An das
Bundesministerium für Inneres
Herrengasse 7
A-1010 Wien

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

Wien, am 18. August 2017

BETREFF: ISPA-STELLUNGNAHME ZUM ENTWURF EINES BUNDESGESETZES MIT DEM DAS SICHERHEITSPOLIZEIGESETZ, DAS BUNDESSTRAßEN-MAUTGESETZ 2002, DIE STRAßENVERKEHRSORDNUNG 1960 UND DAS TELEKOMMUNIKATIONSGESETZ 2003 GEÄNDERT WERDEN

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich im Zusammenhang mit der öffentlichen Konsultation des Bundesministeriums für Inneres zum Entwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden wie folgt Stellung zu nehmen:

Die ISPA möchte anmerken, dass die vorgesehene Regelung zu Verkehrsmanagmentmaßnahmen an die Vorgaben der Telekom-Single-Market Verordnung angepasst werden muss, damit diese für die Betreiber auch anwendbar ist. Zudem steht der Aufwand welcher mit der Registrierung von Prepaid-SIM-Karten verbunden ist keinem entsprechenden Nutzen in der Strafverfolgung gegenüber und führt darüber hinaus zu einem Wettbewerbsrückgang. Eine Registrierung bereits im Umlauf befindlicher Prepaid-SIM-Karten wird von der ISPA abgelehnt. Ferner entspricht nach Ansicht der ISPA das „quick-freeze“ Modell nicht den Vorgaben des Europäischen Gerichtshofs zur Vorratsdatenspeicherung und darf die darin vorgesehene Aufhebung der Löschverpflichtung zu keiner Speicherverpflichtung zusätzlicher Daten führen. Es ist auch fraglich, inwiefern die Strafprozessordnung eine ausreichende Rechtsgrundlage für die vorgesehene staatsanwaltschaftliche Anordnung bietet und wäre zudem der Rechtschutz noch weiter auszubauen. Außerdem wäre die technische Umsetzung mit erheblichem Aufwand für die Betreiber verbunden, der jedenfalls zu ersetzen ist und sind einzelne Bestimmungen zur Auskunftspflicht und Protokollierungspflicht widersprüchlich und erfordern Klarstellung. Die Beauskunftung von Kundendaten an Privatpersonen im Rahmen der Strafverfolgung wird von der ISPA insbesondere aus datenschutzrechtlicher Perspektive klar abgelehnt.

ISPA – Internet Service Providers Austria
Währinger Straße 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675

1) Die vorgesehene Regelung zu Verkehrsmanagmentmaßnahmen muss an die Vorgaben der TSM-VO angepasst werden

Der Gesetzesentwurf sieht die Aufnahme einer neuen Bestimmung in § 17 Abs. 1a TKG vor wonach *„Anbieter von Internetzugangsdiensten Verkehrsmanagmentmaßnahmen im Sinne von Art. 3 der Verordnung (EU) 2015/2120 zur Vermeidung von strafrechtlich relevanten Handlungen, wie* […] *oder strafrechtlich relevanten Urheberrechtsverletzungen anbieten* [können]*".*

Es ist jedoch fraglich inwieweit dies den Bestimmungen zur Netzneutralität in der TSM-VO[1] entspricht. Eine reine Erlaubnis, Verkehrsmanagmentmaßnahmen zu setzen entspricht nicht den Ausnahmefällen in Art. 3 Abs. 3 lit. a TSM-VO. Darin vorgesehen ist, dass der Betreiber solche Maßnahmen nur setzen darf um „*nationalen Rechtsvorschriften zu entsprechen*". In ErwG 13 wird hierzu ferner ausgeführt, es müsse sich um Rechtsvorschriften handeln, welche die Blockierung bestimmter Inhalte, Anwendungen oder Dienste vorschreiben. Der Betreiber muss somit eine Verpflichtung nach einem nationalen Gesetz erfüllen, während in der vorgesehenen Bestimmung lediglich eine Erlaubnis vorhanden ist („*können*").

