechtlich geschützte Position verletzen könnte (vgl. zur Annahme von Verwertungsverboten bei Auslegung von § 46 AVG *Thienel/ Schulev-Steindl*, Verwaltungsverfahrensrecht[5], 190 f). Denn die gleichgelagerte Problematik der Abgrenzung zwischen Zulässigkeit und Unzulässigkeit des in der Verwendung bestehenden Informationseingriffs stellt sich nicht nur hinsichtlich der Verwertbarkeit von Daten mit Ursprung in gerichtlichen Ermittlungen, sondern naturgemäß (und umso dringlicher!) auch hinsichtlich der Verwertbarkeit von Beweisen, die der Behörde zwar vorliegen, aber auf - vergleichbar eingriffsintensive - illegale Überwachungsmaßnahmen zB von Privaten oder von dazu nicht ermächtigten Behörden zurückgehen, so etwa im Fall geheimer Videoüberwachungen, illegaler Computerzugriffe, etc (vgl. zB *Baurecht*, Verwendung und Verwertung von rechtswidrig erlangten Beweismitteln - Zivilprozessuale und datenschutzrechtliche Grenzen, NetV 2006, 97; *Schenk*, Schranken der Verwertung rechtswidrig erlangter Beweismittel im Abgabenverfahren, taxlex 2010, 433; *Kodek*, Die Verwertung rechtswidriger Tonbandaufnahmen und Abhörergebnisse im Zivilverfahren, ÖJZ 2001, 281, 287, 334).

4.6. Wie ausgeführt, kämen als 'Grundlage' des Eingriffs zwar nicht § 140 Abs. 3 StPO, sondern (wenn überhaupt) nur die nach dem BDG 1979 für das Disziplinarverfahren maßgeblichen gesetzlichen Grundlagen der Beweiserhebung und Beweisverwertung in Betracht. Diese beruhen auf dem Prinzip der Unbeschränktheit der Beweismittel (§ 46 AVG).
Selbst wenn man die (wie unter Pkt. II.4.5. erwähnt: hier dahingestellt bleibende) Annahme zugrunde legen würde, dass sich aus den allgemeinen Regelungen über das Ermittlungsverfahren nach dem BDG iVm dem AVG eine 'Ermächtigung' zur Verwendung (auch) solcher Daten ergeben kann, die ursprünglich durch Ermittlung innerhalb des Aufgabenbereichs der Strafverfolgungsbehörden gewonnen worden sind, ist Folgendes zu berücksichtigen: Ob die Ausübung dieser Ermächtigung durch die Disziplinarbehörde angesichts der Sensibilität und gesetzlichen Sonderstellung von Ergebnissen einer geheimen Rufdatenrückerfassung auch mit den übrigen datenschutzrechtlichen Erfordernissen (insbesondere der Abwägung nach dem Überwiegensprinzip des § 7 Abs. 1 DSG und dem Verhältnismäßigkeitsgrundsatz nach § 7 Abs. 3 DSG) in Einklang stand, hätte die Disziplinarbehörde durch Anwendung des DSG 2000 zu beurteilen und allenfalls mit entsprechenden Rechtsfolgen (ggf. Nichtverwendung) zu sanktionieren gehabt.
§ 140 Abs. 3 StPO wäre dieser Beurteilung aber in keiner Weise entgegengestanden. Daher können die Bedenken, der Gesetzgeber 'ermächtige' in undifferenzierter Weise und ohne Rücksicht auf die Gewichtung der in Betracht kommenden Interessen zur Weiterverwendung, auf § 140 Abs. 3 StPO nicht zutreffen.

4.7. Eben diese Interessenabwägung hätte daher auch Thema des Verfahrens vor der Datenschutzkommission sein können, wenn sie die allgemeine Ermächtigung zur Verwertung personenbezogener Daten in § 46 AVG (iVm § 105 BDG 1979) als ausreichende Grundlage erblickt hätte und wenn sie diese Ermächtigung in einer mit dem datenschutzrechtlichen Verhältnismäßigkeitsgrundsatz kompatiblen Weise verstanden hätte. Im Rahmen der gebotenen Interessenabwägung wäre es ihr möglich gewesen, den Umstand zu berücksichtigen, dass die strittigen Beweise ursprünglich in einem gerichtlichen Strafverfahren unter Inanspruchnahme spezifischer Eingriffsbefugnisse der Strafverfolgungsbehörden ermittelt worden sind, die durch wesentlich höher zu gewichtende Eingriffsinteressen der

Verfolgung schwerwiegender Straffälle (vgl. § 135 Abs. 2 StPO) legitimiert sind und gerade angesichts dieser gesetzgeberischen Wertung einem engen Korsett prozessualer Voraussetzungen der StPO (§ 137 StPO) unterliegen, während nunmehr die Weiterverwendung für den Zweck eines anders zu gewichtenden Eingriffsinteresses (Verfolgung von Disziplinarvergehen) zu prüfen gewesen wäre.

4.8. Die Bundesregierung vermag im Übrigen der Prämisse nicht zuzustimmen, dass die Verhinderung von Grundrechtsverletzungen, die darin bestehen, dass Daten ohne überwiegendes öffentliches Interesse verwendet werden, nur Sache des Gesetzgebers sei. Gerade das in Rn 30 des Prüfungsbeschlusses zitierte Erkenntnis VfSlg. 18.975/2009 belegt, dass - je nach Eingriffsintensität - durchaus auch weniger spezifisch formulierte gesetzliche Ermächtigungen zur Datenverwendung verfassungskonform wären, dass es aber auch in diesen Fällen Aufgabe der Vollziehung ist, bei Ausübung der Ermächtigung zur Datenverwendung Sorge dafür zu tragen, dass der Informationseingriff den Ansprüchen des § 1 Abs. 2 DSG 2000 genügt. Der Verfassungsgerichtshof hatte im zitierten Erkenntnis keineswegs Zweifel an der Verfassungsmäßigkeit der gesetzlichen Grundlage (zB mangels fehlender Einschränkungen). Er verlangte darin von der Vollziehung, dass sie eine - allgemein gehaltene - gesetzliche Ermächtigung so ausübt dass der Eingriff durch ein überwiegendes Interesse anderer getragen ist und in der gelindest möglichen Weise erfolgt.

