REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.211/0002-DSR/2015
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Inneres

Per E-Mail:
bmi-III-1@bmi.gv.at

Betrifft: **Entwurf eines Bundesgesetzes, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG) erlassen und das Sicherheitspolizeigesetz geändert wird**
Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **224. Sitzung am 24. April 2015 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Die Diversität der Bedrohungen und eine zunehmend von globalen Rahmenbedingungen abhängige Gefahrenlage erfordern einen **modernen und vernetzten polizeilichen Staatsschutz**. Wollen die Sicherheitsbehörden nicht nur auf Gefahren reagieren, sondern Bedrohungen aktiv schon im Vorfeld entgegentreten, müssen ihnen – aus Sicht des Bundesministeriums für Inneres – dazu auch entsprechende Mittel und Möglichkeiten an die Hand gegeben werden.

Dieses Anliegen ist auch im Arbeitsprogramm der österreichischen Bundesregierung 2013-2018 enthalten, in dem die **Schaffung besonderer bundesgesetzlicher Regelungen für den Staatsschutz als Maßnahme ausdrücklich vorgesehen ist** (06 Sicherheit und Rechtsstaat, Inneres, S 81). Mit dieser Maßnahme soll eine

effektive und effiziente Abwehr der Spionage und der Folgen von Extremismus und Terrorismus durch den Ausbau der präventiven und repressiven Mechanismen ermöglicht werden.

Mit dem vorliegenden Entwurf soll das Regierungsprogramm umgesetzt und eine **bundesgesetzliche Regelung über die Organisation, Aufgaben und Befugnisse des Staatsschutzes** geschaffen werden: Während im ersten Hauptstück Regelungen zur Organisation der polizeilichen Staatsschutzbehörden verankert werden sollen, werden im zweiten Hauptstück jene **Aufgaben** taxativ genannt, die ausschließlich diesen Behörden zukommen: Dazu zählen die erweiterte Gefahrenerforschung und der Schutz vor verfassungsgefährdenden Angriffen, die staatsschutzrelevante Beratung sowie die umfassende Beurteilung und Analyse von staatsschutzrelevanten Bedrohungen zur Information verfassungsmäßiger Einrichtungen. Die im dritten Hauptstück verankerten **Datenverarbeitungs-ermächtigungen** sollen den Bedürfnissen des polizeilichen Staatsschutzes soweit gerecht werden, als es in einem ausgewogenen Verhältnis mit dem Grundrecht auf Schutz des Privatlebens und Achtung der Privatsphäre (Art. 8 EMRK) vereinbar ist. Umfassende Regelungen zum **Rechtsschutz** einschließlich **Informationspflichten** für Betroffene und Berichtspflichten finden sich schließlich im vierten Hauptstück des Entwurfs.

Die in Artikel 2 des Entwurfs vorgesehenen **Änderungen des Sicherheitspolizei-gesetzes (SPG)** berücksichtigen einerseits die erforderlichen Anpassungen an das Polizeiliche Staatsschutzgesetz (PStSG) und anderseits folgende wesentliche Punkte: Der Einsatz von **Bild- und Tonaufzeichnungsgeräten** zur Dokumentation von Amtshandlungen, bei denen die Organe des öffentlichen Sicherheitsdienstes Befehls- und Zwangsgewalt ausüben, soll gesetzlich verankert werden. Zur Verfolgung strafbarer Handlungen und zur Kontrolle der Rechtmäßigkeit einer Amtshandlung kommt einer ausreichenden und an den technischen Möglichkeiten ausgerichteten **Videodokumentation** als Beweismittel wesentliche Bedeutung zu. Daher soll auf diese Art von Dokumentation, der die erforderliche Objektivität eines Sachbeweises inne wohnt, in Zukunft nicht verzichtet werden, um im Anlassfall, also wenn Zweifel an der Rechtmäßigkeit der Amtshandlung laut werden oder es gilt, strafbare Handlungen zu verfolgen, darauf zurückgreifen zu können.