Aus den Erläuterungen zur Gesetzesnovelle geht zudem hervor, dass Accessprovider durch die neue Bestimmung mit anderen Diensteanbietern, welche beispielsweise Online-Filter zum Kinder- und Jugendschutz anbieten, gleichgestellt werden sollen. Die Formulierung des Gesetzesentwurfs geht jedoch weit darüber hinaus, indem Verkehrsmanagmentmaßnahmen allgemein zur Vermeidung strafrechtlich relevanter Handlungen gesetzt werden dürfen, und die beiden erwähnten Schutzziele nur als demonstrative Beispiele angeführt werden. Es ist fraglich inwiefern eine solch allgemein gehaltene Formulierung den Vorgaben der TSM-VO entspricht, welche eine strenge Auslegung der allgemeinen Ausnahmen für Verkehrsmanagmentmaßnahmen fordert.[2]

Um Rechtsicherheit für den Betreiber zu gewährleisten schlägt die ISPA daher vor, die Bestimmung umzuformulieren und das in den Erläuterungen angegebene Telos, Jugendschutz bzw. Datensicherheit, als explizites Schutzziel in das Gesetz aufzunehmen und den allgemeinen Verweis auf die Vermeidung strafrechtlich relevanter Handlungen zu entfernen.

Betreibern wäre es demnach erlaubt, Verkehrsmanagmentmaßnahmen zu treffen, um explizit diese Schutzziele zu erreichen. Wichtig wäre es jedoch dabei klarzustellen, dass kein Zwang zur Sperre bestimmter Webseiten besteht, sondern hierdurch lediglich eine Möglichkeit zur Erreichung des Schutzziels geschaffen wird. Dies hängt jedoch davon ab, ob die Kundin oder der Kunde dies möchte – dann ist der Betreiber gegen ein entsprechendes Entgelt auch dazu verpflichtet – oder nicht. Somit wird auch dem Grundsatz der Selbstbestimmtheit der Kunden entsprochen.

Die Anführung von „*strafrechtlich relevanten Urheberrechtsverletzungen*" ist nach Ansicht der ISPA in diesem Zusammenhang jedoch jedenfalls unverständlich, da ein Angebot an den Kunden zur Sperre von pornografischen oder gewaltverherrlichendem Material – etwa in Form eines

[1] 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.
[2] ibid. ErwG. 11

entsprechenden Jugendschutz-Filters - zwar naheliegend ist, eine Sperre von urheberrechtsverletzenden Webseiten jedoch kaum von Kunden nachgefragt werden würde. Da der Sinn der Bestimmung in der Erlaubnis eines Angebots von Verkehrsmanagmentmaßnahmen auf Anfrage des Kunden liegt, sollte eine Zugangssperre lediglich auf Aufforderung von Rechteinhabern von der Bestimmung keinesfalls umfasst sein. Darüber hinaus steht eine Sperre von potentiell urheberrechtsverletzenden Webseiten auch nicht im Einklang mit dem in den Erläuterungen angegebenen Ziel, eine nicht zu rechtfertigende Benachteiligung von Accessprovidern gegenüber anderen Diensteanbietern aufzuheben, da solche Dienste – mangels Nachfrage – auch sonst von keinem Unternehmen angeboten werden.

Im Gesetzesentwurf zu § 17 Abs. 1a TKG erscheinen folglich zwei unterschiedliche Aspekte miteinander vermischt zu werden. Zum einen geht es um die Erlaubnis, Kunden Produkte anbieten zu können welche diese auch nachfragen. Zum anderen wird jedoch eine Erlaubnis zur Sperre von urheberrechtsverletzenden Webseiten aufgenommen, für welche in diesem Zusammenhang kein Anwendungsbereich besteht. Für einen Accessprovider bestünde zudem auch nach der vorgesehenen Regelung keine Möglichkeit, auf Aufforderung der Rechteinhaber hin zu sperren, da eine Verkehrsmanagmentmaßnahme bzw. die Sperre einer Webseite nur dann im Sinne der Netzneutralität erlaubt wäre, wenn es sich auch tatsächlich um eine strafrechtlich relevante Urheberrechtsverletzung handelt und somit im Sinne der Rechtsprechung um eine strukturell rechtsverletzende Webseite. Dies zu beurteilen obläge jedoch wiederum dem Accessprovider selbst, sofern dieser sich nicht in Gefahr einer möglichen Haftung gegenüber Dritten begeben möchte. Der Accessprovider wird damit auch nach dieser Bestimmung weiterhin in seiner nicht zu rechtfertigenden Richterrolle belassen, in der er die involvierten (Grund-)Rechte – im Speziellen das Grundrecht auf Eigentum sowie das Recht auf Zugang zu Informationen und das Recht auf freie Meinungsäußerung - gegeneinander abwägen muss.