4.9. § 140 Abs. 3 StPO entfaltet somit keine Sperrwirkung gegen zusätzliche, ergänzende Beschränkungen der Verwertbarkeit bei der Datenweiterverwendung durch andere Behörden und Gerichte. Aus diesem Grund ist es auch naheliegend, dass in jenem Bereich, in dem sich § 140 Abs. 3 StPO und § 75 Abs. 5 StPO auf der Tatbestandsebene überschneiden, kumulativ die speziellere (auf der Sanktionsebene strengere) Rechtsfolge des § 75 Abs. 5 StPO anzuwenden ist, denn auch diese wird durch die insofern generellere Norm des § 140 Abs. 3 StPO nicht verdrängt. Bei § 75 Abs. 5 StPO handelt es sich, abweichend von § 140 Abs. 3 StPO um eine Regelung, die zusätzliche Aspekte der datenschutzrechtlichen Interessenabwägung behandelt und Regelungen des DSG insofern - aber ebenfalls nur partiell - verdrängt. Die Verdrängung des DSG 2000 ist schon deswegen auch im Fall des § 75 Abs. 5 StPO nur partiell, weil auch im Anwendungsbereich dieser Norm eine Datenweiterverwendung nicht zwingend angeordnet ist (sondern nur eine Bedingung für ihre Zulässigkeit geregelt wird) und weil auch im Rahmen der Auslegung von § 75 Abs. 5 StPO der unbestimmte Gesetzesbegriff des 'Zusammenhangs' auszulegen sein wird: Dabei wird die zur Weiterverwendung berechtigte Verwaltungsbehörde (das weiter verwendende Gericht) im Lichte des DSG 2000 zu prüfen haben, ob und inwieweit es von einem 'damit in Zusammenhang stehenden Zivil- oder Verwaltungsverfahren' ausgehen darf. Die Reichweite des 'Zusammenhangs' wird bei grundrechtskonformem Verständnis selbstverständlich nur jene Fälle erfassen dürfen, in denen davon ausgegangen werden kann, dass die Verwendung durch 'überwiegende Interessen eines anderen' im Sinne des § 1 Abs. 2 DSG 2000 gerechtfertigt ist.

4.10. Als Zwischenergebnis ist festzuhalten: Die Stoßrichtung der Regelung des § 140 Abs. 3 StPO ist nicht 'autorisierend' in dem Sinn, dass sie die 'Grundlage' (im Sinne des in § 1 Abs. 2 DSG 2000 verwendeten Begriffs 'auf Grund von Gesetzen') für eine Datenverwendung durch eine Verwaltungsbehörde oder ein anderes Gericht bieten könnte, sondern ist ausschließlich 'prohibitiv' in dem Sinne zu verstehen, dass sie - selbst im Fall existierender materiengesetzlicher 'Grundlage' einer Datenweiterverwendung durch andere Behörden - gegenüber der fraglichen Datenverwendung Schranken aufstellt.

4.11. Dazu kommt, dass § 140 Abs. 3 StPO seine beschränkende Wirkung keineswegs exklusiv entfaltet:
Denn es handelt sich nur um eine Beschränkung, die nicht hindert, dass andere (datenschutzrechtliche) Beschränkungen kumulativ zur Anwendung kommen. § 140 Abs. 3 StPO führt daher keinesfalls dazu, dass der Gesetzgeber unter dem Gesichtspunkt des datenschutzrechtlichen Interessenabwägungsgebots nicht auch noch kumulativ - insbesondere im DSG 2000 - Schranken vorsehen dürfte. Zusätzliche gesetzliche Schranken bestehen in der Tat: Das Datenschutzgesetz fordert sowohl bei der Ermittlung als auch der weiteren Verwendung (einschließlich der Beweisverwertung) von personenbezogenen Daten durch eine Verwaltungsbehörde (neben dem Vorhandensein einer gesetzlichen Grundlage) insbesondere die Beachtung des Gesetzmäßigkeits-, des Erforderlichkeits- und des Zweckbindungsprinzips (§ 6 Abs. 1 Z 2 und 3, § 7 Abs. 1 DSG 2000), sowie des Grundsatzes, dass die Datenverwendung nur dann stattfinden darf, wenn dadurch 'die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden' (§ 7 Abs. 1 DSG 2000).

4.12. Gerade im Rahmen der - neben der gesetzlichen Grundlage - erforderlichen Interessenabwägung müssen aber auch die dem Geheimhaltungsinteresse des Betroffenen entgegenstehenden Interessen an einer Weiterverwendung richtig gewichtet werden: Die Bundesregierung geht davon aus, dass das Grundrecht auf Datenschutz die Weiterverwendung von personenbezogenen Daten der hier in Rede stehenden Kategorien nicht generell verbietet. Ein generelles verfassungsrechtliches Verwertungsverbot auch für jene Fälle, in denen Daten im Strafprozess rechtmäßig gewonnen wurden und nach Prüfung der strengen Voraussetzungen der §§ 75 Abs. 5 und 140 Abs. 3 StPO durch die zuständige Staatsanwaltschaft an ein Gericht oder eine Verwaltungsbehörde übermittelt worden sind, kann aus § 1 DSG nicht abgeleitet werden. Die Annahme eines (keiner Interessenabwägung im Einzelfall zugänglichen) Verbots würde den öffentlichen Interessen, denen das betreffende 'andere' Materiengesetz dienen soll (so zB dem Interesse auf Sicherstellung der Aufklärung auch der disziplinarrechtlichen Aspekte eines Sachverhalts) entgegenstehen. Das öffentliche Interesse (oder das Interesse eines am 'anderen Verfahren' beteiligten Dritten) kann fallbezogen höher zu bewerten sein als jenes des Betroffenen auf Geheimhaltung bzw. Löschung seiner personenbezogenen Daten. Keinen Einfluss auf die Bewertung des öffentlichen Interesses hat dabei die Frage, ob das den Anlass der zulässigen Datenermittlung bildende Strafverfahren zum Zeitpunkt der fraglichen Weiterverwendung bereits rechtskräftig beendet ist bzw. ob die Daten im Strafakt inzwischen schon gelöscht worden sind.

5. Zum Anwendungsbereich von § 75 Abs. 5 und § 140 Abs. 3 StPO im Detail:

5.1. Je nach der Intensität eines Eingriffs in das Grundrecht auf Datenschutz und je nach Schutzwürdigkeit der verarbeiteten personenbezogenen Daten bedarf es gemäß § 1 Abs. 2 DSG 2000 der Festlegung angemessener Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen. Solche Garantien können etwa in gesetzlich vorgesehenen Verwendungsbeschränkungen liegen (*Dohr/Pollirer/Weiss/Knyrim*, DSG$^2$ § 1 Anm 19).
Eben eine solche den Erfordernissen des § 1 Abs. 2 DSG 2000 Rechnung tragende Beschränkung normiert § 75 Abs. 5 StPO unter anderem dadurch, dass eine Schranke der Datenverwendung jedenfalls dort eingezogen wird, wo ein inhaltlicher Zusammenhang zwischen dem Strafverfahren, in dem die Daten ermittelt wurden und jenem Zivil- oder Verwaltungsverfahren, in dem diese Verwendung finden sollen, fehlt.