Zudem soll die Möglichkeit geschaffen werden, bei der Sicherheitsbehörde vorhandenes **Videomaterial** (§ 54 Abs. 5) auch zur Verfolgung von Verwaltungsübertretungen zu verwenden, um insbesondere **Verwaltungsübertretungen** nach dem PyrotechnikG 2010 bei Sportgroßveranstaltungen, die ein großes Gefahrenpotential darstellen, wie der Entschließung betreffend Reglementierung pyrotechnischer „Signalstifte“, 61/E, 25. GP vom 10. Dezember 2014 und den diesbezüglichen Ausführungen im Bericht des Ausschusses für innere Angelegenheiten, AB 411 BlgNR 25. GP, zu entnehmen ist, im Nachhinein aufklären zu können.

2) Datenschutzrechtliche Anmerkungen

I. Artikel 1 – Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG)

Der Datenschutzrat begrüßt das grundsätzliche Vorhaben, moderne und zielführende Regelungen für den Staatsschutz auf bundesgesetzlicher Ebene zu schaffen, um damit den Schutz der im Staatsgebiet lebenden Menschen sowie der verfassungsmäßigen Grundordnung zu gewährleisten. Dafür werden Organisation, Aufgaben und Befugnisse der polizeilichen Staatsschutzbehörden neu geregelt, wobei neue Befugnisse – über die bestehenden Regelungen des SPG hinaus – geschaffen werden (zB § 12 Abs. 1 Z 5). Die erweiterte Gefahrenforschung und der Schutz vor verfassungsgefährdenden Angriffen kommen zukünftig ausschließlich dem Verfassungsschutz zu. Gesetzliche Beschränkungen des Schutzes personenbezogener Daten (Art. 8 GRC) haben sich dabei an der Rechtsprechung des Europäischen Gerichtshofes (EuGH) zu orientieren. Diese Standards dürfen keinesfalls unterschritten werden.

Der Datenschutzrat erkennt ein Spannungsverhältnis zwischen dem polizeilichen Staatsschutz und dem Datenschutz und weist daraufhin, dass der EuGH und der VfGH in ihrer Rechtsprechung aufgezeigt haben, wie die Grenzen der Verhältnismäßigkeit zu verstehen sind.

Im Detail wirft der vorliegende Entwurf **aus datenschutzrechtlicher Sicht verschiedene grundlegende Problemstellungen** auf:

Vorweg wird darauf hingewiesen, dass der in § 4 Z 1 des Entwurfes verwendete Begriff „**Computersystem**“ **Unklarheiten** aufwirft. So müsste aus Sicht des Datenschutzrates berücksichtigt werden, dass durch **neue Technologien und Geschäftsmodelle (Stichworte: „Big Data“ sowie Online Speicherdienste/Cloud)** Daten nicht mehr nur lokal auf dem eigenen Computer gespeichert werden. **Es sollte daher ausdrücklich geprüft werden, ob von der im Entwurf verwendeten Definition „Computersystem“, die nach § 74 Abs. 1 Z 8 StGB „sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen“ umfasst, auch diese neuen technischen Entwicklungen abgedeckt sind.**

Der Datenschutzrat regt an, dass in den Erläuterungen ausdrücklich klargestellt werden sollte, welche neuen Technologien unter den Begriff „Computersystem“ fallen.

Die Festlegung der **Aufgaben** auf dem Gebiet des polizeilichen Staatsschutzes ist im **2. Hauptstück** des Entwurfes zum einen – im Hinblick auf die davon umfassten Straftatbestände – **auffallend weit gefasst**, zum anderen stellt er weitgehend auf **die Prognose des Eintritts von Gefahrensituationen und Angriffen** ab. Es sollte **ausführlicher** geregelt werden, **auf welchen zukünftigen Zeitrahmen** hin diese Prognose getroffen werden muss. **Jedenfalls muss vermieden werden, dass aufgrund eines unbegründeten oder bloß vagen Verdachts gegen eine Person bereits eine umfassende und über Jahre hinweg erfolgende Verwendung personenbezogener Daten erfolgt.**

Zu den §§ 4 Z 1 und 6 Abs. 2 Z 5 stellt sich die Frage, warum die Straf-bestimmungen des Zugangskontrollgesetzes – als Teil des Computersrafrechts – nicht berücksichtigt wurden.