Die ISPA fordert darum weiterhin die Einrichtung einer Verwaltungsbehörde mit richterlichem Einschlag als Clearingstelle zur Beurteilung von Zugangssperren zu strukturell rechtsverletzenden Webseiten.[3] Hierdurch kann die Rechtssicherheit deutlich verbessert und für die Wahrung aller involvierten Interessen gesorgt werden. Die vorgesehene Bestimmung ist hingegen dazu geeignet, den Prozess zur Einführung einer solchen Schlichtungsstelle zu konterkarieren.

Die ISPA spricht sich daher für eine Adaptierung der Bestimmung zur Anpassung an die Vorgaben der TSM-VO sowie für eine Streichung des Halbsatzes „*oder strafrechtlich relevante Urheberrechtsverletzungen*“ aus.

2) Dem Aufwand einer Prepaid-SIM-Karten Registrierung steht kein konkreter Nutzen entgegen

In zahlreichen Ländern der Welt können Konsumentinnen und Konsumenten Prepaid-SIM-Karten im Einzelhandel, etwa in Supermärkten, Trafiken oder auch Automaten erwerben, ohne sich dabei

[3] Vgl Tschohl: “Studie zum Konzept einer zentralen Clearingstelle zur inhaltlichen Beurteilung von Netzsperren im Zusammenhang mit Verletzungen des Urheberrechts“ (2017); Gutachten des Research Institutes im Auftrag der ISPA

in irgendeiner Form ausweisen zu müssen und mit möglichst wenig bürokratischem Aufwand. Zahlreiche Menschen, speziell aus ärmeren Verhältnissen, schätzen diese einfachere Form um auf mobile Dienste zugreifen zu können, verglichen mit monatlichen Verträgen bei welchen der SIM-Kartenbenutzer verpflichtet wird, seine persönlichen Daten zu registrieren, sowie unter anderem ein Bankkonto anzugeben.

Gleichzeitig bestehen jedoch auch bereits seit geraumer Zeit Bestrebungen nach einer Einführung einer verpflichtenden Registrierung von Prepaid-SIM-Karten. Begründet wird dies, wie auch im nun vorliegenden Gesetzesentwurf, mit sicherheits- und kriminalpolizeilichen Zwecken, speziell der Bekämpfung von Terrorismus.

Zwar ist es zutreffend, dass Kriminelle vornehmlich Prepaid-SIM-Karten benutzen, auch da diese häufig ihre Telefonnummer ändern und ein Gerät oftmals nur für einige wenige Anrufe benutzen. Erhebungen bzw. Vergleiche zwischen Staaten in welchen eine Registrierungspflicht vorgesehen wurde und jenen in welchen keine solche besteht haben jedoch gezeigt, dass kein direkter Zusammenhang zwischen einer solchen Pflicht und einer Zu- oder Abnahme von kriminellen Aktivitäten oder dessen Aufklärung besteht.[4]

Vielmehr zeigen die Ergebnisse aus Ländern, in welchen tatsächlich ein hohes Kriminalitätsproblem besteht, dass es zu keinem konkreten Nutzen für die Strafverfolgungsbehörden geführt hat. Aus diesem Grund wurde etwa in Mexiko die dort 2009 eingeführte Registrierungspflicht bereits drei Jahre später wieder aufgehoben, wie aus dem entsprechenden Aufhebungsantrag der Regierung hervorgeht.[5]