5.2. Der in § 75 Abs. 5 StPO in Anlehnung an die Terminologie der §§ 149a ff StPO idF vor Inkrafttreten des Strafprozessreformgesetzes BGBl. I Nr. 19/2004 am 1. Jänner 2008 verwendete Begriff der 'Überwachung von Nachrichten' ist angesichts des Charakters der Regelung als Eingriffsschranke (im Gegensatz zu Eingriffsermächtigungen) nicht restriktiv sondern weit zu verstehen. Der Begriff umfasst im weiteren Sinn nicht nur das Ermitteln des Inhalts von Nachrichten (§ 92 Abs. 3 Z 7 TKG), die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) ausgetauscht oder weitergeleitet werden (§ 134 Z 3 StPO), sondern schon grundsätzlich auch die 'Auskunft über Daten einer Nachrichtenermittlung', somit die Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG), die nicht einer Anordnung gemäß § 76a Abs. 2 unterliegen, und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) und seit BGBl. I Nr. 33/2011 die 'Auskunft über Vorratsdaten', also die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe des § 102a Abs. 2 bis 4 TKG zu speichern haben und die nicht nach § 99 Abs. 2 TKG einer Auskunft nach Z 2 unterliegen (§ 134 Z 2 und 2a StPO idF BGBl. I Nr. 33/2011). Diesem umfassenden Verständnis des Begriffs der 'Überwachung von Nachrichten' trägt auch die Praxis insofern Rechnung, als bei Durchführung einer (gerichtlich bewilligten) staatsanwaltschaftlichen Anordnung zur Überwachung von Nachrichten (§ 135 Abs. 3 iVm § 137 Abs. 1 StPO) etwa stets die betreffenden Verkehrsdaten mitübermittelt werden.
Demgemäß ist die 'Überwachung von Nachrichten' nach § 75 Abs. 5 StPO als in Anlehnung an die Gesetzesterminologie vor Inkrafttreten des Strafprozessreformgesetzes BGBl. I Nr. 19/2004 gewählter Überbegriff über die 'Auskunft über Daten einer Nachrichtenermittlung' (§ 134 Z 2 StPO), der 'Auskunft über Vorratsdaten' (§ 134 Z 2a StPO) und der 'Überwachung von Nachrichten' (§ 134 Z 5 StPO: 'Überwachung des Inhalts übertragener Nachrichten', § 134 Z 3 StPO) zu verstehen, woraus die begriffliche Gleichsetzung der in §§ 75 Abs. 5 und 140 Abs. 3 StPO genannten Ermittlungsmaßnahmen folgt.

5.3. Der in § 75 Abs. 5 StPO gebrauchte Begriff der 'optischen oder akustischen Überwachung' umfasst die Überwachung des Verhaltens von Personen unter Durchbrechung ihrer Privatsphäre und der Äußerungen von Personen, die nicht

zur unmittelbaren Kenntnisnahme Dritter bestimmt sind, unter Verwendung technischer Mittel zur Bild- oder Tonübertragung und zur Bild- oder Tonaufnahme ohne Kenntnis der Betroffenen (§ 134 Z 4 StPO) und entspricht der in § 134 Z 5 StPO ergebnisbezogenen Bezeichnung der 'Bild- und Tonaufnahme einer Überwachung'.
Für die Überwachung von Nachrichten im weiteren Sinn sowie die optische und akustische Überwachung von Personen existiert somit ein Überschneidungsbereich, weil sowohl § 140 Abs. 3 StPO als auch § 75 Abs. 5 StPO Regelungen dahingehend vorsehen, unter welchen Voraussetzungen ermittelte Daten verwendet werden dürfen. Im Verhältnis der Bestimmungen zueinander ist die unmittelbar den Einsatz von Informationstechnik regelnde Norm des § 75 Abs. 5 StPO als lex specialis zu betrachten. Überdies ist sie lex posterior, bestand doch mit § 149h Abs. 3 eine § 140 Abs. 3 StPO entsprechende strafprozessuale Regelung bereits vor dem Inkrafttreten des Strafprozessreformgesetzes BGBl. I Nr. 19/2004 am 1. Jänner 2008.
Vor diesem Hintergrund ist in den genannten Bereichen die Datenverwendung insofern zu beschränken, als Daten, deren Verwendung im Strafverfahren zulässig war oder wäre, in Zivil- oder Verwaltungsverfahren lediglich dann Verwendung finden dürfen, wenn diese Verfahren mit dem Strafverfahren in einem inhaltlichen Zusammenhang stehen (vgl *Reindl-Krauskopf*, WK-StPO § 140 Rz 29). Im Sinne dieser schon aus der einschlägigen Kommentierung ersichtlichen Einschränkung erfüllt neben § 75 Abs. 5 StPO auch § 140 Abs. 3 StPO die durch § 1 Abs. 2 DSG 2000 vorgegebenen Schranken der Statthaftigkeit eines Eingriffs in das Grundrecht auf Datenschutz.

5.4. Bei einer ausschließlich am Wortlaut haftenden Betrachtung würde sich die Verwendung der Ergebnisse einer Beschlagnahme von Briefen für andere gerichtliche (verwaltungsbehördliche) Verfahren als jenes wegen der Anlasstat ausschließlich nach § 140 Abs. 3 StPO richten. Zwar ist der mit dieser Maßnahme einhergehende Grundrechtseingriff mit jenem einer technisch unterstützten geheimen Maßnahme bei der Überwachung von Nachrichten oder der optischen oder akustischen Überwachung von Personen nicht vollkommen identisch. Da es sich dabei jedoch ebenso um die (verdeckte) Ermittlung von Kommunikationsinhalten handelt, erweist sich die Maßnahme als ähnlich eingriffsintensiv. Infolge der grundsätzlichen Kongruenz von §§ 140 Abs. 3 und 75 Abs. 5 StPO muss in der fehlende Bezugnahme auf die Beschlagnahme von Briefen in § 75 Abs. 5 StPO daher eine durch Analogie zu schließende planwidrige Lücke gesehen werden. Die Planwidrigkeit dieser Lücke wird umso deutlicher, wenn darauf Bedacht genommen wird, dass § 75 Abs. 5 StPO im Kern eine Regelung ist, die nur in spezifischer Weise einen Gedanken zum Ausdruck bringt, der bereits in allgemeiner Weise dem Verhältnismäßigkeitsgrundsatz des DSG 2000 zugrunde liegt.
Im Ergebnis sind die Verwendungsbeschränkungen des § 75 Abs. 5 StPO daher auch bei der Verwendung der durch die Beschlagnahme von Briefen gewonnenen Daten maßgebend. Sämtliche der in § 135 Z 1 bis 4 StPO aufgezählten Ermittlungsmaßnahmen sind von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen, lediglich eine Überwachung nach § 136 Abs. 1 Z 1 StPO kann die Kriminalpolizei von sich aus durchführen (§ 137 Abs. 1 StPO). Auftraggeber der Datenanwendung nach § 4 Z 4 DSG 2000, wozu jede Art der Datenhandhabung, sohin auch die Übermittlung von Daten (§ 4 Z 8 und 12 DSG 2000) zählt, ist daher allein die zuständige Staatsanwaltschaft. Es obliegt daher

zunächst der Staatsanwaltschaft, im Lichte der durch §§ 75 Abs. 5 und 140 Abs. 3 StPO zum Ausdruck gebrachten Verwendungsbeschränkungen, vorausschauend die Zulässigkeit einer Weitergabe rechtmäßig ermittelter Daten an Gerichte und Verwaltungsbehörden im Lichte der diesen Behörden zugewiesenen Befugnisse und Aufgaben zu prüfen und es obliegt sodann diesen Gerichten und Verwaltungsbehörden, im Rahmen der Wahrnehmung ihrer Aufgaben (abschließend) über die Zulässigkeit der Verwertung dieser Daten zu entscheiden.