Die **neue Aufgabe** des Bundesamtes und der Landesämter nach § 7, zur Vorbeugung verfassungsgefährdender Angriffe, insbesondere auf dem Gebiet der Cybersicherheit, **die Bereitschaft und Fähigkeit des Einzelnen zu fördern**, sich

über eine Bedrohung seiner Rechtsgüter Kenntnis zu verschaffen und Angriffen entsprechend vorzubeugen, scheint **nicht in unmittelbarem Konnex** mit den anderen Aufgabengebieten des 2. Hauptstücks zu stehen. **Derartige Öffentlichkeitsarbeit steht im Bereich der Datensicherheit mit den nicht-öffentlichen Kernaufgaben in einem Spannungsverhältnis, daher sollte diese Beratungsfunktion besser durch eine unabhängige Einrichtung vorgesehen werden.**
In § 8 sollte näher dargelegt werden, ob bei der **Information verfassungsmäßiger Einrichtungen** auch – allenfalls **sensible** – **personenbezogene Daten** verwendet werden. Im Übrigen ist nicht nachvollziehbar, weshalb solche Informationen zur **Wahrung des Ansehens** von Personen und Institutionen vorgenommen werden. **Um Interpretationsschwierigkeiten zu vermeiden, sollte § 8 präzisiert werden.**

Zu § 10 im **3. Hauptstück** des Entwurfes („**Verwenden personenbezogener Daten auf dem Gebiet des polizeilichen Staatsschutzes**“) merkt der Datenschutzrat vorweg an, dass die **Auskunft** über personenbezogene Daten nach § 10 Abs. 3 derart ausgestaltet werden muss, dass sie den **Vorgaben § 1 Abs. 2 DSG 2000** entspricht. So muss daher im Sinne des **Verhältnismäßigkeitsgrundsatzes** für die Zulässigkeit der Verweigerung der Auskunft nach dem letzten Satz des § 10 Abs. 3 auch auf die **Interessen des Betroffenen** abgestellt werden, über den Auskunft erteilt werden soll.

Weiters ist in § 10 Abs. 5 fraglich, was unter „**allen anderen verfügbaren Quellen**“ zu verstehen ist. Um dem Verhältnismäßigkeitsgrundsatz zu entsprechen, müssten diese **Quellen (zB Datenbanken) näher dargestellt** und – dem angestrebten Ziel entsprechend – **begrenzt** werden.

Zudem wird zum **3. Hauptstück** des Entwurfes allgemein angemerkt, dass – nachdem schon die Definition der Aufgaben auffallend weit gefasst ist – **auch die Datenverwendung** zur Erfüllung dieser Aufgaben **nicht ausreichend klar abgegrenzt wird**. So ist etwa fraglich, von welchen Personen tatsächlich Daten für die Erfüllung dieser Aufgaben benötigt werden. Diese Problematik wird sogar noch verstärkt, indem in § 11 die Verwendung von Daten **nicht nur** zum Zweck der **Bewertung der Wahrscheinlichkeit** einer Gefährdung, sondern auch **zum**

Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse vorgesehen ist. So werden auch Daten von **Kontakt- oder Begleitpersonen**, die nicht nur zufällig mit verdächtigen Personen in Verbindung stehen, verarbeitet, wenn ausreichende Gründe für die Annahme bestehen, dass über sie Informationen zu diesen Personen beschafft werden können. Dies stellt eine verdachtsunabhängige (d.h. anlasslose) Datenverarbeitung dar.
Unter diesem Blickwinkel könnten wohl auch **Arbeitskollegen jener Person**, die sich in ein Drittland (zB Kriegsgebiet) begibt, von dieser Datenanwendung erfasst werden. Aus einer derartig **weiten Formulierung** ist daher **kaum vorhersehbar**, wer in die Datenanwendung des Bundesamts und der Landesämter aufgenommen wird. **Der Kreis solcher „unbeteiligter" Personen muss daher klar definiert werden. Es dürfen nur unbedingt erforderliche Verarbeitungen von Daten dieser Personen vorgenommen werden, dabei ist in jedem einzelnen Fall der Verhältnismäßigkeitsgrundsatz zu beachten.**