Aus diesem Grund haben auch zuletzt mehrere europäische Länder, darunter das Vereinigte Königreich, Rumänien und die Tschechische Republik von der Einführung einer Registrierungspflicht abgesehen und einen entsprechenden Antrag abgelehnt.[6] Insbesondere im Vereinigten Königreich, welches zuletzt mehrfach unter terroristischen Anschlägen zu leiden hatte, war dieser Schritt bemerkenswert, zeigt jedoch umso mehr, wie wenig Vertrauen selbst bei Sicherheitsexperten gegenüber einer solchen Registrierungspflicht besteht.

Für die mangelnde Eignung einer solchen Maßnahme zur Verbrechensbekämpfung gibt es mehrere Gründe. Zunächst ist es Kriminellen oftmals ein leichtes, sich unter falschem Namen bei der Registrierung auszuweisen, da in den Geschäften welche die Prepaid-SIM-Karten vertreiben zumeist keine Möglichkeit zur authentischen Identifizierung besteht. Die Abfrage eines zentralen Registers durch die Angestellten, etwa des Melderegisters, ist bereits aus Datenschutzgründen nicht zulässig.

Darüber hinaus entstand etwa in Mexiko lediglich ein größerer Schwarzmarkt für Prepaid-SIM-Karten, oftmals aus gestohlenen Mobilfunkgeräten. Dies hatte zur Folge, dass Ermittlungen in vielen Fällen gegen Unschuldige eingeleitet wurden, lediglich da die SIM-Karte noch auf ihren

[4] Vgl *Nicola Jentzsch*: "Implications of Mandatory Registration of Mobile Phone Users in Africa" (2012), http://www.diw.de/documents/publikationen/73/diw_01.c.394079.de/dp1192.pdf (01.08.2017)
[5] http://www.senado.gob.mx/?ver=sp&mn=2&sm=2&id=28925 (01.08.2017)
[6] GSMA White Paper zur Registrierung von Prepaid-Karten, November 2013, https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_WhitePaper_MandatoryRegistrationofPrepaidSIM-Users.pdf (01.08.2017)

Namen registriert war und sie es etwa verabsäumt hatten diese als gestohlen zu melden. Dadurch wurden Ermittlungen nicht nur nicht gefördert, sondern sogar verlangsamt.

Darüber hinaus hätte die verpflichtende Registrierung jedoch auch negative Folgen speziell für sozial benachteiligte Gesellschaftsschichten wie etwa Personen deren monatliches Budget keinen Vertragsabschluss zulässt oder etwa für Migrantinnen und Migranten, welche nach einer erfolgten Flucht über keine ausreichenden Ausweisepapiere verfügen jedoch trotzdem eine Möglichkeit zur Kontaktaufnahme mit ihrer Heimat oder auch Hilfsorganisationen benötigen, ebenso auch für Obdachlose ohne Ausweispapiere.

Nicht zuletzt entsteht auch für den Mobilfunkanbieter selbst ein enormer Aufwand, da von diesem die registrierten Daten aufzunehmen, zuzuordnen und aufzubewahren sind, wofür ein hoher personeller und finanzieller Aufwand notwendig ist. Darunter fällt etwa die Schulung des Personals im Einzelhandel wie eine korrekte Registrierung abzulaufen hat, welche die akzeptablen Identitätsnachweise sind bzw. wie diese zu überprüfen sind. Daneben haben Mobilfunkbetreiber hohe Investitionen in öffentliche Sensibilisierungskampagnen zu investieren, um ihre Kunden über die Notwendigkeit der Registrierung zu informieren. Außerdem entstehen laufende Kosten hinsichtlich der Wartung der Kundendatenbank sowie der Überwachung des Systems und der Deaktivierung unregistrierter SIM-Karten. Für all diese Kosten muss der Mobilfunkbetreiber gemäß dem Entwurf alleine aufkommen um erneut bei der Erfüllung staatlicher Schutzpflichten mitzuwirken. Mobilfunkbetreiber kommen dieser Verpflichtung bereits jetzt in weitaus größerem Ausmaß nach als jegliche anderen Unternehmen, trotzdem ist erneut kein Kostenersatz vorgesehen. Die ISPA fordert daher deutlich – wie dies auch in der Rechtsprechung des Verfassungsgerichtshofs gefestigt ist – einen Kostenersatz für die zusätzlichen Aufwände, zumindest jedoch 80 % des personellen und finanziellen Aufwands.

Es folgt aus den Ausführungen, dass einer verpflichtenden Registrierung von Prepaid-SIM-Karten kein konkreter Nutzen für die Strafverfolgung gegenübersteht, jedoch zum Teil immense sozialpolitische Nachteile entstehen. Angesichts dieser Abwägung sowie auch mit Verweis auf die Erfahrungen in anderen Staaten sollte in Österreich nach Ansicht der ISPA daher von der Einführung einer solchen Bestimmung abgesehen werden.

3) Keine Registrierungspflicht von bereits erworbenen Prepaid-SIM-Karten

Nach dem Wortlaut des Entwurfs zu § 97 Abs. 1a TKG sollen die erforderlichen Stammdaten des Teilnehmers bei Vertragsabschluss mit einem Anbieter von oder für diesen (etwa durch Angestellte des Supermarkts) registriert werden, um eine nachträgliche Identifizierung durch Strafverfolgungsbehörden zu ermöglichen. Gemäß den Erläuterungen ist „Vertragsabschluss“ jedoch offensichtlich äußerst weit auszulegen und erfasst nicht nur den Erwerb der Prepaid-SIM-Karte, sondern zudem auch jeglichen Erwerb von entsprechendem Guthaben.

Daraus folgt, dass auch alle bereits erworbenen Prepaid-SIM-Karten, sobald das Guthaben aufgebraucht ist, registriert werden müssen. Hierdurch wird der bereits für die verpflichtende Registrierung bei Erwerb der SIM-Karte entstehende Aufwand weiter erhöht. Aktuell beläuft sich

die Anzahl der im Umlauf befindlichen Prepaid-SIM-Karten auf über fünf Millionen, welche nach Ende der Gültigkeit des Guthabens ebenfalls neu registriert werden müssten. Der dabei entstehende Aufwand müsste allein von den Mobilfunkanbietern getragen werden, welche hierzu jedoch nicht über ausreichend Kapazitäten verfügen.

Die ISPA spricht sich daher – unter Aufrechterhaltung der generellen Ablehnung der Registrierungspflicht mangels praktischem Nutzen - klar gegen die Registrierung bereits erworbener Prepaid-SIM-Karten aus.

4) Die Prepaid-SIM-Karten Registrierung führt zu einem Wettbewerbsrückgang

In den vergangenen Jahren ist die Anzahl der Kundinnen und Kunden mit Prepaid-SIM-Karten kontinuierlich gestiegen, innerhalb der vergangenen zwei Jahre um über 30 %[7], während die Anzahl der Postpaid-SIM-Karten stagnierte. Aktuell befinden sich über fünf Millionen Prepaid-SIM-Karten im Umlauf. Speziell MVNOs (Mobile Virtual Network Operators) setzen in ihrem Geschäftsmodell auf die Verwendung von Prepaid-SIM-Karten und haben damit seit ihrem Markteintritt in den vergangenen Jahren den Mobilfunkmarkt deutlich belebt und verfügen mittlerweile über Marktanteile in Höhe von knapp 5 %. Der Vertrieb ihrer Produkte erfolgt dabei hauptsächlich über den Einzelhandel, speziell in Supermärkten. Hierdurch zeigt sich die Nachfrage der Kundinnen und Kunden nach einem einfachen, unbürokratischen Zugang zu Mobilfunk- und Internetdiensten.

