Republik Österreich
Datenschutzbehörde

A-1010 Wien, Hohenstaufengasse 3
Tel.: ++43-1-53115 202769
Fax: ++43-1-53109 202690
E-Mail: dsb@dsb.gv.at
DVR: 0000027

GZ: DSB-D054.765/0001-DSB/2017

Sachbearbeiter: Mag. Michael SUDA

Präsidium des Nationalrats

Dr. Karl Renner-Ring 3
1017 Wien

Begutachtung - Legistik (BMI)
Entwurf für ein BG Änderung SPG, BStMG 2002, StVO, TKG 2003

per E-Mail: begutachtungsverfahren@parlament.gv.at

Betrifft: Stellungnahme der DSB zum Gesetzesentwurf GZ: BMI-LR1340/0019-III/1/2017

Bezug: Parlamentszahl 326/ME

1. Die Datenschutzbehörde (DSB) nimmt in o.a. Angelegenheit aus Sicht Ihres Wirkungsbereiches wie folgt Stellung:

   a) Allgemeines

2. Der vorliegende Entwurf einer Sammelnovelle sieht eine Änderung mehrerer Bundesgesetze, die teilweise nicht in den Vollzugsbereich des Bundesministers für Inneres fallen, vor. Er steht als sogenanntes „Sicherheitspaket“ im Zusammenhang mit dem Entwurf eines Strafprozessrechtsänderungsgesetzes 2017, GZ: BMJ-S578.031/0008-IV 3/2017 des Bundesministeriums für Justiz, der zeitlich parallel einem öffentlichen Begutachtungsverfahren unterzogen wird. Die folgende Stellungnahme folgt der Gliederung nach den vorgesehenen datenschutzrechtlich relevanten Maßnahmen als da wären b) erweiterte Nutzung nicht-sicherheitsbehördlicher Videoüberwachungen (in der Terminologie des DSG zukünftig: Bildaufnahmen), c) automatische Fahrzeugdatenerfassung samt Datenabgleich, d) Verbot nicht-identifizierter Nutzung von Telekommunikationsdiensten, e) Ermächtigung zur Umsetzung unionsrechtlich vorgesehener Verkehrsmanagementmaßnahmen, f) Einführung einer „Quick-Freeze“-Regelung und g) Datenverwendung für Zwecke von „Sicherheitsforen“.

3. Da das Inkrafttreten (vorgesehen für den 1. Jänner 2018) frühestens im Laufe des Jahres 2018 zu erwarten wäre, wurden als allgemeiner datenschutzrechtlicher Maßstab die Datenschutzgrundverordnung (Verordnung des Europäischen Parlaments und des Rates 2016/679 vom 27. April 2016), das Datenschutzgesetz (DSG) in der ab 25. Mai 2018 anzuwendenden Fassung gemäß Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017, sowie die RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119/89-139, die bis zum 25. Mai 2018 in nationales Recht umzusetzen ist, herangezogen.

4. Formell ist generell anzumerken, dass die im Normtext und den Materialien verwendeten Begriffe von rechtlicher Bedeutung an die Terminologie der beiden Vorschriften des Unionsrechts und des Datenschutz-Anpassungsgesetzes 2018 anzupassen wären. Demnach sollten etwa Begriffe wie *„Videoüberwachung“*, *„Verwenden“* oder *„Verwendung“* von Daten vermieden werden. Hierzu wird auf das inzwischen ergangene Rundschreiben des Bundeskanzleramts-Verfassungsdienst vom 2. August 2017, BKA-810.026/0035-V/3/2017, verwiesen.

b) <u>erweiterte Nutzung nicht-sicherheitsbehördlicher Videoüberwachungen/Bildaufnahmen (Art. 1 Z 2 bis 17 Entwurf)</u>