Aus datenschutzrechtlicher Sicht problematisch erscheint auch die Formulierung des § 11 Abs. 1, wonach „**tat- und fallbezogene Informationen und Verwaltungsdaten**" verarbeiten werden dürfen, auch wenn es sich um **besonders schutzwürdige Daten iSd § 4 Z 2 DSG 2000 handelt.** § 1 Abs. 2 DSG 2000 verlangt bei der Verwendung von „besonders schutzwürdigen" Daten (=**sensiblen Daten**, wozu insbesondere auch **Gesundheitsdaten** zählen), dass diese nur zur Wahrung **wichtiger öffentlicher Interessen** vorgesehen werden darf und gleichzeitig **angemessene Garantien** für den **Schutz der Geheimhaltungsinteressen der Betroffenen** festlegt werden müssen. Es ist im vorliegenden Entwurf jedoch überhaupt nicht ersichtlich, dass derartige **angemessene Garantien** für die Verarbeitung sensibler Daten getroffen werden, obwohl diese Daten auch noch dazu im Rahmen eines **Informationsverbundsystems** (§ 11 Abs. 2) verarbeitet werden. Hinsichtlich dieses Informationsverbundsystems sollte zudem klarer geregelt werden, wer **Auftraggeber** – und allenfalls auch **Betreiber** – ist.

Allgemein – jedoch insbesondere auch im Hinblick auf die Verarbeitung der Daten im Rahmen des **Informationsverbundsystems** gemäß § 11 Abs. 2 – ist darauf hinzuweisen, dass aufgrund des in § 1 Abs. 2 DSG 2000 (iVm § 7 Abs. 3 DSG 2000) verankerten **Verhältnismäßigkeitsgrundsatzes** personenbezogene Daten sofort zu

löschen sind, **wenn sie für den Zweck, für den sie erhoben worden sind, nicht mehr benötigt werden.** Insofern erscheint die Festlegung in § 11 Abs. 2, dass Daten gemäß § 11 Abs. 1 Z 1, 2 und 4 (und sohin gerade auch **sensible Daten**) längstens nach fünf Jahren zu löschen sind, zu undifferenziert. Selbst die Löschung der Daten gemäß § 11 Abs. 1 Z 3 (Daten zu Kontakt- oder Begleitpersonen) **„bei Wegfall der ausreichenden Gründe für die Annahme“** erscheint in der Praxis schwer auslegbar, da offen bleibt, **wann „ausreichende“ Gründe vorliegen**. Aus Sicht des Datenschutzrates muss in jedem Fall gewährleistet werden, dass die vorgesehene Datenbank **nur die für die Erfüllung der Aufgaben unbedingt notwendigen Daten enthält und diese nicht länger als erforderlich gespeichert werden sowie der Kreis der erfassten Personen und Datenarten – insbesondere im Hinblick auf sensible Daten – eng umgrenzt wird. Diese gilt besonders auch für die Übermittlung der Daten aus dem Informationsverbundsystem an andere Behörden und Gerichte.**

Hinsichtlich der **Protokollierung** von Daten nach § 11 Abs. 4 ist fraglich, von **wem** die **Überprüfung der Protokolldaten** vorgenommen wird und ob diese Überprüfung nur nach Stichproben erfolgt oder aber eine Überprüfung jeder Abfrage im Hinblick auf einen vorliegenden konkreten Geschäftsfall durchgeführt werden soll. Im Übrigen erscheint – angesichts der langen Speicherfristen – eine **Aufbewahrung der Protokollaufzeichnung von bloß drei Jahren zu kurz.** Es muss gewährleistet werden, dass Protokollaufzeichnung **grundsätzlich solange aufbewahrt werden müssen, wie auch die Daten zu dieser Person gespeichert werden bzw. bis die in der Datenbank erfasste Person (Betroffener) nach § 17 informiert werden kann.**

Die **besonderen Bestimmungen für die Ermittlung** nach § 12 umschreiben – ebenso wie bereits der Aufgabenbereich nach § 6 – nur vage, wann die einzelnen Ermittlungsmethoden zulässig sind. So erscheint fraglich, wann eine Erfüllung einer Aufgabe ohne Einsatz dieser Methoden „**aussichtslos**“ oder „**wesentlich erschwert**“ wäre. Zudem betreffen diese Ermittlungen zum Teil auch personenbezogene Daten von **Kontakt- und Begleitpersonen**. Insbesondere hinsichtlich dieser Personen ist dafür zu sorgen, dass erhobene Daten (zB Fotos

eines Treffens mit Arbeitskollegen), die **nicht für die Ermittlung benötigt werden, umgehend gelöscht werden.**