Die nunmehr vorgesehene Registrierungsverpflichtung würde jedoch dazu führen, dass Prepaid-SIM-Karten in Hinkunft in weniger Geschäften verfügbar wären, da es an entsprechend geschultem Personal mangelt und dieses für die Supermärkte auch nicht rentabel wäre. Andererseits verfügen speziell MVNOs nicht über ausreichend eigene Infrastruktur um selbst die Registrierung anzubieten. Letztendlich könnte die verpflichtende Registrierung von Prepaid-SIM-Karten damit das Ende für deren Verkauf im Einzelhandel bedeuten. Dies würde einerseits der Nachfrage der Kundinnen und Kunden und damit der Marktentwicklung entgegenlaufen, andererseits wären MVNOs unverhältnismäßig stark betroffen, die erst kürzlich den Wettbewerb belebt haben und nun quasi wieder vom Markt verdrängt werden würden.

Eine solche Entwicklung ist weder im Interesse der österreichischen Wirtschaft, noch im Interesse der Kundinnen und Kunden, welche bei einem starken Wettbewerb von günstigen Preisen profitieren.

5) Das vorgesehene „quick - freeze“ Modell entspricht nicht der Rechtsprechung des Europäischen Gerichtshofs

Einleitend möchte die ISPA positiv anmerken, dass der Gesetzgeber auf die bisherige Rechtsprechung zur Vorratsdatenspeicherung und damit auf die auch von der ISPA in der

[7] RTR Monitor 1/2017

Vergangenheit vorgebrachten Argumente eingeht und diese auch zum Teil berücksichtigt. Dies äußert sich etwa in der vorgesehenen strikten Protokollierungspflicht sowie im verpflichtenden Datentransfer über die Durchlaufstelle (DLS). Jedoch entspricht der vorgelegte Entwurf in einigen Bereichen nicht den Vorgaben zur Vorratsdatenspeicherung, welche der EuGH in zwei Grundsatzurteilen[8] festgesetzt hat:

a) Die Vorratsdatenspeicherung ist ausschließlich zur Bekämpfung schwerer Kriminalität zulässig

Zunächst stellt nach Ansicht des EuGHs allein die Bekämpfung der schweren Kriminalität als Ausformung des Schutzes der öffentlichen Sicherheit ein legitimes Eingriffsziel dar, welches eine solche Maßnahme, die einen massiven Eingriff in das Recht auf Privatsphäre, den Schutz personenbezogener Daten sowie das Recht auf freie Meinungsäußerung (Art. 7, 8 und 11 GRC) bedeutet, rechtfertigt.[9]

Eine Definition von schwerer Kriminalität bzw. Straftat existiert weder in der Rechtsprechung des EuGHs – der dies den nationalen Gesetzen überlässt - noch in der österreichischen Rechtsordnung. Angesichts der Wortwahl des EuGHs muss es sich hierbei jedoch um solches Verhalten handeln, dessen Unwert sich gerade dadurch äußert, dass dieser gegenüber anderen Straftaten als „schwer“ einzustufen ist. Somit muss es sich um jene Straftaten handeln, deren Strafrahmen am oberen Ende angesiedelt ist.

Naheliegend wäre daher zum einen ein Rückgriff auf die Unterscheidung zwischen Vergehen und Verbrechen im österreichischen Strafrecht, wonach ein Verbrechen gemäß § 17 Abs. 1 StGB eine vorsätzliche Handlung ist, die mit lebenslanger oder mit mehr als dreijähriger Freiheitsstrafe bedroht ist. Daneben besteht auch die Möglichkeit, die Bestimmungen zur Gerichtszuständigkeit im Strafprozess heranzuziehen und eine Straftat ab Zuständigkeit des Landesgerichts als Schöffengericht als schwer zu qualifizieren.

Grundsätzlich wäre auch der Verweis auf einen Strafrahmen ab drei Jahren Freiheitstrafe denkbar. Hierfür spräche, dass ausgenommen der „schweren Sachbeschädigung“, sämtliche der als „schwer“ qualifizierten Grunddelikte (etwa „Schwerer Diebstahl“, „Schwerer Betrug“, „schwere Nötigung“, „schwere Körperverletzung“…) bei einem Strafrahmen von zumindest drei Jahren ansetzen.