5. Die DSB macht zunächst darauf aufmerksam, dass der Begriff des „öffentlichen Raums“ in Art. 1 Z 3 des Entwurfs sehr weit gefasst ist, und in umfassender Betrachtung sowohl Orte und Flächen umfasst, an denen Gemeingebrauch besteht (wie Straßenflächen, öffentliche Brücken, Unterführungen, Parkanlagen u.dgl.m.), als auch Orte und Flächen, die im Regelfall für jedermann, eventuell aber nur gegen Entgelt (oder unter ähnlichen Beschränkungen wie der Pflicht zum Besitz eines Fahrausweises oder einer Bordkarte), zugänglich sind. Die Pflicht zur Unterstützung der Sicherheitsbehörden durch erweiterte Nutzung der Daten einer Bildaufnahme träfe nur Rechtsträger des öffentlichen Bereichs und solche des privaten Bereichs, denen *„ein öffentlicher Versorgungsauftrag zukommt“*. Gedacht ist an die Überwachung von Bahnhofs- Nahverkehrs- und Flughafenanlagen, Zügen und Linienbussen aller Art (Fern- und Nahverkehr) sowie von Parkplätzen, Tankstellen und Raststätten an Autobahnen. Der vorliegende Entwurf würde demnach auch Rechtsträgern des privaten Bereichs, denen ein öffentlicher Versorgungsauftrag zukommt, etwa Eisenbahninfrastruktur-, Eisenbahnverkehrsunternehmen und integrierten Eisenbahnunternehmen (§ 1a bis 1c des Eisenbahngesetzes 1957 - EisbG, BGBl. Nr. 60/1957 idgF) oder Zivilflugplatzhaltern („Flughafenbetreiber“, § 75 des Luftfahrtgesetzes - LFG, BGBl. Nr. 253/1957 idgF) bestimmte Pflichten zugunsten der Sicherheitsbehörden auferlegen. Die Abgrenzung könnte im Streitfall schwierig sein (z.B. unterliegt auch der Pächter und Betreiber einer Autobahnraststätte einer Herausgabepflicht betreffend Bildaufnahmen aus dem Inneren seiner Gasträume?).

6. Die Bilddaten einer Bildaufnahme sind auf Verlangen einer Sicherheitsbehörde unverzüglich an diese zu übermitteln (*„weiterzugeben“*) oder Vorkehrungen zu treffen, um einer verlangenden Sicherheitsbehörde Zugang zu den Daten zu gewähren (Entwurf Art. 1 Z 3), sowie die Bildaufnahme zu melden und die Bilddaten auf bescheidmäßigen Auftrag hin länger als 72 Stunden zu speichern (Art. 1 Z 15 des Entwurfs). Zulässige Zwecke des Eingriffs wären a) die Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, sexuelle Integrität und Selbstbestimmung, Freiheit oder Vermögen, b) die Abwehr gefährlicher Angriffe wie zu a), c) die Abwehr krimineller Verbindungen sowie d) die Fahndung nach Personen (§ 24 SPG). Eine Befassung des Rechtsschutzbeauftragten ist vorgesehen (Art. 1 Z 12 des Entwurfs) und ein länger als drei Tage dauernder „Zugriff“ der Sicherheitsbehörden auf Bildaufnahmen wäre an dessen Zustimmung gebunden.

7. Bei Gesichtsbildern, die aus dem Datenbestand einer Bildaufnahme gewonnen werden können, handelt es sich um biometrische Daten gemäß § 36 Abs. 2 Z 13 DSG.

8. Der Wortlaut der im Entwurf vorgesehenen Bestimmung lässt die Antwort der Frage offen, ob mit der Alternativvariante der Zugangsgewährung (*„oder Zugang dazu zu gewähren...“*, Hervorhebung durch die Datenschutzbehörde) eine Ermächtigung an die Sicherheitsbehörden verbunden ist, sich in eine Bildaufnahme einzuschalten und deren Daten gegebenenfalls selbst zu speichern, da nach dem Wortlaut nur *„dazu“*, das heißt zu den bereits verarbeiteten und gemäß Hauptfall zu übermittelnden Bilddaten, Zugang zu gewähren wäre. Der für die Verarbeitung einer Bildaufnahme Verantwortliche wäre daher nach dem Wortlaut verpflichtet, der Sicherheitsbehörde etwa Zugriff zu den auf eigenen Datenträgern oder auf dem Server eines Dienstleisters, z.B. eines Sicherheitsunternehmens (Wachdienst, Berufsdetektiv o.ä.) oder Cloud-Speicherdienstes, liegenden Daten zu gewähren, nicht jedoch einen Echtzeitzugriff auf die Bildaufnahme zu gestatten.