Weiters dürfen die Ermittlungsermächtigungen nach § 12 Abs. 1 – insbesondere im Hinblick auf die Erhebung von **Telekommunikationsdaten** sowie Einholung von Auskünften von **Beförderungsunternehmen** – nicht dazu führen, dass in jedem Fall derartige Daten routinemäßig abgefragt werden, zumal auch solche Personen betroffen sein können, bei denen sich **nachträglich herausstellt, dass der Verdacht unbegründet** war. **Bei diesen, weit in die Privatsphäre eingreifenden Maßnahmen muss aus Sicht des Datenschutzrates sichergestellt werden, dass die im konkreten Fall angewandte Ermittlungsmethode im Verhältnis zu der vermuteten Straftat steht, um dem Verhältnismäßigkeitsgrundsatz – und damit dem Gebot der Verwendung des gelindesten, zum Ziel führenden Mittels – gerecht zu werden.**

Darüber hinaus sollte in den Erläuterungen klargestellt werden, ob die in § 11 Abs. 2 definierten Übermittlungsbefugnisse auf die in der Datenanwendung selbst gespeicherten Daten beschränkt sind, oder auch die daraus gewonnenen Schlüsse und Analysen umfasst.

Hinsichtlich § 12 Abs. 1 Z 7 PStSG wurde als datenschutzrechtlich bedenklich empfunden, dass das BVT künftig bei Zugriffen auf Verkehrsdaten nicht mehr der richterlichen Kontrolle unterliegt, sondern ohne Genehmigung auf diese Daten zugreifen kann.

Im Zusammenhang mit der **Vertrauenspersonenevidenz** nach § 13 erscheint unklar, weshalb auch **sensible Daten über den Betroffenen** verarbeitet werden. Es sollte klargestellt werden, welche Daten davon umfasst sind und zu welchem **Zweck** diese benötigt werden.

Hinsichtlich der **Löschungsregelung** in § 14 Abs. 2 ist unklar, aufgrund welcher „**bestimmter**“ Tatsachen erwartet werden kann, dass die Person einen neuen Anlass für eine Aufgabe nach § 6 Abs. 1 Z 1 oder 2 geben wird. Es ist konkreter und verständlicher zu regeln, unter welchen **taxativ aufgezählten Voraussetzungen**

eine **Verlängerung der Aufbewahrungsdauer von Daten** vorgenommen werden kann.

Zum Rechtsschutz nach dem 4. Hauptstück des Entwurfes ist anzumerken, dass der Entwurf weitgehende Eingriffe in das Grundrecht auf Datenschutz vorsieht.

Als Gegengewicht zu diesen Eingriffsbefugnissen muss eine **effiziente Kontrolle der Eingriffe sichergestellt** und müssen **bei unzulässigen Datenverwendungen wirksame Sanktionen vorgesehen werden**. In diesem Zusammenhang erscheint fraglich, ob dafür eine bloße Kontrolle durch den **Rechtsschutzbeauftragten** ausreicht. Dies auch vor dem Hintergrund, dass die **Informationsmöglichkeit des Betroffenen** nach § 17 zum Teil (bei Vorliegen von Gründen nach § 26 Abs. 2 DSG 2000) durchbrochen ist und der Betroffene daher unter Umständen selbst nicht erfährt, dass von ihm unrechtmäßig Daten verwendet worden sind bzw. er – allenfalls sogar über mehrere Jahre hinweg – unrechtmäßig überwacht worden ist.
Besonders nachdenklich stimmt die Tatsache, dass nach § 16 Abs. 1 letzter Satz der Rechtsschutzbeauftragte von bestimmten Informationen generell ausgeschlossen ist. Dazu ist anzumerken, dass – im Gegensatz zum Rechtsschutzbeauftragten – im Bereich der **Gerichtsbarkeit** dem mit der Sache befassten **Richter** in der Regel **alle erforderlichen Informationen** zur Verfügung stehen. **Die Regelungen zum Rechtsschutz sollten daher unter diesen Gesichtspunkten grundlegend überarbeitet und ein mit dem gerichtlichen Rechtsschutz vergleichbares Niveau sichergestellt werden. Gleichzeitig sind aber auch entsprechende Ressourcen sicherzustellen. Der Datenschutzrat hält in diesem Zusammenhang fest, dass von den informierten Vertretern in der Sitzung des Datenschutzrates die Erhöhung der Ressourcen des Rechtsschutzbeauftragten zugesichert worden ist.**