6. Zusammenfassung

§ 140 Abs. 3 StPO ist nur eine Schranke der Datenweiterverwendung. § 140 Abs. 3 StPO ist - für sich genommen - keine ausreichende Ermächtigung zur Datenweiterverwendung durch andere Behörden und Gerichte. § 140 Abs. 3 StPO kommt kumulativ zur Anwendung und verdrängt zusätzliche datenschutzrechtliche Beschränkungen der Datenweiterverwendung nicht. Für sämtliche der von § 140 Abs. 3 StPO erfassten Datenkategorien (dh. auch für die 'Auskunft über Daten einer Nachrichtenermittlung' und beschlagnahmte Briefe) kommt zusätzlich die Schranke des § 75 Abs. 5 StPO zur Anwendung. § 140 Abs. 3 StPO steht im Einzelfall einer Prüfung dahingehend, ob ein Materiengesetz existiert, das die Weiterverwendung (in hinreichender Weise) erlaubt, nicht entgegen. § 140 Abs. 3 StPO steht auch der bei Anwendung einer solchen Ermächtigung vorzunehmenden Interessenabwägung nicht entgegen.
Zusammenfassend wird daher festgehalten, dass § 140 Abs. 3 der Strafprozessordnung 1975, BGBl. Nr. 631 idF BGBl. I Nr. 19/2004, nach Ansicht der Bundesregierung nicht verfassungswidrig ist."

Der Verfassungsgerichtshof hat am 12. Juni 2013 eine öffentliche mündliche Verhandlung durchgeführt. 8

## II. Rechtslage

1. Die maßgeblichen Vorschriften des DSG 2000, BGBl. I 165/1999 idF BGBl. I 133/2009, lauten: 9

"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 Art. 8 Abs. 2 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. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(5) Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung zuständig, es sei denn, daß Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind."

"Artikel 2
1. Abschnitt
Allgemeines

Definitionen

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

1. 'Daten' ('personenbezogene Daten'): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; 'nur indirekt personenbezogen' sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) 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. – 3. […]

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 zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden;

5. – 7. […]

8. Verwenden von Daten: jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;

9. Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten;

10. – 11. […]

12. Übermitteln von Daten: die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;

13. – 15. […]"

"2. Abschnitt
Verwendung von Daten"

"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) Daten dürfen nur übermittelt werden, wenn

1. sie aus einer gemäß Abs. 1 zulässigen Datenanwendung stammen und

2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis - soweit diese nicht außer Zweifel steht - im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und

3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

(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) Schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder
2. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
3. lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder
4. überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.

(2) Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung zulässigerweise veröffentlichter Daten gemäß § 28 Widerspruch zu erheben, bleibt unberührt.

(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 Abs. 2 - 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 oder
4. die Datenweitergabe zum Zweck der Erstattung einer Anzeige an eine zur Verfolgung der angezeigten strafbaren Handlungen (Unterlassungen) zuständige Behörde erfolgt."

2. Die relevanten Bestimmungen der StPO, BGBl. 631/1975, haben in der hier maßgeblichen Fassung BGBl. I 52/2009 folgenden Wortlaut (die in Prüfung gezogene Bestimmung ist hervorgehoben): 10

"1. Teil
Allgemeines und Grundsätze des Verfahrens"

"5. Hauptstück
Gemeinsame Bestimmungen

1. Abschnitt
Einsatz der Informationstechnik

Verwenden von Daten

§ 74. (1) Soweit zum Verwenden von Daten im Einzelnen nichts anderes bestimmt wird, finden die Bestimmungen des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999, Anwendung.

(2) Kriminalpolizei, Staatsanwaltschaft und Gericht haben beim Verwenden (Verarbeiten und Übermitteln) personenbezogener Daten den Grundsatz der Gesetz- und Verhältnismäßigkeit (§ 5) zu beachten. Jedenfalls haben sie schutzwürdige Interessen der Betroffenen an der Geheimhaltung zu wahren und vertraulicher Behandlung der Daten Vorrang einzuräumen. Beim Verwenden sensibler und strafrechtlich relevanter Daten haben sie angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen.

Berichtigen, Löschen und Sperren von Daten

§ 75. (1) Unrichtige oder entgegen den Bestimmungen dieses Gesetzes ermittelte Daten sind unverzüglich richtig zu stellen oder zu löschen.

(2) – (4) […]

(5) Soweit Daten, die durch eine Überwachung von Nachrichten, eine optische oder akustische Überwachung oder einen automationsunterstützten Datenabgleich ermittelt worden sind, in einem Strafverfahren als Beweis verwendet werden dürfen, ist ihre Verwendung auch in einem damit in Zusammenhang stehenden Zivil- oder Verwaltungsverfahren und zur Abwehr mit beträchtlicher Strafe bedrohter Handlungen (§ 17 SPG) sowie zur Abwehr erheblicher Gefahren für Leben, Leib oder Freiheit einer Person oder für erhebliche Sach- und Vermögenswerte zulässig.

2. Abschnitt
Amts- und Rechtshilfe, Akteneinsicht

Amts- und Rechtshilfe

§ 76. (1) – (3) […]

(4) Kriminalpolizei, Staatsanwaltschaften und Gerichte sind berechtigt, über nach diesem Gesetz ermittelte personenbezogene Daten Auskunft für Zwecke der Sicherheitsverwaltung, der Strafrechtspflege sowie der Kontrolle der Rechtmäßigkeit des Handelns der genannten Organe zu erteilen. Übermittlungen von Daten an andere Behörden als Finanzstrafbehörden für deren Tätigkeit im

Dienste der Strafrechtspflege, Sicherheitsbehörden, Staatsanwaltschaften und Gerichte sind im Übrigen nur zulässig, wenn hierfür eine ausdrückliche gesetzliche Ermächtigung besteht.

(5) […]"

"2. Teil
Das Ermittlungsverfahren"

8. Hauptstück
Ermittlungsmaßnahmen und Beweisaufnahme

5. Abschnitt
Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung sowie Überwachung von Nachrichten und von Personen

Definitionen

§ 134. Im Sinne dieses Bundesgesetzes ist

1. 'Beschlagnahme von Briefen' das Öffnen und Zurückbehalten von Telegrammen, Briefen oder anderen Sendungen, die der Beschuldigte abschickt oder die an ihn gerichtet werden,

2. 'Auskunft über Daten einer Nachrichtenübermittlung' die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG) und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes),

3. 'Überwachung von Nachrichten' das Ermitteln des Inhalts von Nachrichten (§ 92 Abs. 3 Z 7 TKG), die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) ausgetauscht oder weitergeleitet werden,

4. 'optische und akustische Überwachung von Personen' die Überwachung des Verhaltens von Personen unter Durchbrechung ihrer Privatsphäre und der Äußerungen von Personen, die nicht zur unmittelbaren Kenntnisnahme Dritter bestimmt sind, unter Verwendung technischer Mittel zur Bild- oder Tonübertragung und zur Bild- oder Tonaufnahme ohne Kenntnis der Betroffenen,

5. 'Ergebnis' (der unter Z 1 bis 4 angeführten Beschlagnahme, Auskunft oder Überwachung) der Inhalt von Briefen (Z 1), die Daten einer Nachrichtenübermittlung oder des Inhalts übertragener Nachrichten (Z 2 und 3) und die Bild- oder Tonaufnahme einer Überwachung (Z 4).

Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung sowie Überwachung von Nachrichten

§ 135. (1) Beschlagnahme von Briefen ist zulässig, wenn sie zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, erforderlich ist und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde.

(2) Auskunft über Daten einer Nachrichtenübermittlung ist zulässig,

1. wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird,

2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder

3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.

(3) Überwachung von Nachrichten ist zulässig,

1. in den Fällen des Abs. 2 Z 1,

2. in den Fällen des Abs. 2 Z 2, sofern der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Überwachung zustimmt,

3. wenn dies zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, erforderlich erscheint oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten strafbaren Handlungen ansonsten wesentlich erschwert wäre und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, dringend verdächtig ist, die Tat begangen zu haben oder zu planen,

4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

### Optische und akustische Überwachung von Personen

§ 136. (1) Die optische und akustische Überwachung von Personen ist zulässig,

1. wenn und solange der dringende Verdacht besteht, dass eine von der Überwachung betroffene Person eine andere entführt oder sich ihrer sonst bemächtigt hat, und sich die Überwachung auf Vorgänge und Äußerungen zur Zeit und am Ort der Freiheitsentziehung beschränkt,

2. wenn sie sich auf Vorgänge und Äußerungen beschränkt, die zur Kenntnisnahme eines verdeckten Ermittlers oder sonst einer von der Überwachung informierten Person bestimmt sind oder von dieser unmittelbar wahrgenommen werden können, und sie zur Aufklärung eines Verbrechens (§ 17 Abs. 1 StGB) erforderlich scheint oder

3. wenn die Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder des Verbrechens der kriminellen Organisation oder der terroristischen Vereinigung (§§ 278a und 278b StGB) oder die Aufklärung oder Verhinderung von im Rahmen einer solchen Organisation oder Vereinigung begangenen oder geplanten strafbaren Handlungen oder die Ermittlung des Aufenthalts des wegen einer solchen Straftat Beschuldigten ansonsten aussichtslos oder wesentlich erschwert wäre und

a. die Person, gegen die sich die Überwachung richtet, des mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder eines Verbrechens nach § 278a oder § 278b StGB dringend verdächtig ist oder

b. auf Grund bestimmter Tatsachen anzunehmen ist, dass ein Kontakt einer solcherart dringend verdächtigen Person mit der Person hergestellt werde, gegen die sich die Überwachung richtet.

(2) […]

(3) Die optische Überwachung von Personen zur Aufklärung einer Straftat ist überdies zulässig,

1. wenn sie sich auf Vorgänge außerhalb einer Wohnung oder anderer durch das Hausrecht geschützter Räume beschränkt und ausschließlich zu dem Zweck erfolgt, Gegenstände oder Örtlichkeiten zu beobachten, um das Verhalten von Personen zu erfassen, die mit den Gegenständen in Kontakt treten oder die Örtlichkeiten betreten, oder

2. wenn sie ausschließlich zu dem in Z 1 erwähnten Zweck in einer Wohnung oder anderen durch das Hausrecht geschützten Räumen erfolgt, die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, ansonsten wesentlich erschwert wäre und der Inhaber dieser Wohnung oder Räume in die Überwachung ausdrücklich einwilligt.

(4) Eine Überwachung ist nur zulässig, soweit die Verhältnismäßigkeit (§ 5) gewahrt wird. Eine Überwachung nach Abs. 1 Z 3 zur Verhinderung von im Rahmen einer terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278a und 278b StGB) begangenen oder geplanten Straftaten ist überdies nur dann zulässig, wenn bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen.

Gemeinsame Bestimmungen

§ 137. (1) Eine Überwachung nach § 136 Abs. 1 Z 1 kann die Kriminalpolizei von sich aus durchführen. Die übrigen Ermittlungsmaßnahmen nach den §§ 135 und 136 sind von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen, wobei das Eindringen in Räume nach § 136 Abs. 2 jeweils im Einzelnen einer gerichtlichen Bewilligung bedarf.

(2) Bei der Beschlagnahme von Briefen sind die §§ 111 Abs. 4 und 112 sinngemäß anzuwenden.

(3) Ermittlungsmaßnahmen nach den §§ 135 und 136 dürfen nur für einen solchen künftigen, in den Fällen des § 135 Abs. 2 auch vergangenen, Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks voraussichtlich erforderlich

ist. Eine neuerliche Anordnung ist jeweils zulässig, soweit auf Grund bestimmter Tatsachen anzunehmen ist, dass die weitere Durchführung der Ermittlungsmaßnahme Erfolg haben werde. Im Übrigen ist die Ermittlungsmaßnahme zu beenden, sobald ihre Voraussetzungen wegfallen."

"§ 140. (1) Als Beweismittel dürfen Ergebnisse (§ 134 Z 5), bei sonstiger Nichtigkeit nur verwendet werden,

1. wenn die Voraussetzungen für die Ermittlungsmaßnahme nach § 136 Abs. 1 Z 1 vorlagen,

2. wenn die Ermittlungsmaßnahme nach den §§ 135 oder 136 Abs. 1 Z 2 oder 3 oder Abs. 3 rechtmäßig angeordnet und bewilligt wurde (§ 137), und

3. in den Fällen des § 136 Abs. 1 Z 2 und 3 nur zum Nachweis eines Verbrechens (§ 17 Abs. 1 StGB),

4. in den Fällen der §§ 135 Abs. 1, Abs. 2 Z 2 und 3, Abs. 3 Z 2 bis 4 nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, deretwegen die Ermittlungsmaßnahme angeordnet wurde oder hätte angeordnet werden können.

(2) Ergeben sich bei Prüfung der Ergebnisse Hinweise auf die Begehung einer anderen strafbaren Handlung als derjenigen, die Anlass zur Überwachung gegeben hat, so ist mit diesem Teil der Ergebnisse ein gesonderter Akt anzulegen, soweit die Verwendung als Beweismittel zulässig ist (Abs. 1, § 144, § 157 Abs. 2).

(3) In anderen gerichtlichen und in verwaltungsbehördlichen Verfahren dürfen Ergebnisse nur insoweit als Beweismittel verwendet werden, als ihre Verwendung in einem Strafverfahren zulässig war oder wäre."

"8. Abschnitt
Besondere Durchführungsbestimmungen, Rechtsschutz und Schadenersatz

Besondere Durchführungsbestimmungen

§ 145. (1) Sämtliche Ergebnisse einer der im 4. bis 6. Abschnitt geregelten Ermittlungsmaßnahmen sind von der Staatsanwaltschaft zu verwahren und dem Gericht beim Einbringen der Anklage zu übermitteln. Das Gericht hat diese Ergebnisse nach rechtskräftigem Abschluss des Verfahrens zu löschen, soweit sie nicht in einem anderen, bereits anhängigen Strafverfahren als Beweismittel Verwendung finden. Gleiches gilt für die Staatsanwaltschaft im Fall der Einstellung des Verfahrens.

(2) – (3) […]"

2.1. Nach den Erläuterungen zur Regierungsvorlage des nachmaligen Strafprozessreformgesetzes (25 BlgNR 22. GP, 192) ist § 140 Abs. 3 StPO in der hier maßgeblichen, am 1. Jänner 2008 in Kraft getretenen Fassung mit der bis dahin 11

in Geltung gestandenen Vorschrift des § 149h Abs. 3 StPO, die mit Bundesgesetz BGBl. I 105/1997 in die StPO eingefügt wurde, nahezu wortident. Diese Bestimmung hatte folgenden Wortlaut:

"§ 149h. (1) Ergeben sich bei Prüfung der Aufnahme Hinweise auf eine andere strafbare Handlung als diejenige, die Anlaß zur Überwachung gegeben hat, so sind von diesem Teil der Aufnahme Bilder und schriftliche Aufzeichnungen gesondert herzustellen, soweit die Verwendung als Beweismittel zulässig ist (Abs. 2, §§ 151 Abs. 2, 152 Abs. 3, § 31 Abs. 2 des Mediengesetzes).

(2) Als Beweismittel dürfen Überwachungsergebnisse, insbesondere die Aufnahmen und von diesen hergestellte Bilder und schriftliche Aufzeichnungen, bei sonstiger Nichtigkeit nur verwendet werden,

1. wenn die Voraussetzungen für eine Überwachung nach § 149d vorlagen,
2. wenn die Überwachung rechtmäßig angeordnet wurde (§ 149e) und
3. in den Fällen des § 149d Abs. 1 Z 2 und 3 nur zum Nachweis einer strafbaren Handlung, die mit einer Freiheitsstrafe bedroht ist, deren Obergrenze nicht weniger als fünf Jahre beträgt,
4. im Fall des § 149d Abs. 2 Z 2 nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, deretwegen die Überwachung angeordnet wurde oder hätte angeordnet werden können.

(3) In anderen gerichtlichen und in verwaltungsbehördlichen Verfahren dürfen Überwachungsergebnisse nur insoweit als Beweismittel verwendet werden, als ihre Verwendung in einem Strafverfahren zulässig war oder wäre."

Zu dieser Bestimmung wird im Bericht des Justizausschusses ausgeführt (812 BlgNR 20. GP, 9 f.): 12

"[...] Neu aufgenommen wurde in § 149h ein Verbot der Beweisverwertung von Überwachungsergebnissen in anderen (nicht strafrechtlichen) Gerichtsverfahren und in verwaltungsbehördlichen Verfahren, wenn die Verwertung dieser Ergebnisse im Strafverfahren unzulässig war oder – nach Einstellung eines Verfahrens oder Abbrechung gemäß § 412 StPO – in der Hauptverhandlung unzulässig gewesen wäre. In diesen Verfahren ist daher die Frage der zulässigen Verwendung von Überwachungsergebnissen im Strafverfahren als Vorfrage zu lösen. Die Erweiterung des strafrechtlichen Beweisverwertungsverbotes auf sämtliche Gerichts- und Verwaltungsverfahren kann aus Sicht des Justizausschusses damit begründet werden, daß nur dadurch das Wesen und der rechtsstaatliche Wert einer Verfahrensordnung zum Ausdruck gebracht werden kann, die massive Eingriffe in die Privatsphäre nur unter dem Gesichtspunkt und im Ausmaß eines angestrebten Nachweises organisierter Kriminalität und schwerster Straftaten in Kauf nehmen will. Das Gesetz dient dazu, diese Wertung durchzusetzen. Hinzukommt, daß eine dritte, private Partei kein subjektives Recht hat, Beweise, die in einem Strafverfahren von Amts wegen aufgenommen worden sind, in einem Zivilprozeß zu gebrauchen. Dies gilt in besonderem Maß für eine unzulässige Überwachung, die – wie jede heimliche Tonbandaufnahme einer nichtöffentli-

chen Äußerung – ein Eingriff in das Recht am gesprochenen Wort ist, der dann besonders schwer wiegt, wenn er 'illegal' durch staatliche Organe erfolgt. [...]"

2.2. Die §§ 134, 135, 137, 140 und 145 StPO wurden zuletzt durch Bundesgesetz BGBl. I 33/2011 im Hinblick auf die Umsetzung der Vorgaben der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung novelliert, wobei § 140 Abs. 3 nicht geändert wurde; diese Novellierungen traten mit 1. April 2012 – also nach Erlassung des Bescheides im Anlassverfahren – in Kraft. 13

3. § 105 Beamten-Dienstrechtsgesetz 1979 (BDG), BGBl. 333 idF BGBl. I 96/2007, lautet samt Überschrift: 14

"3. Unterabschnitt
Disziplinarverfahren

Anwendung des AVG und des Zustellgesetzes

§ 105. Soweit in diesem Abschnitt nicht anderes bestimmt ist, sind auf das Disziplinarverfahren
1. das AVG mit Ausnahme der §§ 2 bis 4, 12, 42 Abs. 1 und 2, 51, 51a, 57, 62 Abs. 3, 63 Abs. 1, 64 Abs. 2, 64a, 67a bis 67h, 68 Abs. 2 und 3 und 75 bis 80 sowie
2. das Zustellgesetz, BGBl. Nr. 200/1982,
anzuwenden."

4. § 46 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 (AVG), BGBl. 51, hat folgenden Wortlaut: 15

"§ 46. Als Beweismittel kommt alles in Betracht, was zur Feststellung des maßgebenden Sachverhaltes geeignet und nach Lage des einzelnen Falles zweckdienlich ist."

## III. Erwägungen

### 1. Zur Zulässigkeit des Verfahrens

Im Verfahren hat sich nichts ergeben, was an der Präjudizialität der in Prüfung gezogenen Bestimmung zweifeln ließe. Auch die Bundesregierung ist der im Prüfungsbeschluss hiezu vorläufig vertretenen Auffassung nicht entgegengetre- 16

ten. Da auch sonst keine Prozesshindernisse hervorgekommen sind, erweist sich das Gesetzesprüfungsverfahren als zulässig.

**2. In der Sache**

Die im Prüfungsbeschluss dargelegten Bedenken, dass § 140 Abs. 3 StPO dem Grundrecht auf Datenschutz widerspricht, konnten im Gesetzesprüfungsverfahren auch nach Durchführung einer mündlichen Verhandlung nicht zerstreut werden: 17

2.1. Dem – verfassungsgesetzlich gewährleisteten – Recht auf Datenschutz (§ 1 Abs. 1 DSG 2000) zufolge hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf die Achtung seines Privat- und Familienlebens, hat. Ein schutzwürdiges Interesse ist von vornherein bei allgemeiner Verfügbarkeit der Daten oder deren mangelnder Rückführbarkeit auf den Betroffenen ausgeschlossen. 18

2.2. Beschränkungen dieses Grundrechts sind dem Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 zufolge (abgesehen vom lebenswichtigen Interesse der Betroffenen an der Verwendung personenbezogener Daten oder ihrer Zustimmung dazu) nur zur Wahrung überwiegender berechtigter Interessen eines anderen, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen zulässig, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind. 19

2.3. Gemäß Art. 8 Abs. 2 EMRK sind Eingriffe in das in diesem Artikel verbürgte Grundrecht nur statthaft, insoweit sie 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 notwendig ist. Auch im Fall zulässiger Beschränkungen darf gemäß dem letzten Satz des § 1 Abs. 2 DSG 2000 der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden. 20

2.4. Nach der Rechtsprechung des Verfassungsgerichtshofes ist die Ermittlung und Verwendung personenbezogener Daten durch Eingriffe einer staatlichen 21

Behörde wegen des Gesetzesvorbehalts des § 1 Abs. 2 DSG 2000 nur auf Grund von Gesetzen zulässig, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind und ausreichend präzise, also für jedermann vorhersehbar regeln, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig ist (VfSlg. 16.369/2001, 18.146/2007, 18.963/2009, 18.975/2009, 19.657/2012; VfGH 12.3.2013, G 76/12).

2.5. § 1 Abs. 2 DSG 2000 beschränkt also im Interesse des grundrechtlichen Schutzes personenbezogener Daten den Gesetzgeber, wann und in welcher Weise er staatliche Behörden zur (Ermittlung und) Verwendung solcher Daten ermächtigen darf (vgl. VfSlg. 19.673/2012). Damit legt das DSG 2000 der Verwendung von Daten eine strenge Zweckbindung zugrunde, der zufolge erhobene Daten ausschließlich für die im jeweiligen Materiengesetz definierten Zwecke benutzt werden dürfen (vgl. VfSlg. 18.146/2007, 19.659/2012). 22

2.6. Die Bundesregierung verteidigt den in Prüfung gezogenen § 140 Abs. 3 StPO auf das Wesentliche zusammengefasst mit dem Argument, dass diese Vorschrift ausschließlich als Zulässigkeitsschranke (im Sinne eines Beweisverwertungsverbotes hinsichtlich unrechtmäßig ermittelter Daten) für die Datenweiterverwendung bzw. -verwertung in anderen Verfahren zu verstehen sei und keinen darüber hinausgehenden Regelungsinhalt – insbesondere nicht den vom Verfassungsgerichtshof vorläufig angenommenen zusätzlichen Gehalt einer Ermächtigungsnorm zur Daten(weiter)verwendung durch andere Behörden – besitze; dafür spreche auch die in § 76 Abs. 4 StPO für eine (bloße) Datenübermittlung zur "außerprozessualen" Verwendung ausdrücklich normierte Voraussetzung einer materienspezifischen Ermächtigung. § 140 Abs. 3 StPO sei als konkrete Ausgestaltung des allgemeinen datenschutzrechtlichen Grundsatzes der Verhältnismäßigkeit und (nur) insoweit – bezogen auf den Regelungsgegenstand der Legalität der Datenquelle – als von den Vorschriften des DSG 2000 abweichende Bestimmung iSd § 74 Abs. 1 StPO anzusehen und hindere die kumulative Anwendung anderer (datenschutzrechtlicher) Beschränkungen ebenso wenig wie die Vornahme einer Interessenabwägung im Einzelfall. 23

Für sämtliche der von § 140 Abs. 3 StPO erfassten Datenkategorien sei zusätzlich die Schranke des – weit auszulegenden – § 75 Abs. 5 StPO heranzuziehen; diese 24

(später geschaffene) Bestimmung erfasse nicht nur die "Überwachung von Nachrichten" im engeren Sinn, sondern auch "die Auskunft über Daten einer Nachrichtenermittlung", woraus eine "begriffliche Gleichsetzung" der in § 75 Abs. 5 StPO (als *lex specialis*) genannten Ermittlungsmaßnahmen mit jenen des § 140 Abs. 3 leg.cit. folge. Damit erfordere auch die in Prüfung gezogene Vorschrift in Bezug auf die Zulässigkeit der Verwendung von in einem Strafverfahren rite ermittelten Daten einen inhaltlichen Zusammenhang zwischen diesem Strafverfahren und dem anderen Gerichts- oder Verwaltungsverfahren. Das Fehlen einer Bezugnahme auf die Beschlagnahme von Briefen in § 75 Abs. 5 StPO stelle eine durch Analogie schließbare planwidrige Lücke dar.

2.7. Die Bestimmung des § 140 Abs. 3 StPO ist – unabhängig von der Frage, ob die Regelung (nur) als Beweisverwertungsverbot oder auch als rechtliche Grundlage für die Übermittlung von Daten zu verstehen ist, – jedenfalls unverhältnismäßig und verstößt deshalb gegen das Grundrecht auf Datenschutz: 25

2.7.1. Eine Regelung betreffend die Zulässigkeit der Übermittlung von Daten an Behörden findet sich in der im 1. Teil ("Allgemeines und Grundsätze des Verfahrens"), 5. Hauptstück ("Gemeinsame Bestimmungen"), 2. Abschnitt ("Amts- und Rechtshilfe") enthaltenen – von der Bundesregierung angesprochenen – Bestimmung des § 76 Abs. 4 StPO. Für eine Übermittlung an andere Behörden als im Dienste der Strafrechtspflege agierende Finanzstrafbehörden, Sicherheitsbehörden, Staatsanwaltschaften und Gerichte muss jedoch schon nach der Diktion dieser Vorschrift (§ 76 Abs. 4 zweiter Satz) eine ausdrückliche gesetzliche Ermächtigung bestehen. Eine solche Ermächtigung besteht nicht. 26

2.7.2. Nun ist es dem Gesetzgeber durch das Grundrecht auf Datenschutz nicht von vornherein untersagt, die Zulässigkeit einer Datenverwendung als Beweismittel in anderen Verfahren als in jenem, in dem diese Daten rechtmäßig ermittelt wurden, vorzusehen und an bestimmte Bedingungen zu knüpfen, jedoch ist ein solcher Eingriff gemäß § 1 DSG 2000 iVm Art. 8 Abs. 2 EMRK nur dann zulässig, wenn dieser auf einer zur Datenerhebung ermächtigenden Norm beruht, einem der enumerativ aufgezählten Eingriffsziele dient und auf das Erforderliche beschränkt, geeignet und verhältnismäßig ist (vgl. VfSlg. 18.975/2009 mwN). Der Gesetzgeber darf daher die Verwendung von Ergebnissen über personenbezogene Daten, die in einem Strafverfahren rite erlangt wurden, in sonstigen (gerichtlichen oder verwaltungsbehördlichen) Verfahren nur insoweit vorsehen, als der Zweck der Datenverwendung in diesen Verfahren ein öffentliches Interesse oder 27

das Interesse eines anderen verfolgt, welches das Interesse des Betroffenen an der Geheimhaltung (bzw. Löschung) der Daten übersteigt und das gelindeste Mittel zur Erreichung des Verfahrenszieles darstellt.