9. Die Bestimmung dürfte daher auf Grund des Wortlauts, anders als in den Erläuterungen (Seite 2, zu Z 3, 11 und 12) angeführt, in der vorgeschlagenen Fassung nach Ansicht der Datenschutzbehörde grundrechtskonform nur so ausgelegt werden, dass damit eine Ermächtigung zum *„Echtzeitstreaming“* an die Sicherheitsbehörde nicht verbunden wäre. Es wird angeregt klarzustellen, welche Pflichten den für die Verarbeitung Verantwortlichen tatsächlich treffen sollen, nicht zuletzt da ein *„Echtzeitstreaming“* ganz andere technische Voraussetzungen erfordern könnte als die bloße Übermittlung einer Bilddatendatei.

10. Mit diesem vorliegenden Gesetzesvorschlag wäre zweifellos ein nachhaltiger Eingriff in die datenschutzrechtliche Geheimhaltungssphäre einer potenziell sehr hohen Zahl von Betroffenen verbunden, da er die Reichweite und den Fokus der „Augen des Gesetzes“ beträchtlich erweitern würde. Eine Interessenabwägung gemäß den Verfassungsbestimmungen Art. 1 Abs. 2 DSG iVm Art. 8 Abs. 2 EMRK kann nur erfolgen, wenn die Notwendigkeit des Grundrechtseingriffs ausreichend dargelegt worden ist. Die Datenschutzbehörde verkennt nicht, dass der vorgesehene Eingriff ein denkmöglich geeignetes Mit-

tel insbesondere zur Aufklärung von Straftaten sein könnte, was in eine gesetzgeberische Interessenabwägung einzubeziehen wäre. Dass er jedoch notwendig in dem Sinne ist, dass die Aufgaben der Sicherheitsbehörden ohne die entsprechende Ermächtigung nicht oder nicht ausreichend erfüllt werden könnten, geht nach Ansicht der DSB weder aus den Erläuterungen noch aus der WFA mit ausreichender Klarheit hervor. Die vorgesehenen Bestimmungen sind weiters so gestaltet, dass die Pflicht zur Zugänglichmachung der Bildaufnahme legistisch unschwer, etwa durch Änderung oder Entfall des Begriffs *„öffentlicher Versorgungsauftrag“*, auch auf andere private Verantwortliche (wie Betreiber von Einkaufszentren oder Kaufhäusern, Theatern, Konzert- und Veranstaltungshallen oder Parkgaragen) ausgedehnt werden könnte.

11. Kritisch zu betrachten ist auch die in Art. 1 Z 15 bis 17 des Entwurfs vorgesehene Ermächtigung an die Sicherheitsbehörden, öffentliche und private Verantwortliche im obigen Sinne zu einer Meldung ihrer Bildaufnahmen bei der örtlichen Sicherheitsbehörde zu verpflichten und letztere Behörde dazu zu ermächtigen, eine verpflichtende Speicherdauer von Bilddaten bis zu zwei Wochen durch Bescheid festzulegen. Dabei ist praxisbezogen wohl davon auszugehen, dass die Sicherheitsbehörden versucht sein werden, jeden meldepflichtigen Verantwortlichen zu einer zweiwöchigen Bilddatenspeicherung zu verpflichten, da die Voraussetzungen dafür in allen in Frage kommenden „Grobfällen“ (Bahnhöfe, Flughäfen, Autobahnen, öffentliche Verkehrsmittel) in etwa gleich gelagert sein werden. Eine sachlich gerechtfertigte Differenzierung *„im Einzelfall“* könnte aber nur nach Auswertung ortsbezogener Vorfallsstatistiken, erfolgen und müsste dann zur Festlegung einer Speicherdauer für jeden einzelnen Standort einer Bildaufnahme (und nicht für jeden Verantwortlichen pauschal) führen. Wie dies im Fall der Bildaufnahme in Fahrzeugen, die etwa im Linienbetrieb eines Verkehrsunternehmens einmal auf einer *„vorfallsgeneigten“*, einmal aber wieder auf einer *„ruhigen“* Linie zum Einsatz kommen, bewerkstelligt werden soll, lässt sich dem vorliegenden Entwurf nicht entnehmen. Es wäre hinsichtlich einer verlängerten Speicherdauer von Daten bestimmter Bildaufnahmen, so diese für unerlässlich erachtet wird, wohl ehrlicher, klarer und für die Verantwortlichen und die Sicherheitsbehörden einfacher, in den in Frage kommenden und genau definierten Fällen durch das Gesetz eine längere Speicherdauer festzulegen.