Hinsichtlich der **Übergangsbestimmung** in § 22 des Entwurfes sollte klargestellt werden, dass nur solche bereits vorhandene personenbezogene Daten in der neuen Datenanwendung des § 11 verarbeitet werden dürfen, die **zuvor bereits konkret für diese Zwecke erhoben worden sind.**

II. Artikel 2 – Änderung des Sicherheitspolizeigesetzes

Der in § 13a Abs. 3 geregelte **offenen Einsatz von Bild- und Tonaufzeichnungsgeräten** zum Zweck der Dokumentation von Amtshandlungen, bei denen die Organe des öffentlichen Sicherheitsdienstes Befehls- und Zwangsgewalt ausüben, ist **im Gesetzeswortlaut** klarer zu regeln, **wann die Aufzeichnung gestartet wird.** Weiters sollte ausdrücklich ausgeschlossen werden, dass durch die verwendeten Geräte – wenn auch nur im Hintergrund – **eine ständige Aufzeichnung von Bild und Ton erfolgt. Weiters sollte näher dargestellt werden, ob auch Verwaltungsübertretungen** im Zuge des **offenen Einsatzes von Bild- und Tonaufzeichnungsgeräten** erfasst bzw. verfolgt werden. In diesem Fall wird auf die **nachfolgenden Ausführungen zu § 54 Abs. 5 verwiesen.**

Zudem wird darauf hingewiesen, dass der **bloße Verweis auf den § 14 DSG 2000 nicht ausreicht.** Nachdem wohl auch **sensible Daten** auf den Bildaufzeichnungen festgehalten werden könnten (zB erlittene Verletzungen im Zuge der Amtshandlung), erscheint eine **genauere Festlegung der gemäß § 14 DSG 2000 festzulegenden Datensicherheitsmaßnahmen erforderlich.**

Hinsichtlich des in § 53a Abs. 5a geregelten **Informationsverbundsystems** sollte klarer geregelt werden, wer **Auftraggeber** – und allenfalls auch **Betreiber** – dieses Informationsverbundsystems ist. Weiters sollte im Lichte des in § 1 Abs. 2 DSG 2000 verankerten **Verhältnismäßigkeitsgrundsatzes** festgelegt werden, **wie lange die Daten im Rahmen des Informationsverbundsystems verwendet werden dürfen.**

Nach § 54 Abs. 5 dürfen die mit **Bild- und Tonaufzeichnungsgeräten** ermittelten Daten auch zur **Abwehr gefährlicher Angriffe und Verfolgung strafbarer Handlungen**, die sich **im Zusammenhang mit oder während der Zusammenkunft** ereignen, verarbeitet werden. Nach den **Erläuterungen** soll es ermöglicht werden, dass diese Geräte etwa auch bei Aufsplitterungen kleinerer Gruppen im Zusammenhang mit solchen Zusammenkünften **zum Zweck der Vorbeugung** zum Einsatz gelangen können. Wie in § 54 Abs. 6 SPG sollen die Bild- und Tonaufzeichnungen, die unter den Voraussetzungen des § 54 Abs. 5 ermittelt wurden, nicht nur für die Zwecke der Verfolgung von gerichtlich strafbaren

Handlungen, sondern **auch zur Verfolgung von Verwaltungsübertretungen** verwendet werden dürfen.

Der Datenschutzrat hält dazu fest, dass bei der Verfolgung von Verwaltungsübertretungen mittels Bild- und Tonaufzeichnungen jedenfalls der Verhältnismäßigkeitsgrundsatz zu beachten ist und diese daher nicht bei „geringfügigen" Verwaltungsübertretungen zum Einsatz kommen dürfen.

Zusammenfassend merkt der Datenschutzrat an, dass der vorliegende Entwurf eines „Polizeilichen Staatsschutzgesetzes" einer Korrektur und weiteren Überarbeitung im Lichte der aufgeworfenen Problemstellungen aus datenschutzrechtlicher Sicht bedarf.

Der Datenschutzrat hält im Übrigen fest, dass die informierten Vertreter in der Sitzung des Datenschutzrates zugesichert haben, dass die derzeitige Praxis mit der Durchlaufstelle beibehalten wird. Der Datenschutzrat begrüßt dieses Vorhaben.

12. Mai 2015
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt