DIE ÖSTERREICHISCHEN RECHTSANWÄLTE

Bundesministerium für Inneres
Herrengasse 7
1010 Wien

per E-Mail: bmi-III-1@bmj.gv.at
begutachtungsverfahren@parlament.gv.at

**Zl. 13/1 17/99**

**BMI-LR1340/0019-III/1/2017**
**BG, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden**

**Referent: VP Dr. Bernhard Fink, Rechtsanwalt in Klagenfurt**

Sehr geehrte Damen und Herren!

Der Österreichische Rechtsanwaltskammertag (ÖRAK) dankt für die Übersendung des Entwurfes und erstattet dazu folgende

**S t e l l u n g n a h m e :**

## 1. Allgemeines:

### 1.1. Begutachtungsfrist

Mit dem hier vorliegenden Teil des sogenannten *Sicherheitspakets* werden im Wesentlichen die Bestimmungen von SPG, TKG, StVO und BStMG dahingehend geändert bzw. ergänzt, dass den Sicherheitsbehörden weitreichende – insbesondere die Grund- und Freiheitsrechte der Bürger einschneidende – Befugnisse eingeräumt bzw. massiv ergänzt werden.

Der ÖRAK, zu dessen Aufgaben es auch gehört, Gesetzesbegutachtungen durchzuführen, um auch auf diese Weise die Interessen der rechtsuchenden Bevölkerung entsprechend zu wahren, begrüßt den angemessenen Begutachtungszeitraum von knapp sechs Wochen.

Der ÖRAK würde es in diesem Zusammenhang begrüßen, wenn bei anderen Gesetzesvorhaben mit ebenfalls wesentlichen Rechtsfolgen für die Rechtsunterworfenen ähnlich adäquate Zeiträume zur Verfügung stünden, um diese einer effizienten inhaltlichen, allenfalls auch interdisziplinären Begutachtung zu unterziehen.

### 1.2. Gesetzgebungsverfahren

Im Hinblick auf diese massiven Eingriffe in die Grundrechte der Bevölkerung ist es befremdlich, dass der gegenständliche Gesetzesvorschlag noch kurz vor der bevorstehenden Nationalratswahl am 15. Oktober 2017 durch den Nationalrat beschlossen werden soll. Dies ist insbesondere deshalb bemerkenswert, da der gegenständliche Ministerialentwurf des Teiles des sogenannten *Sicherheitspaketes* betreffend die Änderungen von SPG, TKG, StVO und BStMG erst zum 01. Jänner 2018 und die im zweiten Teil des Sicherheitspakets vorgesehene StPO-Regelung zur Überwachung verschlüsselter Nachrichten sogar erst mit 01. August 2019 in Kraft treten sollen.

## 2. Ausweitung der Videoüberwachung

### 2.1. Zu Art 1 Z 3, 11 und 12 des Entwurfs (§§ 53 Abs 5, 84 Abs 1 Z 7 und 91c Abs 3 SPG-ME)

Mit der Änderung des § 53 Abs 5 SPG soll ein Ausbau der technischen Ermittlungsmöglichkeiten der Sicherheitsbehörden dahingehend erfolgen, dass zur bestehenden Videoüberwachung eine Herausgabepflicht von Videomaterial, sowie die Möglichkeit eines Echtzeitstreamings umgesetzt wird. In diesem Sinn sollen die Rechtsträger des öffentlichen Bereichs oder des privaten Bereichs, sofern letzteren ein öffentlicher Versorgungsauftrag zukommt, den öffentlichen Raum zu überwachen, verpflichtet werden, bei ihr anfallendes Videomaterial auf Verlangen unverzüglich den Sicherheitsbehörden weiterzugeben oder zumindest Zugang dazu zu gewähren. Zudem soll es laut den Erläuterungen zu Art 1 Z 3, 11 und 12 des Entwurfs und der Maßnahmenbeschreibung (vgl Vorblatt/WFA 6) künftig zulässig sein, freiwillig von privaten oder öffentlichen Rechtsträgern überlassenes Videomaterial zur Aufgabenerfüllung zu verwenden.

Zur Durchsetzung der in § 53 Abs 5 dritter Satz des Entwurfs normierten Herausgabepflicht wird in § 84 Abs 1 Z 7 SPG ein Verwaltungsstraftatbestand für den Fall normiert, dass der Zugang zu den verarbeiteten Bilddaten nicht unverzüglich, somit ohne unnötigen Aufschub, gewährt wird. Für den vermeintlichen „Rechtsschutz“ diese Maßnahme betreffend hätte nach § 91c Abs 3 des Entwurfs der Rechtsschutzbeauftragte zu sorgen. Demnach ist dieser unverzüglich von der Sicherheitsbehörde von der Verwendung personenbezogener Bild- und Tondaten zu verständigen. Dauert die Maßnahme länger als drei Tage an, ist überdies die Genehmigung des Rechtsschutzbeauftragten erforderlich.

Fraglich ist hierbei allerdings zunächst, warum diese Befugniserweiterung im Allgemeinen überhaupt notwendig ist. **Nach geltender Rechtslage haben die Sicherheitsbehörden jedenfalls ausreichende Kompetenzen** im Rahmen ihrer Ermittlungstätigkeiten. Sohin dürfen diese nach § 53 SPG idgF rechtmäßig erzeugte personenbezogene Bilddaten verwenden, soweit dies zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht, zum Zwecke der Fahndung, zur Aufrechterhaltung der öffentlichen Ordnung, zur Abwehr krimineller Verbindungen oder gefährlicher Angriffe einschließlich Gefahrenerforschung dienlich ist.

Darüber hinaus soll den Sicherheitsbehörden diese Kompetenz laut dem vorliegenden Entwurf auch bereits zur Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt oder für die Vorbeugung gefährlicher Angriffe mittels Kriminalitätsanalyse zukommen, wenn nach der Art des Angriffes eine wiederholte Begehung wahrscheinlich ist. Insbesondere ist es aber für den ÖRAK nicht nachvollziehbar, warum die Beschränkung des § 53 Abs 3 SPG idgF hinsichtlich der Ermittlungsbefugnisse der Sicherheitsbehörden betreffend die Abwehr krimineller Verbindungen oder gefährlicher Angriffe (§ 53 Abs 1 Z 2 und 3 SPG idgF) durch die gegenständliche Gesetzesänderung ausgehebelt werden soll. Die Sicherheitsbehörden sollen daher nicht mehr nur in jenen Fällen rechtmäßig erzeugte personenbezogene Bilddaten verwenden dürfen, in welchen die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert wären, sondern soll dies künftig eine allgemeine Ermittlungsbefugnis darstellen.

Derartige in die Grundrechte der Bürger eingreifende Kompetenzen der Ermittlungsbehörden sind jedoch gerade in jenen Situationen, in denen eben **keine Gefahr oder erhebliche Erschwerung** der Ermittlungen besteht, **keinesfalls notwendig** und wären diese Maßnahmen einschließlich ihrer gesetzlichen Grundlage **nicht mehr mit dem verfassungsrechtlichen und auch im SPG verankerten Verhältnismäßigkeitsprinzip in Einklang zu bringen.**

Soweit der vorliegende Entwurf tatsächlich vorsieht, dass **freiwillig** (so zumindest die Erläuterungen zu Z 3, 11 und 12 Abs 2 erster Satz) von privaten oder öffentlichen Rechtsträgern überlassenes Videomaterial zur Aufgabenerfüllung verwendet werden kann, ist dies ebenso **abzulehnen**. Zunächst ist die Überwachung des öffentlichen Raumes, insbesondere durch Private, nach den Bestimmungen des DSG 2000 idgF nur in sehr engen Grenzen zulässig, nämlich nur dann, wenn ein geeigneter Zweck bzw gesetzlicher Auftrag erreicht werden soll und eine Überwachung des öffentlichen Raums zur Zielerreichung unumgänglich ist. Weiters ist diese Gesetzesänderung auch aus rechtspolitischen Erwägungen abzulehnen. Es kann nicht Ziel staatlichen Zusammenlebens sein, Private in Reminiszenz an *DDR-Methoden* zu animieren, ihre Umgebung zu überwachen und die daraus resultierenden personenbezogenen Bilddaten als halbstaatliche „Hilfssheriffs“ an die Sicherheitsbehörden zu übergeben.

Nicht nachvollziehbar ist zudem, dass die Sicherheitsbehörden laut dem gegenständlichen Entwurf nicht nur auf vorhandene, bereits erzeugte und den Sicherheitsbehörden übergebene personenbezogene Bilddaten zugreifen können sollen, sondern dass diese darüber hinaus direkt auf die Überwachungskameras (per Livestream) zugreifen dürfen. **Der ÖRAK lehnt eine solche verdachtsunabhängige Echtzeitüberwachungsmöglichkeit vehement ab.**

Diese Ablehnung ist vor allem auch eine Folge der im vorliegenden Entwurf mangelhaft umgesetzten Rechtsschutzmodalitäten, soweit man überhaupt von solchen sprechen kann. So dürfen durch die Sicherheitsbehörden gemäß § 91c Abs 3 SPG-ME alle zuvor erwähnten Ermittlungsmaßnahmen **ohne zuvor ergangenen Beschluss eines Gerichts** durchgeführt werden und müssen lediglich dem Rechtsschutzbeauftragen gemeldet werden. Erst wenn diese Ermittlungsmaßnahmen einen Zeitraum von drei Tagen übersteigen, bedarf dies der Genehmigung des Rechtsschutzbeauftragten. Es ist äußerst **besorgniserregend**, dass die Bevölkerung nach diesem Entwurf **den sehr umfassenden und grundrechtsintensiven Ermittlungsmaßnahmen der**

**Sicherheitsbehörden in den ersten drei Tagen gänzlich ohne Rechtsschutzmöglichkeit ausgesetzt werden soll** und dass danach lediglich der Rechtsschutzbeauftragte und eben **kein Gericht** mit dieser Angelegenheit befasst wird.

Auch aus diesem Grund erscheint es dem ÖRAK nicht empfehlenswert, Rechtsträger des öffentlichen Bereichs oder des privaten Bereichs, sofern letzteren ein öffentlicher Versorgungsauftrag zukommt, den öffentlichen Raum zu überwachen, dazu zu verpflichten, der Sicherheitsbehörde ohne richterlichen Beschluss ihr anfallendes Videomaterial auf Verlangen unverzüglich weiterzugeben oder Zugang dazu zu gewähren. Eine solche **Zweckentfremdung von bildgebenden Ressourcen zur unterschiedslosen und verdachtsunabhängigen Massenüberwachung** durch die Sicherheitsbehörde ist daher **abzulehnen**. Insbesondere steht diese Maßnahme auch im krassen Widerspruch zur Erreichung von Ziel 2 (Vorblatt/WFA 5), nämlich der Stärkung des Sicherheitsgefühls durch bürgernahe Polizeiarbeit. Durch diese Ermittlungsbefugnisse wird nämlich genau das Gegenteil erreicht, sohin eher das **Gefühl der ständigen Überwachung des Privatlebens** durch die Sicherheitsbehörden. Die in § 84 Abs 1 Z 7 SPG-ME vorgesehene mit Geldstrafe bedrohte Verwaltungsübertretung bei nicht unverzüglicher Weitergabe von personenbezogenen Bilddaten an die Sicherheitsbehörden mag zwar im Lichte dieses Entwurfes konsequent sein, ist aber, wie sämtliche Maßnahmen des § 53 Abs 5 SPG-ME, abzulehnen.

### 2.2. Zu Art 1 Z 4 und 15 des Entwurfs (§§ 53a Abs 6, 93a SPG-ME)

§ 53a Abs 6 SPG-ME sieht eine Verlängerung der Löschungsfrist von Daten zu Verdächtigen vor. Demnach soll im Fall einer mit mindestens dreijähriger Freiheitsstrafe bedrohten, vorsätzlichen strafbaren Handlung erst nach fünf Jahren eine Löschungsverpflichtung bestehen. Dies erscheint nicht rechtfertigbar. Vor allem dann nicht, wenn man in den Erläuterung zur betreffenden Bestimmung argumentiert, dass die Löschungsfrist nach geltender Rechtslage *„oftmals zu Ermittlungsdefiziten“* führt. Ein derart maßgeblicher Grundrechtseingriff vermag die strengen Voraussetzungen des verfassungsgesetzlich verankerten Verhältnismäßigkeitsprinzips nicht zu erfüllen.

§ 93a SPG-ME sieht vor, dass öffentliche und private Auftraggeber, soweit letzteren ein öffentlicher Versorgungsauftrag zukommt, den öffentlichen Raum zu überwachen, dazu verpflichtet werden, die örtlich zuständige Sicherheitsbehörde über die Verwendung von technischen Einrichtungen zur Bildverarbeitung zu informieren und räumt der Sicherheitsbehörde die Befugnis ein, mit Bescheid eine zwei Wochen nicht übersteigende Aufbewahrungsverpflichtung festzulegen, soweit dies aus Gründen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit oder allgemein der Strafverfolgung erforderlich ist.

Auch diese Befugnis ist nach Ansicht des ÖRAK viel **zu weitgreifend**. Die im Gesetzesvorschlag vorgesehene Begründung der Befugnisausübung ist zu allgemein gefasst. Insbesondere geht weder aus dem Gesetzeswortlaut, noch aus den Erläuterungen zu dieser Bestimmung oder aus den sonstigen beiliegenden Materialien hervor, wann eine Erforderlichkeit im Sinne des § 93a SPG-ME vorliegt. Die Sicherheitsbehörden können daher schon eine **Erforderlichkeit ohne ein**

**bestimmtes personenbezogenes Verdachtsmoment** erblicken und sodann eine zweiwöchige **de facto unterschiedslose und verdachtsunabhängige Vorratsdatenspeicherung von personenbezogenen Bilddaten öffentlicher und privater Rechtsträger anordnen**. Ein derartiger flächendeckender und verdachtsunabhängiger Eingriff in die Grundrechte auf Achtung des Privat- und Familienlebens und Datenschutz ist keinesfalls rechtfertigbar (VfGH G47/2012 ua).

Nach der Rechtsprechung des VfGH zur Vorratsdatenspeicherung (G47/2012 ua) ist auch beachtlich, dass der Zugriff eines sehr großen Personenkreises auf diese Daten ein überaus bedeutsames **Missbrauchsrisiko** birgt. Dies wird auch bei der gegenständlichen Bestimmung des Entwurfs einschlägig sein, da keine Einschränkung hinsichtlich des zugriffslegitimierten Personenkreises innerhalb der Sicherheitsbehörden getroffen wird. Darüber hinaus ist der Rechtsprechung des EuGH zur Vorratsdatenspeicherung von Standort- und Verkehrsdaten (siehe nur EuGH verb RS C-293/12 und C-594/12; C-203/15 und C-698/15) zu entnehmen, dass die Speicherung von Daten auf Vorrat nur dann zulässig wäre, wenn dadurch **schwere Straftaten** bekämpft werden sollen und wenn ein **Zugang zu diesen Daten der Kontrolle eines Gerichtes** oder einer sonstigen unabhängigen Stelle unterliegt. Außerdem **muss** der von der Datennutzung **Betroffene über diesen Vorgang informiert werden**.

Da bei gegenständlichem Gesetzesentwurf auch diese im Lichte der Judikatur des EuGH notwendigen Rechtsschutz- und Informationsmodalitäten nicht ersichtlich sind und nicht zwischen Maßnahmen betreffend die Bekämpfung schwerer und nicht schwerer Straftaten differenziert wird**, genügt diese Bestimmung auch den Anforderungen des Unionsrechts, insbesondere jenen der EU-Grundrechtecharta, nicht**.

### 2.3. Zu Art 1 Z 5, Z 7 bis 10, Art 2 und Art 3 des Entwurfs (§§ 54 Abs 4b, 57-59 SPG-ME, §§ 19a, 33 Abs 10 BStMG-ME und §§ 98a und 103 Abs 18 StVO-ME)

Mit der Änderung der obig bezeichneten Bestimmungen in SPG, BMStG und StVO soll es nunmehr zulässig sein, jene Bilddaten, die durch den Einsatz von bildgebenden technischen Einrichtungen an regelmäßig wechselnden Mautabschnitten zur Feststellung der ordnungsgemäßen Entrichtung der zeitabhängigen Maut erzeugt wurden, an die Sicherheitsbehörde zu übermitteln. Die Sicherheitsbehörde wird durch diese Gesetzesänderung dazu ermächtigt, die übermittelten Daten in Rahmen der polizeieigenen Kennzeichenerkennungssysteme zu benützen. Derartig übermittelte Daten sollen laut ME erst nach 48 Stunden gelöscht werden, sofern diese infolge nicht zur weiteren Verfolgung aufgrund eines Verdachts strafbarer Handlungen erforderlich sind.

Dies bedeutet im Zusammenhang mit § 53 Abs 5 SPG-ME (vgl dazu oben Punkt 2.1.), dass die ASFINAG hinkünftig dazu verpflichtet wird, alle durch den Einsatz von bildgebenden technischen Einrichtungen erzeugten Bilddaten an die Sicherheitsbehörde zu übermitteln. Dies allerdings nicht nur zur Erfassung und Abgleichung der Kennzeichen der die Mautstraßen befahrenden Fahrzeuge sondern auch, um im Trefferfall über das Kennzeichen hinausgehende Informationen zu erhalten. So insbesondere Informationen betreffend **Fahrzeugfarbe,**

**Fahrzeugmarke, Fahrzeugtype und Informationen zur Person des Fahrzeuglenkers**. Aufgrund dieser personenbezogenen Verkehrsdaten kann sodann auch ein **Bewegungsprofil der Verkehrsteilnehmer erstellt** werden.

Der ÖRAK lehnt eine **derartig unterschiedslose und vor allem verdachtsunabhängige Vollüberwachung der österreichischen Mautstraßen** einschließlich der damit verbunden Vorratsdatenspeicherung von personenbezogenen Bilddaten über 48 Stunden ab. Insbesondere bestürzend an dieser Bestimmung ist, dass diese auf Vorrat gesammelten personenbezogenen Bilddaten **überhaupt keinem Rechtsschutz (!)** unterliegen. So werden diese Daten in Zukunft schlichtweg an die Sicherheitsbehörde übermittelt. Dies ohne Information der betroffenen Personen (Lenker bzw. Fahrzeughalter) und gänzlich ohne gerichtliche Kontrolle oder durch die Kontrolle einer sonstigen unabhängigen Stelle. Nicht einmal dem Rechtsschutzbeauftragten wird hierbei eine Entscheidungskompetenz eingeräumt.

Auch bei dieser **Form der Vorratsdatenspeicherung** von personenbezogenen Bilddaten gilt das obig zu Punkt 2.2. Erwähnte betreffend die Judikatur des VfGH und EuGH zu auf Vorrat gespeicherten Standort- und Verkehrsdaten. So genügt auch diese unterschiedslose, flächendeckende und verdachtsunabhängige Überwachung aller Benützer der österreichischen mautpflichtigen Straßen nicht den Anforderungen der einschlägigen Rechtsprechung. Abgesehen davon, dass den **Betroffenen keinerlei Informationen über ihre Überwachung** zukommt und dass der Überwachungszweck nicht auf die Bekämpfung schwerer Straftaten beschränkt ist – nach den Erläuterungen zum ME werden diese Daten zur allgemeinen Gefahrenabwehr und zu allgemeinen Zwecken der Fahndung verwendet – **fehlt jegliche Rechtsschutzmöglichkeit durch von der Verwaltung unabhängige Gerichte**.

Einschlägig sind weiters auch jene Voraussetzungen, die der **VfGH** in seinem *Section Control*-Erkenntnis zu G147/06 ua entwickelt hat, um einen Eingriff in das Grundrecht auf Datenschutz durch den Einsatz von bilderzeugenden technischen Einrichtungen auf den österreichischen Mautstraßen auf seine verfassungsrechtliche Konformität zu prüfen und ist dabei zunächst auf die Einführung dieser Aufzeichnungskompetenz der ASFINAG gem § 19a BStMG abzustellen. Sohin ist ein Erfassen von Kennzeichen durch derartige technische Anlagen sinngemäß nur dann zulässig, wenn gesetzlich vorgesehen ist, dass alle jene Daten, aus denen kein Vorwurf des Mautprellens abgelesen werden kann, unverzüglich gelöscht werden. Weiters muss der Überwachungsbereich räumlich und zeitlich genau definiert sein. Der überwachte Abschnitt darf nicht beliebig gewählt werden, sondern muss eine besondere Notwendigkeit der Überwachung, also eine besondere Gefahrensituation in Hinblick auf Mautprellerei, aufweisen und die Messstellen müssen durch den zuständigen Bundesminister per Verordnung festgelegt und vor Ort auch für den Verkehrsteilnehmer erkennbar gekennzeichnet werden. Genau um diesen Voraussetzungen zu entsprechen, wurde **§ 19a BStMG idgF so konstruiert, dass insbesondere Daten aus denen sich nach dezentralem Abgleich ergibt, dass die Maut ordnungsgemäß entrichtet wurde, unverzüglich und auf nicht rückführbare Weise zu löschen sind**. Dies vor allem auch, um das Erstellen von Bewegungsprofilen zu vermeiden (ErlRV 1587 BlgNR 25 GP 5 f), wenngleich zum Zeitpunkt der Begutachtung dieser Bestimmung das BMI in seiner Stellungnahme zu

5/SN-284/ME 25 GP schon auf die gegenständliche Änderung des § 19a BStMG idgF hingewiesen hat.

Die nunmehrige durch den ME vorgesehene Zweckentfremdung der technischen Anlagen zur Kontrolle der ordentlichen Mautentrichtung ist mit all diesen Voraussetzungen keinesfalls mehr in Einklang zu bringen. So erfolgt die Massenüberwachung der österreichischen Mautstraßen nicht nur in bestimmten, besonders gekennzeichneten Gefahrenbereichen hinsichtlich des Mautprellens (wie beispielsweise Auffahrten zu mautpflichtigen Straßen), sondern **es wird das gesamte mautpflichtige Verkehrsnetz in Österreich umfasst**. Ein Datenabgleich mit hierdurch erfassten Bilddaten, die wesentlich mehr personenbezogene Daten beinhalten als zur Kontrolle der ordentlichen Maut notwendig sind, werden auch nicht dezentral, sondern durch ein **zentrales polizeieigenes Kennzeichenabgleichsystem** überprüft. Sie werden auch nicht unverzüglich gelöscht, sondern 48 Stunden gespeichert. Dies unabhängig davon, ob ihre Auswertung eine ordnungsgemäße Mautentrichtung ergibt oder nicht. Auch der eigentliche Zweck dieses Systems, nämlich das Schaffen der rechtlichen Rahmenbedingungen zur Einführung einer *digitalen Vignette* (vgl ErlRV 1587 BlgNR 25 GP 5) hat mit dem Überwachungszweck gemäß des vorliegenden Entw überhaupt nichts mehr zu tun.

Insgesamt ist diese Bestimmung des vorliegenden Entwurfs daher **nicht** mit den von VfGH und EuGH entwickelten Erfordernissen vereinbar, da sie auf nicht rechtfertigbare Weise in die Grundrechte auf Achtung des Privatlebens und Datenschutz eingreifen.

## 3. Sicherheitsforen

### 3.1. Zu Art 1 Z 2 und Z 6 des Entwurfs (§§ 25, 56 Abs 1 Z 9 und 10, 84 Abs 1 Z 8 SPG-ME)

Mit der Änderung dieser Bestimmungen soll die Möglichkeit geschaffen werden, „auf regionaler Ebene Plattformen zu bilden, in deren Rahmen (situationsbezogen) erforderliche Maßnahmen angeregt und koordiniert werden sollen“. Zur Teilnahme an diesen Sicherheitsforen sind Menschen, Einrichtungen und private Vereine, wie etwa Jugend- oder Elternvereine, NGOs und Wohnpartner aufgefordert, die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken wollen, um gemeinsam mit der Sicherheitsbehörde Problemlösungen in Sicherheitsfragen zu erarbeiten (Sicherheitspartner). Um eine *rasche und effektive Koordinierung im Rahmen von Sicherheitsforen zu bewirken*, bedarf es mitunter auch der Bekanntgabe personenbezogener Daten an die Teilnehmer dieser Sicherheitsforen.

Der gegenständliche Entwurf zielt laut seinen Erläuterungen darauf ab, **Präventionsmaßnahmen auf sicherheitspolizeilichem Gebiet auf Private (!) auszulagern**. Dies wird damit begründet, dass derartige Präventionsmaßnahmen nicht eine ausschließliche Angelegenheit der Sicherheitsbehörde seien.

Für den ÖRAK ist diese Argumentation überhaupt nicht nachzuvollziehen. Gerade weil dies eben Präventionsmaßnahmen auf sicherheitspolizeilichem Gebiet sind, geht es hier um eine der **Kernaufgaben von Sicherheitsbehörden**. **Es ist schlichtweg unerklärlich, warum anstelle einer adäquaten personellen und finanziellen**

**Ausstattung der Sicherheitsbehörden, sohin anstelle einer professionellen Problembewältigung durch dazu besonders ausgebildete Fachkräfte, Laien die Aufgaben von Sicherheitsbehörden (zumindest teilweise) übernehmen sollen**. Verdeutlicht wird diese Notwendigkeit einer ausschließlichen Aufgabenerfüllung durch qualifiziertes Personal unter Ansehung der Ausführungen des BMI in den beiliegenden Erläuterungen. So werden Privatpersonen durch diese Bestimmungen dazu animiert, sich als „Hilfssheriffs" an der regionalen Sicherheitsverwaltung zu beteiligen, um **erhöhte Sicherheitsrisiken, die infolge zu vermehrten gefährlichen Angriffen führen könnten, zu eliminieren**. Gerade an diesen Ausführungen wird veranschaulicht, wie wichtig eine professionelle Vorgehensweise bei derartigen Sicherheitsrisiken ist und dass eine laienhafte Erledigung diesen Anforderungen wohl kaum gerecht werden kann.

Darüber hinaus zeigen auch die Anwendungsbeispiele in den Erläuterungen dieses Entwurfs, wie **ineffizient und ineffektiv** durch die Sicherheitsforen gearbeitet werden soll und wie **wenig durchdacht** dieses Konzept der Sicherheitsverwaltung in Form von *community policing* eigentlich ist. So soll beispielsweise bei mangelhaft beleuchteten Parkanlagen ein Sicherheitsforum, bestehend aus der Sicherheitsbehörde, dem Stadtgartenamt, der Abfallbewirtschaftsungsstelle und der Straßenreinigung, „gebildet" werden, um dieses Sicherheitsrisiko zu eliminieren. Übersehen wird hierbei zunächst, dass all diese Teilnehmer des Sicherheitsforums aber eigentlich typischerweise weder dazu berechtigt sind, derartige Beleuchtungsmittel im Park aufzustellen (Entscheidungsträger ist vielmehr die Politik), noch über die hierfür notwendigen finanziellen Mittel verfügen können. Anstatt einen solchen bürokratischen Aufwand zu betreiben, der im Ergebnis dazu führt, dass bei den eigentlich zuständigen Entscheidungsträgern der kommunalen Verwaltung angeregt wird, einen Park mit Beleuchtungsmitteln auszustatten, könnte die Sicherheitsbehörde auch sogleich dieses offenkundige Sicherheitsrisiko wahrnehmen und ein Aufstellen von Beleuchtungsmittel bei den verantwortlichen Entscheidungsträgern anregen.

Für den ÖRAK ist der **besorgniserregendste** Teil dieses Entwurfs, dass **den Beteiligten der Sicherheitsforen zur Erledigung der Aufgaben der Sicherheitsbehörden, personenbezogene Daten übermittelt werden sollen**. So sollen beispielsweise bei Nachbarschaftskonflikten erforderliche personenbezogene Daten von den Sicherheitsbehörden an einen Wohnpartner (offensichtlich gemeint ist die Tätigkeit sogenannter Wohnpartner in der Verantwortung der Wohnservice Wien GmbH, welche im Auftrag der Stadt Wien arbeitet) übermittelt werden, dass dieser im Vorfeld in den Nachbarschaftskonflikt eingreift, um mögliche gerichtlich strafbare Handlungen zu verhindern. Hier wird sehr deutlich, wie **unbeteiligten Dritten personenbezogene Daten leichtfertig übermittelt** werden sollen (Art 1 Z 6 des Entwurfs). Bemerkenswert ist hierbei auch, dass Teilnehmer des Sicherheitsforums auch derartige Daten (wenngleich auch ohne Rechtsanspruch) von den Sicherheitsbehörden anfordern können. Besonders absurd ist jedoch die geplante Verwaltungsübertretung in § 84 Abs 1 Z 8 SPG (Art 1 Z 11 ME). So soll jener Teilnehmer des Sicherheitsforums, dem (sensible) personenbezogene Daten Dritter zur Aufgabenerfüllung von sicherheitsbehördlichen Kernaufgaben übermittelt werden, nur eine Geldstrafe in Höhe von € 500.-- bezahlen, wenn dieser bei der Erfüllung der auf ihn ausgelagerten Aufgaben seine Verpflichtung betreffend den vertraulichen Umgang mit den an ihn übermittelten Daten verletzt.

**Insgesamt ist auch diese im ME vorgesehene Gesetzesbestimmung absolut untauglich, um dem Ziel 2 (Vorblatt/WFA 7 f), nämlich der Stärkung des Sicherheitsgefühls durch bürgernahe Polizeiarbeit, zu erreichen. Vielmehr wird dadurch eher ein Gefühl der Überwachung und Bespitzelung des Privatlebens der Bürger durch ihre Nachbarn erzeugt.**

## 4. Quick Freeze

### 4.1. Zu Art 4 Z 4 und 5 des Entwurfs (§§ 99 Abs 1a bis 1f, 109 Abs 4 Z 9 bis 13 TKG-ME)

Mit diesem Entwurf soll die nach der derzeitigen Rechtslage geltende Verpflichtung von Telekommunikationsanbietern, Verkehrsdaten unverzüglich nach Beendigung der Verbindung bzw. sobald der Bezahlvorgang durchgeführt wurde und innerhalb einer Frist von drei Monaten, sofern die Entgelte nicht schriftlich beeinsprucht wurden, zu löschen, dahingehend geändert werden, dass eine **Unterbrechung dieser Löschungsverpflichtung** bei Vorliegen eines Anfangsverdachts bestimmter gerichtlich strafbarer Handlungen, durch die Staatsanwaltschaft angeordnet werden kann. Sohin können Telekommunikationsanbieter infolge dazu verpflichtet werden, die gespeicherten Daten bis zu 12 Monate zu speichern.

Der gegenständliche Gesetzesentwurf sieht eine **Anordnungsbefugnis der Staatsanwaltschaft** betreffend die Unterbrechung der Löschungsfristen vor, sofern ein Anfangsverdacht auf die Begehung einer Straftat vorliegt, der ein Vorgehen nach § 135 Abs 2 Z 2 bis 4 StPO rechtfertigen würde. Sohin soll eine derartige Anordnung zulässig sein, wenn dadurch die **Aufklärung einer Straftat begünstigt wird, die mit einer mehr als sechsmonatigen Freiheitsstrafe bedroht** ist.

Die Judikatur des EuGH zu C-293/12 und C-594/12 und C-203/15 und C-698/15 gibt jedoch vor, dass eine Vorratsspeicherung von Verkehrs- und Standortdaten nur dann zulässig sein soll, wenn dadurch die Aufklärung einer **schweren Straftat** bzw. einer Beteiligung hieran begünstigt wird. Eine Definition dieses Begriffs ist der Judikatur des EuGH nicht zu entnehmen. Es wird lediglich darauf verwiesen, dass dies nach den nationalen Regelungen auszulegen ist. Der Begriff der schweren Straftat findet sich auch nicht in der österreichischen Rechtsordnung wieder. Lediglich erfolgt eine Einteilung zwischen Vergehen und Verbrechen nach § 17 StGB im Hinblick darauf, ob eine Strafdrohung eine mit mehr als dreijährige Freiheitsstrafe vorsieht oder nicht bzw stellen schwerwiegende Straftaten einen Ausschlussgrund für eine diversionelle Erledigung gem § 198 Abs 2 StPO dar (*Seiler*, Strafprozessrecht[15] Rz 688). Hierunter fallen Straftaten, die mit mehr als fünf Jahren Freiheitsstrafe bedroht sind, bei denen die Schuld des Beschuldigten als schwer anzusehen ist oder den Tod eines Menschen zur Folge hatten. Unabhängig davon, welche dieser Definitionen man diesem Begriff zugrunde legt, wird sehr schnell **klar, dass die Anknüpfung an § 135 Abs 2 Z 2 bis 4 StPO in Ansehung der dort angeführten Strafdrohungen ab sechs Monaten (!) nicht mit der Rechtsprechung des EuGH in Einklang zu bringen ist**. Da in § 99 Abs 1a letzter Satz TKG-ME lediglich auf die Schwere der Straftat im Sinne von § 132 Abs 2 Z 2 bis 4 StPO abgestellt wird, ist davon auszugehen, dass eine Zustimmung des Inhabers der technischen Einrichtung keine Voraussetzung für diese Maßnahme darstellt.

Nach der Rechtsprechung des VfGH zur Vorratsdatenspeicherung (G47/2012 ua) ist auch beachtlich, dass der Zugriff eines sehr großen Personenkreises auf diese Daten ein überaus bedeutsames Missbrauchsrisiko birgt. Auch die Judikatur des EuGH (siehe nur C-203/15 und C-698/15 Rn 122 ff) sieht vor, dass dieses enorme Missbrauchsrisiko bei der Vorratsdatenspeicherung von Standort- und Verkehrsdaten dadurch eingeschränkt werden soll, dass die Mitgliedstaaten die Einhaltung des Schutzniveaus, das das Unionsrecht im Rahmen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten garantiert, durch eine unabhängige Stelle vorsehen. Anderenfalls würde den Personen, deren personenbezogene Daten gespeichert wurden, das durch Art. 8 Abs. 1 und 3 der EU-Grundrechtecharta garantierte Recht vorenthalten, sich zum Schutz ihrer Daten mit einer Eingabe an die nationalen Kontrollstellen zu wenden.

Gem § 99 Abs 1c TKG des Entwurfs ist geplant, dass die Telekommunikationsanbieter im Falle eines Zugriffs der Sicherheitsbehörden auf per Quick Freeze gesammelte Daten genaue Protokollierungen betreffend die zugreifende Person vornehmen müssen. Diese Protokolldaten haben aber gem § 99 Abs 1e TKG des Entwurfs nur auf schriftliches Ersuchen der Datenschutzbehörde zu erfolgen und stellt diese Bestimmung eine lex specialis zu Abs 1d leg cit dar, wo vorgesehen ist, dass die Telekommunikationsanbieter die Protokolldaten so aufzubereiten haben, dass dem Auskunftsrecht nach allgemeinen datenschutzrechtlichen Bestimmungen entsprochen werden kann. Fraglich ist aufgrund dieser Bestimmungen daher, wie man als von Quick Freeze Betroffener überhaupt von missbräuchlichen Zugriffen auf seine Verkehrs- und Standortdaten erfahren und infolge überhaupt eine Überprüfung durch ein Gericht bzw eine unabhängige Stelle beantragen kann, wenn man doch die genauen Protokolldaten gar nicht erst bekommt, sondern zunächst bei der Datenschutzbehörde anregen muss, dass diese schriftlich um Übermittlung der Protokolldaten bei dem betroffenen Telekommunikationsanbieter ersucht. Aufgrund dieser Konstruktion ist der durch die Rechtsprechung des EuGH vorgesehene Rechtsschutz so sehr und wesentlich erschwert, dass auch im Hinblick auf das Grundrecht auf effektiven Rechtsschutz gem Art 47 Abs 1 EU-GRC viel dafür spricht, dass auch diese Variante der Vorratsdatenspeicherung **nicht mit den Grundsätzen der Judikatur des EuGH vereinbar** ist.