12. Welchem Zweck das in Art. 1 Z 17 des Entwurfs vorgesehene Inkenntnissetzen der Datenschutzbehörde durch die Sicherheitsbehörde dienen soll, erschließt sich aus dem Normtext nicht. Da die Datenschutzbehörde ab dem 25. Mai 2018 keine entsprechenden Meldungen mehr entgegennimmt oder Bildaufnahmen registriert, gibt es hier keinen Bezug zu einem bestimmten behördlichen Verfahren. Die Mitteilung könnte daher nur aktenmäßig dokumentiert, also abgelegt werden. Eine Rechtsmittelbefugnis der Datenschutzbehörde als Amtspartei gegen den vorgesehenen Bescheid ist nicht im Gesetz vorgesehen.

c) automatische Fahrzeugdatenerfassung samt Datenabgleich (Art. 1 Z 5, 7 und 9, Art. 2 Z 1 und 2 und Art. 3 Z 1 und 2 des Entwurfs)

13. Die vorgeschlagenen Bestimmungen würden die Sicherheitsbehörden ermächtigen, Bilddaten von Kraftfahrzeugen und Insassen mittels Bilderkennungssoftware zu verarbeiten und mit anderen Systemen, insbesondere mit dem zentralen Kraftfahrzeugregister (KZR) des BMI und polizeilichen Fahndungsevidenzen, abzugleichen. Dabei würde nach Inkonsistenzen zwischen dem real aufgenommenen und dem zugelassenen Kraftfahrzeug (z.B. Farbe oder Marke passen nicht zum Kennzeichen, Kennzeichen könnte daher gefälscht oder gestohlen sein) gesucht und das Kennzeichen – und nur dieses – mit den Fahndungsevidenzen (insbesondere der gestohlenen Kraftfahrzeuge) abgeglichen werden. Zweiteres ist bereits jetzt gemäß § 54 Abs. 4b SPG idgF zulässig. Die Sicherheitsbehörden dürfen dafür bereits jetzt eigene bildverarbeitende technische Einrichtungen zum Einsatz bringen. Nach dem Entwurfstext dürften auch Bilddaten des Fahrzeuglenkers verarbeitet werden, deren direkter Abgleich mit Fahndungsevidenzen wäre nicht zulässig. Sie dürften allerdings verarbeitet (gespeichert, verglichen) und übermittelt werden, wenn sich aus anderen Gründen der Verdacht eines gefährlichen Angriffs oder einer kriminellen Verbindung ergibt.

14. Die vorgeschlagenen Gesetzesbestimmungen würden die Verkehrs- und Straßenpolizeibehörden und die ASFINAG verpflichten, für Zwecke der Verkehrsüberwachung und der Mautkontrolle verarbeitete Bilddaten an die Sicherheitsbehörden zu übermitteln. Der entsprechende Datenvergleich bzw. –abgleich dürfte gemäß Art. 1 Z 7 des Entwurfs nur durch den Bundesminister für Inneres (bzw. die diesem direkt unterstehenden Dienststellen und Einheiten der Sicherheits- und Kriminalpolizei) erfolgen.

15. Hierzu ist zu bemerken, dass die ASFINAG zwar nach Kenntnis der Datenschutzbehörde Eigentümerin (mobiler) technischer Einrichtungen zur Verkehrsüberwachung gemäß § 98a StVO (Abschnittsbezogene Geschwindigkeitsüberwachung, alias „Section Control“) ist, die behördlichen Befugnisse und damit auch die Rolle als für die Verarbeitung Verantwortlicher aber auf Autobahnen gemäß § 94a Abs. 1 und Abs. 2 lit a) StVO bei den Landesregierungen liegt. Entsprechendes geht auch aus dem Stand des von der Datenschutzbehörde geführten DVR hervor. Für andere Straßen liegt die entsprechende Befugnis bei der Bezirksverwaltungsbehörde oder der Landespolizeidirektion im Rahmen der Aufgaben gemäß § 94b StVO. Insbesondere die ASFINAG ist daher gar nicht befugt, entsprechende Bilddaten *„auf Grundlage des § 98a StVO“* zu ermitteln und kann solche daher auch nicht übermitteln. Es wird angeregt, die Erläuterungen (zu Artikel 3, Seite 5) entsprechend anzupassen. Die Befugnisse der ASFINAG zur Bilddatenverarbeitung erstrecken sich nur auf die Zwecke des § 19a BStMG (*„zur Feststellung der ordnungsgemäßen Entrichtung der Maut und zur Verfolgung von Mautprellerei“*).

16. Die Verarbeitung der selbst ermittelten oder von ASFINAG oder Verkehrs- und Straßenpolizeibehörden übermittelten Bilddaten würde auf die Zwecke der Abwehr und Aufklärung gefährlicher Angriffe gegen Leben, Gesundheit, sexuelle Integrität und Selbstbestimmung, Freiheit oder Vermögen sowie zur Abwehr krimineller Verbindungen beschränkt. Grundsätzlich würde sonst eine Löschungsfrist von 48 Stunden nach Verarbeitung (Art. 1 Z 5 des Entwurfs) oder Übermittlung (Art. 2 Z 9 des Entwurfs) gelten.

17. Auch in diesem Fall gilt sinngemäß das oben in Rz. 10 Gesagte. Dies allerdings mit der Maßgabe, dass die Bilddatenverarbeitung auf deutlicher konkretisierte Zwecke der Fahndung fokussiert, und die zur Datenübermittlung verpflichteten Verantwortlichen nur solche aus dem öffentlichen Bereich (wobei die ASFINAG hier hinsichtlich der Mauteinhebung als mit hoheitlichen Befugnissen beliehener Privatrechtsträger zu betrachten ist) wären. Dabei ist auch in Rechnung zu stellen, dass insbesondere die Verkehrsüberwachung gemäß § 98a StVO auf bestimmte, an strenge Voraussetzungen gebundene Anlassfälle beschränkt ist. Faktisch würde sich die eingriffsintensivste, ständige bzw. nicht allgemein wahrnehmbare Überwachung (durch Section-Control-Einrichtungen und Mautkontrolleinrichtungen der ASFINAG) laut lit. c) auf bestimmte Hauptverkehrswege, insbesondere Autobahnen und Schnellstraßen, beschränken.

18. Um die Regelung grundrechtskonform zu gestalten und zu verhindern, dass damit ein System einer durchgehenden Überwachung sämtlicher Wegstrecken im Bundesgebiet (vgl. dazu VfGH E 15.06.2007, VfSlg 18146/2007, Section Control) geschaffen wird, könnte vorgesehen werden, die aktuell auch im Dienste der Sicherheitsbehörden betriebenen Überwachungseinrichtungen oder die von den Sicherheitsbehörden selbst gemäß Art. 1 Z 5 des Entwurfs mit bildverarbeitenden technischen Einrichtungen überwachten Streckenabschnitte, ähnlich wie Section-Control-Abschnitte, möglichst in Echtzeit (etwa durch eine ein- und ausschaltbare optische Kennzeichnung) anzukündigen. Weiters wird angeregt, die Durchführung einer solchen Überwachung an die nachweisliche Notwendigkeit von Maßnahmen zur Abwehr oder Aufklärung gefährlicher Angriffe und die Zustimmung des Rechtsschutzbeauftragten beim Bundesminister für Inneres zu binden.

d) Verbot nicht-identifizierter Nutzung von Telekommunikationsdiensten (Art. 4 Z 2 und 3 des Entwurfs)

19. Die vorgeschlagene Regelung kommt einem Verbot nahe, ohne persönliche Identifizierung des Teilnehmers bzw. Nutzers öffentliche Kommunikationsdienste in Anspruch zu nehmen. Sie ist damit ein Eingriff sowohl in das Grundrecht auf Datenschutz (Art. 8 GRC, § 1 Abs. 1 DSG 2000), da sie eine Verpflichtung zu Verarbeitung personenbezogener Daten schafft, als auch, wenn auch in geringerem Maße, in das Grundrecht auf informations- und Kommunikationsfreiheit (Art. 10 EMRK, Art. 10 GRC).

20. Gesetzestechnisch wird dies dadurch umgesetzt, dass Betreiber von Kommunikationsdiensten (wenn auch ohne Vorkehrung einer Strafdrohung) verpflichtet werden, die *„zur Identifizierung des Teilnehmers erforderlichen Stammdaten zu registrieren“*. Die im TKG 2003 zur Verarbeitung vorgesehenen Stammdaten werden dabei um das Geburtsdatum (vorgesehener § 92 Abs. 3 Z 3 lit g) TKG 2003) ergänzt. Das Geburtsdatum soll dabei vermutlich erhoben und verarbeitet werden, um einen zuverlässigeren Abgleich der Daten mit polizeilichen Datenverarbeitungen zu ermöglichen.

21. Ein legistisch präziser Grundrechtseingriff sollte jedenfalls die *„erforderlichen Stammdaten“* genau umschreiben (siehe § 92 Abs. 3 Z 3 lit a) bis f) (in eventu g)) TKG 2003. Für die Identifizierung einer Per-

son werden nach Ansicht der Datenschutzbehörde höchstens jene gemäß lit a) bis c) (und in eventu g)), keinesfalls jedoch Daten zur Bonität des Teilnehmers benötigt.

e) Ermächtigung zur Umsetzung unionsrechtlich vorgesehener Verkehrsmanagementmaßnahmen (Art. 4 Z 1 des Entwurfs)

22. Die hier vorgesehene Regelung hat vorrangig kommunikationsrechtlichen Charakter. Der Anwendungsbereich erscheint insoweit fraglich, als eine entsprechende Ermächtigung zu „Verkehrsmanagementmaßnahmen“ bereits durch Art. 3 Abs. 3 Unterabsatz 3 lit.a) bis c) der VERORDNUNG (EU) 2015/2120 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union, Abl. L 310/1-18, geschaffen wird. Es handelt sich um eine unmittelbar anwendbare Vorschrift des Unionsrechts. In Art. 3 Abs. 3 Unterabsatz 3 lit. a) der Verordnung 2015/2120/EU ist festgelegt, dass solche Eingriffe in den freien Datenverkehr u.a. erforderlich sein können, um mit dem Unionsrecht im Einklang stehenden nationalen Rechtsvorschriften, denen der Internetzugangsanbieter unterliegt, oder mit dem Unionsrecht im Einklang stehenden Maßnahmen zur Umsetzung dieser Gesetzgebungsakte der Union oder dieser nationalen Rechtsvorschriften zu entsprechen.

23. Konkret geht es beim vorliegenden Gesetzesvorschlag darum, ob und inwieweit Internetzugangsdienste ermächtigt werden, die freie Kommunikation im Internet 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, zu blockieren. Ein solches Blockieren, auch als Netzsperre bekannt, wäre ein massiver Eingriff in die grundrechtlich garantierte Informationsfreiheit der Betroffenen (Art. 10 EMRK, Art. 11 GRC) dar.

24. Es wird angeregt, eine Art. 3 Abs. 3 Unterabsatz 3 lit. a) der Verordnung 2015/2120/EU entsprechende nationale Rechtsvorschrift (arg: *„...denen der der Internetzugangsanbieter unterliegt“*; Hervorhebung durch die Datenschutzbehörde) als „Muss“- und nicht als „Kann“-Bestimmung zu fassen, da es auch nach der Verordnung 2015/2120/EU nicht ins Ermessen von Privatunternehmen gestellt werden darf, Eingriffe in das Grundrecht auf Informationsfreiheit gemäß Art. 11 GRC vorzunehmen. In Erwägungsgrund 13 zur Verordnung 2015/2120/EU ist die Rede von Rechtsvorschriften *„(beispielsweise die Rechtmäßigkeit von Inhalten, Anwendungen oder Diensten, oder die öffentliche Sicherheit betreffend), einschließlich strafrechtlicher Vorschriften, die beispielsweise die Blockierung bestimmter Inhalte, Anwendungen oder Dienste vorschreiben“*. Daraus geht aus Sicht der Datenschutzbehörde klar hervor, dass es sich um staatliche Maßnahmen zwingenden Charakters und nicht um bloße Ermächtigungsnormen handeln muss.

25. Auch erschließt sich der Sinn der Ermächtigung an Internetzugangsanbieter nicht, entsprechende Verkehrsmanagementmaßnahmen anzubieten. Falls damit gemeint sein sollte, dass ein Internetzugangsanbieter seinen Kunden damit vertraglich anbieten dürfte, etwa alle bekannten IP-Adressen, über die Schadsoftware oder Kinderpornografie verbreitet werden, zu deren eigener Sicherheit zu sperren, so würde der Internetzugangsanbieter damit eine Gewährleistungspflicht in der Art einer strafrechtlichen Garantenstellung für den Nichtkontakt mit Schadsoftware oder Kinderpornografie übernehmen, die einerseits bei realistischer Betrachtung kaum lückenlos zu bewältigen wäre und andererseits schon aus Gründen des Haftungsrisikos nur gegen ein entsprechend hohes Entgelt erbracht werden könnte. Überdies steht es jedem Nutzer von Internetdiensten frei, auf seinen eigenen Geräten entsprechende Schutz- und Sicherheitssoftware (z.B. wenn Kinder solche Geräte nutzen) zu installieren.

26. Insbesondere durch die Bezugnahme auf strafrechtlich relevante Urheberrechtsverletzungen könnte nicht ausgeschlossen werden, dass auf die vorgeschlagene Bestimmung auch Eingriffe auf Verlangen Dritter gestützt werden könnten. Soweit es sich dabei um gerichtlich angeordnete Sperren auf Grundlagen urheberrechtlicher Ansprüche handeln sollte, so besteht dafür in § 81 Abs. 1a UrhG bereits eine ausreichende Grundlage und eine inzwischen gefestigte Rechtsprechung zu Gunsten von Rechteinhabern (vgl. insbesondere OGH 24.06.2014, 4 Ob 71/14s, SZ 2014/59 uam).

f) Einführung einer „Quick-Freeze“-Regelung (Art. 4 Z 4 des Entwurfs)

27. Die vorgeschlagene Bestimmung würde die grundsätzliche Löschungspflicht der Kommunikationsdiensteanbieter betreffend Verkehrsdaten (§ 99 Abs. 1 TKG 2003) dahingehend modifizieren, dass auf staatsanwaltschaftliche Anordnung hin an die Stelle der Löschungs- eine Speicherpflicht betreffend bestimmte, gemäß StPO bezeichnete, Daten tritt. Eine solche Vorgehensweise wird international verbreitet als „Quick-Freeze“-Verfahren bezeichnet. Auch die Bezeichnung „anlassbedingte Vorratsdatenspeicherung“ wäre passend. Die Bedingungen einer solchen Anordnung wären gleich wie in Art. 135 Abs. 2 Z 2 bis 4 StPO, sie wäre also (ohne Zustimmung des Inhabers der Einrichtung) zulässig zur Aufklärung einer mit Freiheitsstrafe von mehr als einem Jahr bedrohten Straftat, oder 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.