2.7.3.1. Nach dem Wortlaut des § 140 Abs. 3 StPO "dürfen Ergebnisse nur insoweit als Beweismittel verwendet werden, als ihre Verwendung in einem Strafverfahren zulässig war oder wäre"; dies bedeutet, dass die Verwendung von Ergebnissen einer Datenermittlung aus einem Strafverfahren als Beweismittel in sonstigen gerichtlichen und verwaltungsbehördlichen Verfahren zwar nur unter dieser (einzigen) einschränkenden Prämisse, im Übrigen aber unbeschränkt erlaubt wird. Denn es wird mit der in Prüfung stehenden Regelung nicht nur das legitime Ziel der Verhinderung von Sekundärverwendungen illegal zustande gekommener Ermittlungsergebnisse erreicht, sondern gleichzeitig bewirkt, dass rite ermittelte Ergebnisse iSd § 134 Z 5 StPO, die in anderen gerichtlichen oder verwaltungsbehördlichen Verfahren – auf welche Weise auch immer – bekannt werden, in diesen anderen Verfahren schlechthin als Beweismittel Verwendung finden können. Dies ohne weitere Kautelen, wie etwa jene eines inhaltlichen Zusammenhanges des anderen Verfahrens mit dem Strafverfahren, in dem die Ergebnisse produziert wurden sowie jene der Gewichtung der Bedeutung der Ermittlungsergebnisse für die mit dem anderen Verfahren verfolgten öffentlichen oder berechtigten Interessen einer am anderen Verfahren beteiligten Person einerseits und des Grundrechtseingriffs für den Betroffenen durch die Weiterverwendung seiner aus einem Strafverfahren stammenden personenbezogenen Daten andererseits. 28

2.7.3.2. Die Norm hat somit den Inhalt, dass jedwede personenbezogenen Daten, sofern sie im Strafverfahren zulässigerweise ermittelt wurden, in jedwedem anderen gerichtlichen oder verwaltungsbehördlichen Verfahren verwendet werden dürfen. Auch in der Verhandlung ist nichts hervorgekommen, was die diesbezüglichen Bedenken entkräften könnte. 29

2.7.3.3. Die Auffassung der Bundesregierung, dass für sämtliche der von § 140 Abs. 3 StPO erfassten Datenkategorien zusätzlich die Schranke des § 75 Abs. 5 StPO heranzuziehen sei, vermag der Verfassungsgerichtshof nicht zu teilen: 30

2.7.3.4. Die – im 1. Teil ("Allgemeines und Grundsätze des Verfahrens"), 1. Abschnitt ("Einsatz der Informationstechnik"), 5. Hauptstück ("Gemeinsame Bestimmungen") unter der Überschrift "Berichtigen, Löschen und Sperren von Daten" enthaltene – Regelung des § 75 Abs. 5 StPO bezieht sich nach ihrem klaren Wortlaut auf Daten, die durch eine Überwachung von Nachrichten, eine optische oder akustische Überwachung oder einen automationsunterstützten Datenabgleich ermittelt worden sind. Die Definitionen dieser Begriffe finden sich in § 134 Z 3 und 4 StPO sowie in § 141 StPO. Entgegen der Auffassung der Bundesregierung sind daher die im Anlassfall relevanten Ergebnisse einer Nachrichtenübermittlung (§ 134 Z 2 StPO) – ebenso wie der Inhalt beschlagnahmter Briefe (§ 134 Z 1 StPO) – nicht Gegenstand der Regelung des § 75 Abs. 5 StPO. 31

2.7.3.5. Die Bundesregierung unterlegt dieser Bestimmung einen weiten Anwendungsbereich und vermeint, dass im Auslegungswege sämtliche von § 134 Z 5 leg.cit. erfassten Ergebnisse unter § 75 Abs. 5 leg.cit. zu subsumieren seien und daher das nach dieser Vorschrift für die Verwendung von strafrechtlichen Daten in anderen gerichtlichen oder verwaltungsbehördlichen Verfahren vorausgesetzte Erfordernis des Bestehens eines Zusammenhanges mit dem Strafverfahren, in dem die Ermittlung rechtmäßig erfolgte, auch auf § 140 Abs. 3 StPO übertragbar sei. 32

2.7.3.6. Abgesehen davon, dass der eindeutige Wortlaut des § 75 Abs. 5 StPO (wie dargelegt) u.a. gerade die im Anlassfall maßgeblichen Daten einer Nachrichtenübermittlung nicht umfasst und § 75 Abs. 5 StPO auch nach Auffassung der Bundesregierung gegenüber § 140 Abs. 3 StPO als *lex specialis* anzusehen ist, spricht die divergierende systematische Einordnung in verschiedenen – getrennte Bereiche regelnden – Teilen der StPO gegen eine vom Gesetzgeber intendierte Gleichsetzung der beiden Bestimmungen. 33

2.7.3.7. Im Übrigen wäre im vorliegenden – eine Disziplinarrechtssache betreffenden – Anlassverfahren für den Standpunkt der Bundesregierung, die in der Vorschrift des § 46 AVG iVm § 105 BDG eine mögliche gesetzliche Grundlage für die Erlaubnis zur Weiterverwendung und Verwertung der strafrechtlichen Ermittlungsresultate erblickt, im Ergebnis gleichfalls nichts zu gewinnen: Abgesehen davon, dass sich die belangte Behörde im Anlassfall ausdrücklich nur auf den von ihr als Ermächtigungsnorm beurteilten § 140 Abs. 3 StPO stützte, hat § 46 AVG (auf den § 105 BDG verweist) in Bezug auf datenschutzrechtliche Anforderungen keinen engeren Inhalt, bringt diese Bestimmung doch lediglich den allgemeinen 34

Grundsatz der Unbeschränktheit von Beweismitteln im Verwaltungsverfahren zum Ausdruck.

## IV. Ergebnis

1. § 140 Abs. 3 StPO idF BGBl. I 19/2004 ist daher wegen Verstoßes gegen das Grundrecht auf Datenschutz aufzuheben. 35

2. Die Bestimmung einer Frist für das Außerkrafttreten der aufgehobenen Gesetzesstelle gründet sich auf Art. 140 Abs. 5 dritter und vierter Satz B-VG. 36

3. Der Ausspruch, dass frühere gesetzliche Bestimmungen nicht wieder in Kraft treten, beruht auf Art. 140 Abs. 6 erster Satz B-VG. 37

4. Die Verpflichtung des Bundeskanzlers zur unverzüglichen Kundmachung der Aufhebung und der damit im Zusammenhang stehenden sonstigen Aussprüche erfließt aus Art. 140 Abs. 5 erster Satz B-VG und § 64 Abs. 2 VfGG iVm § 3 Z 3 BGBlG. 38

Wien, am 01.10.2013
Der Präsident:
Dr. HOLZINGER

Schriftführer:
Mag. Dr. GRATZL und
Dr. TROFAIER-LESKOVAR