Weiters sieht die Rechtsprechung des EuGH vor, dass dem von der Nutzung von auf Vorrat gespeicherten Daten Betroffenen umfassende Informationsrechte eingeräumt werden müssen. **Während im Arbeitsprogramm der Bundesregierung vom 30.01.2017 (Seite 24) noch die Pflicht der Sicherheitsbehörde vorzufinden war, dass im Ergebnis zu Unrecht überwachte Personen nach Abschluss der Ermittlungsmaßnahmen über diesen Umstand zu informieren wären, ist eine solche Bestimmung dem gegenständlichen Entwurf bedauerlicherweise nicht zu entnehmen.**

Die in § 109 Abs 4 Z 9 bis 13 TKG-ME eingefügten Strafbestimmungen mögen zwar konsequent sein im Lichte der Einführung einer Vorratsdatenspeicherung in Form von Quick Freeze, jedoch spricht sich der ÖRAK strikt gegen dieses Überwachungsmodell einschließlich der geplanten Strafbestimmungen aus den zuvor genannten Gründen aus.

## 5. Netzneutralität

### 5.1. Zu Art 4 Z 1 des Entwurfs (§ 17 Abs 1a TKG-ME)

Anbieter von Internetzugangsdiensten können Verkehrsmanagementmaßnahmen zur Vermeidung von strafrechtlich relevanten Handlungen, wie etwa Datenbeschädigung durch Viren, Computerkriminalität, Verbreitung von pornografischen oder gewaltverherrlichenden Darstellungen im Sinn der Jugendschutzgesetze an Minderjährige oder strafrechtlich relevante Urheberrechtsverletzungen, anbieten. Nach den Erläuterungen zu dieser Bestimmung soll hierdurch die Netzneutralität nicht berührt werden und sollen diese Verkehrsmanagementmaßnahmen im Einklang mit Art 3 der Verordnung 2015/2120/EU stehen.

Begründet wird dieser Vorschlag damit, dass hierdurch eine nicht zu rechtfertigende Benachteiligung der österreichischen Accessprovider verhindert werden würde und dass damit die Kompetenzen von Accessprovidern dahingehend erweitert werden, dass diese Accessprovider (IAP) in netzneutraler Weise die gleichen Services wie Serviceprovider (ISP) anbieten könnten. Völlig offen gelassen wird hierbei, welche Form der Benachteiligung die österreichischen Accessprovider bis zur Einführung des § 17 Abs 1a TKG-ME ohne die gesetzliche Ermächtigung zur Errichtung von Netzsperren trifft. Darüber hinaus ist nicht nachzuvollziehen, warum es überhaupt notwendig sein soll, dass IAPs die gleichen Dienstleistungen wie ISPs anbieten können, handelt es sich bei diesen Internetdienstleistern doch um gänzlich verschiedene Modelle und sind die dementsprechenden technischen und rechtlichen Bedürfnisse dementsprechend andere. Während IAPs lediglich den Zugang zum Internet herstellen sollen, sind die gebührenpflichtigen Dienste von ISPs umfassender und beinhalten daher das Herstellen und Bereitstellen der Konnektivität und Housings zum Internet, sowie der Instandhaltung, des Services, der Beratung und des Hostings. Folglich divergiert auch die Haftung dieser beiden Providertypen hinsichtlich der bereitgestellten Inhalte.

Darüber hinaus wird in dem gegenständlichen Gesetzesentwurf auch nicht dargelegt, wie diese Netzsperren technisch umzusetzen sind, sodass dieser Entwurf schon aus Gründen der Rechtssicherheit ungenügend erscheint und wird dabei auch unberücksichtigt gelassen, dass jene Netzsperren, die in der Vergangenheit von österreichischen Providern implementiert wurden, sehr häufig einfach durch die Verwendung von alternative DNS umgangen wurden.

**Art 3 Abs 3 UAbs 1 der VO 2015/2120/EU** ermöglicht den Internetzugangsdiensten, angemessene Verkehrsmanagementmaßnahmen anzuwenden. Dies ist der Fall, **wenn diese transparent, nichtdiskriminierend, verhältnismäßig sind und nicht auf kommerziellen Erwägungen, sondern auf objektiv unterschiedlichen technischen Anforderungen an die Dienstqualität bestimmter Datenverkehrskategorien beruhen**. Mit diesen Maßnahmen darf nicht der konkrete Inhalt überwacht werden und sie dürfen nicht länger als erforderlich aufrechterhalten werden. Der ÖRAK erlaubt sich anzumerken, dass den Providern hierdurch ein probates Mittel zur Zensur überlassen wird. Da in den Materialen und dem Gesetzeswortlaut selbst auch keinerlei Hinweis auf die nach der Art 3 Abs 3 UAbs 1 der VO 2015/2120/EU notwendigerweise anzuwendende Verhältnismäßigkeit

gemacht wird, erscheint eine **Vereinbarkeit dieser beiden Normen im Geltungsfall fraglich** und hätte diese nationale Bestimmung daher wohl unangewendet zu bleiben.

Insgesamt nicht nachzuvollziehen ist, warum diese Befugnis im Rahmen des Sicherheitspakets überhaupt vorgesehen wird. Dies insbesondere deswegen, weil aus den beiliegenden Materialen ganz klar hervorgeht, dass mit dieser Maßnahme überhaupt **keines der Ziele** des Sicherheitspakets erreicht werden soll.