28. Zunächst möchte die Datenschutzbehörde darauf hinweisen, dass nicht klar ist, inwieweit durch den vorgeschlagenen Abs. 1c (Mitwirkung der Datenschutzbehörde bei der Überprüfung der Protokolldaten der Übermittlung von „Quick-Freeze“-Daten) eine Erhöhung des Datenschutzniveaus erreicht werden kann. Ob die Anordnungen der Staatsanwaltschaft weiterhin gemäß Art. 90a B-VG als Akte der Gerichtsbarkeit der Kontrolle durch die Datenschutzbehörde entzogen bleiben, wird sich erst aus der zukünftigen verbindlichen Auslegung von § 31 Abs. 1 2. Satz DSG iVm Art. 45 Abs. 2 der Richtlinie 2016/6807EU ergeben. Es scheint sich bei der Bestimmung vielmehr um eine Regelung ähnlich jener

der Datensicherheitsverordnung - TKG-DSVO, BGBl. II Nr. 402/2011 idgF, zu handeln, welche mit der Aufhebung der Vorratsdatenspeicherung weitestgehend ihre Anwendbarkeit verloren hat, und die eine auf die Rechtmäßigkeit der Datenverwendung durch zur Speicherung von Verkehrsdaten verpflichtete Kommunikationsdienstleister beschränkte Überprüfung zum Ziel hat.

29. Darüber hinaus wird auf das Urteil des EuGH vom 08.04.2014, C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger ua, sowie das Erkenntnis des VfGH vom 27.06.2014, G 47/2012 ua, VfSlg 19892/2014, hingewiesen. Angesichts insbesondere der niedrig angesetzten Schwelle für „Quick-Freeze“ könnte sich die Regelung aus Sicht der Datenschutzbehörde als verfassungsrechtlich problematisch erweisen.

g) f) <u>Datenverwendung für Zwecke von „Sicherheitsforen“ (Art. 1 Z 2 des Entwurfs)</u>

30. Die vorgeschlagene Bestimmung sieht vor, dass die Sicherheitsbehörde mit vertrauenswürdigen Privatpersonen über „Plattformen“ genannt „Sicherheitsforen“ (zu denken wäre wohl etwa auch an besonders gesicherte Internet-Diskussionsforen) über sicherheitspolizeiliche Maßnahmen diskutiert und zu diesem Zweck auch Informationen – und eventuell auch personenbezogene Daten -, die der Amtsverschwiegenheit unterliegen - übermitteln darf, nämlich wenn diese den Teilnehmer dem Grunde nach bekannt sind oder eine Übermittlung im überwiegenden wesentlichen Interesse Betroffener ist.

31. Die Bestimmung erscheint nach Ansicht der Datenschutzbehörde sehr vage und zu unbestimmt, um eine Übermittlung personenbezogener Daten rechtfertigen zu können. Als Mindesterfordernis wäre jedenfalls vorzusehen, die personenbezogenen Daten, die eventuell zum Zweck der Erörterung mit Bürgerinnen und Bürgern letzteren mitzuteilen oder offenzulegen wären, präzise zu umschreiben. Soweit es um andere Informationen geht, die der Amtsverschwiegenheit unterliegen, kann auch bereits jetzt Art. 21 Abs. 2 und 4 B-VG (Amtsverschwiegenheit und Auskunftspflicht) sinnvoll so zur Anwendung gebracht werden, dass eine Information der und eine Diskussion mit Beteiligten möglich ist.

21. August 2017
Die Leiterin der Datenschutzbehörde:
JELINEK

REPUBLIK ÖSTERREICH DATENSCHUTZBEHÖRDE @ AMTSSIGNATUR	Unterzeichner	serialNumber=1119505,CN=Datenschutzbehörde,C=AT
	Datum/Zeit	2017-08-21T12:40:08+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.dsb.gv.at/-/amtssignatur
	Hinweis	Dieses Dokument wurde amtssigniert.