## 6. SIM-Karten-Registrierung

### 6.1. Zu Art 4 Z 2 und 3 des Entwurfs (§§ 92 Abs 3 Z 3 lit g, 97 Abs 1a TKG-ME)

Nach dieser Bestimmung des gegenständlichen Gesetzesentwurfes soll es beim bisher anonymen Kauf von Prepaid-Karten für den Anbieter hinkünftig verpflichtend sein, die Identität des Teilnehmers, sohin seiner Stammdaten einschließlich Geburtsdatum, zu erfassen und zu registrieren.

Begründet wird diese drastische Maßnahme vor allem damit, dass *„sicherheitspolitische- und kriminalpolitische Zwecke“* (Vorblatt/WFA 3) dies erfordern würden.

Der ÖRAK spricht sich gegen diese Maßnahme aus. **Es ist absolut unverhältnismäßig die ca. 5,1 Mio. Verwender von Prepaid-Karten in Österreich** (vgl RTR Telekom Monitor, Jahresbericht 2016 20) **unter Generalverdacht zu stellen und folglich in ihre Grundrechte einzugreifen**. Darüber hinaus haben auch vergleichbare Maßnahmen in den anderen Ländern **nicht zu einer Erhöhung der Aufklärungsrate bzw. der Verhinderung von strafbaren Handlungen** geführt. Diese im Entwurf vorgesehene Maßnahme ist daher keinesfalls zur Zielerreichung geeignet und stellt hierfür schon gar nicht das gelindeste Mittel dar.

## 7. Pauschalbetrag nach Einschreiten der Organe des öffentlichen Sicherheitsdienstes

### 7.1. Zu Art 1 Z 13 und 14 des Entwurfs (§§ 92a Abs 1 und Abs 1a SPG-ME)

Mit gegenständlicher Gesetzesänderung soll die bestehende Regelung in **§ 92a Abs 1 SPG** idgF dahingehend ausgeweitet werden, dass die Inhaber von technischen Alarmeinrichtungen im Falle eines Fehlalarms einen Pauschalbetrag zur Abgeltung der einsatzbezogenen Aufwendungen des Bundes zu entrichten haben. Dies nunmehr auch in jenen Fällen, in denen die Alarmeinrichtung nicht nur zum Schutz von Eigentum oder Vermögen, sondern auch zum Schutz anderer Rechtsgüter dient. Hiergegen bestehen seitens des ÖRAK keine Einwände.

Ein differenziertes Bild ergibt sich in Ansehung der geplanten Änderung von **§ 92a Abs 1a** SPG-ME. So soll ein solcher Pauschalbetrag auch von demjenigen zu bezahlen sein, der ein Einschreiten von Organen des öffentlichen Sicherheitsdienstes verursacht, weil er **vorsätzlich** eine falsche Notmeldung abgibt oder sich grob fahrlässig einer Gefahr für Leben oder Gesundheit ausgesetzt hat. **Gegen die erste alternative Voraussetzung hat der ÖRAK keine Bedenken**. Er spricht sich jedoch dagegen aus, einen solchen Pauschalbetrag entrichten zu müssen, wenn man sich

grob fahrlässig in eine Gefahrensituation begibt. Sollte man in einer Alltagssituation tatsächlich einmal die objektiv gebotene Sorgfalt bei Weitem außer Acht lassen und sich sodann die Notwendigkeit eines Einsatzes des öffentlichen Sicherheitsdienstes ergeben, erscheint es nicht vertretbar, einen Pauschalbetrag zu diesem Einsatz leisten zu müssen. Dies insbesondere in Ansehung dessen, dass die Abgrenzung von Vorsatz und Fahrlässigkeit gerade darin besteht, dass eben der den Einsatz auslösende Erfolg nicht gewollt ist. Darüber hinaus werden diese Einsatzkosten ohnehin durch steuerliche Abgaben finanziert, sohin auch von dem grob fahrlässig Handelnden. Es ist daher nicht nachvollziehbar, warum dieser infolge doppelt zu den Aufwendungen dieses Einsatzes beitragen soll, obwohl er diesen Erfolg ja gerade **nicht herbeiführen wollte**. Der verwaltungstechnische Aufwand steht überdies in keinem Verhältnis zu den Pauschalbeträgen.

## 8. Zusammenfassung

Der gegenständlich vorliegende ME des Teils zum Sicherheitspaket betreffend die Änderung von SPG, TKG, BStMG und StVO enthält zahlreiche Maßnahmen, die nach Ansicht des ÖRAK nicht mit den durch die grundrechtliche Judikatur von VfGH und den vom EuGH entwickelten Grundsätzen in Einklang zu bringen sind, da **sie tiefgreifende, nicht rechtfertigbare Einschnitte in die Grundrechte der Bevölkerung** in Österreich darstellen. **Besonders besorgniserregend sind die Bestrebungen des BMI betreffend die flächendeckende, verdachtsunabhängige und maßlose Videoüberwachung und Vorratsdatenspeicherung**, wenn auch in Form von Quick Freeze. Darüber hinaus ist der ÖRAK besorgt, wie leichtfertig in Zukunft mit sensiblen personenbezogenen Daten im Rahmen eines in wesentlichen Teilen verfehlten „Sicherheitskonzeptes“ umgegangen werden soll. Nicht nachvollziehbar ist zudem, warum **5,1 Mio. Prepaid-Kartenbenützer in Österreich unter Generalverdacht** gestellt werden und aus welchem Grund im Rahmen dieses Sicherheitspaketes die österreichische Netzneutralität umgangen werden soll.

Insgesamt spricht sich der ÖRAK daher gegen den vorliegenden Teil des Sicherheitspaketes, wie auch gegen das gesamte Sicherheitspaket, aus.

Wien, am 21. August 2017

DER ÖSTERREICHISCHE RECHTSANWALTSKAMMERTAG

Dr. Rupert Wolff
Präsident