Aufgrund des Verweises auf § 135 Abs. 2 Z 2 bis 4 StPO wäre nach der vorgesehenen Rechtslage eine entsprechende Anordnung zur Vorratsdatenspeicherung jedoch bereits zur Ermittlung, Feststellung und Verfolgung von Straftaten zulässig, deren Strafrahmen ein Jahr übersteigt, im Fall der Zustimmung des Betroffenen sogar bei Delikten mit einer Höchststrafe von sechs Monaten. Diese niedrig angesetzte Zulässigkeitsschranke kann in keinem Fall der Rechtsprechung des EuGHs entsprechen und muss daher in jedem Fall angehoben werden.

[8] EuGH 16.5.2014, C-293/12, *Digital Rights Ireland*; EuGH 21.12.2016, C 203/15 *Tele2 Sverige*
[9] EuGH 16.5.2014, C-293/12, *Digital Rights Ireland* Rz 60, EuGH 21.12.2016, C 203/15 *Tele2 Sverige* Rz 102

b) Die gespeicherten Daten müssen auf das absolut Notwendigste beschränkt werden

Der EuGH verweist jedoch auch darauf, dass selbst die Bekämpfung schwerer Kriminalität für sich genommen die Erforderlichkeit einer Vorratsdatenspeicherung nicht alleine zu rechtfertigen vermag, sondern auch in diesem Fall Schutzmechanismen, die eine Limitierung der Daten auf das Notwendigste gewährleisten, vorzusehen sind.[10]

Als Grundvoraussetzung für eine rechtmäßige Bestimmung zur Vorratsdatenspeicherung, sieht der EuGH daher klare und präzise, objektive Zulässigkeitskriterien vor. Dabei ist jeweils der Bezug der gespeicherten Daten zum Schutz der öffentlichen Sicherheit wiederzugeben um sicherzustellen, dass die Vorratsdatenspeicherung hinsichtlich der Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer auf das zur Erreichung dieses Ziels absolut Notwendigste beschränkt wird.[11] Solche klaren und präzisen Zulässigkeitsvoraussetzungen fehlen jedoch in der vorgesehenen Bestimmung.

Der Formulierung wonach die Speicherung zulässig sei *„zur Ermittlung, Feststellung und Verfolgung von Straftaten*, *deren Schwere eine Anordnung nach § 135 Abs. 2 Z 2 bis 4 StPO rechtfertigt“* ist die Gefahr immanent, dass eine umfangreiche Speicheranordnung ergeht, welche in überschießendem Ausmaß Kundendaten erfasst welche zur Bekämpfung schwerer Kriminalität nicht notwendig wären. Es wäre darum zwingend notwendig objektive Kriterien festzusetzen, anhand derer der obligatorische Zusammenhang festgestellt werden kann. Speziell dass bereits die Speicherung zur „Feststellung und Ermittlung“ von Straftaten angeordnet werden kann ist überaus bedenklich, da hierbei noch kein konkreter Beschuldigter vorliegen muss, sondern die Maßnahme pro-forma bei einem Anfangsverdacht, dass eine Straftat begangen werde, angeordnet werden kann, um den potentiellen Beschuldigen anschließend ausfindig zu machen. Auf diese Möglichkeit wird auch in den Erläuterungen explizit verwiesen.

Damit würde beispielsweise die Anordnung zur Speicherung aller Verkehrsdaten von Nutzerinnen und Nutzern an einem bestimmten geographischen Standort bzw. innerhalb einer Funkzelle ermöglicht werden, wenn der Verdacht besteht, dass an diesem Ort eine gerichtlich strafbare Handlung mit einem Strafrahmen von über einem Jahr begangen werde. Dies hätte zur Folge, dass etwa alle Verkehrsdaten von Besucherinnen und Besuchern einer Demonstration, einer religiösen Einrichtung oder einer Großveranstaltung gespeichert werden müssten. Eine solche Anordnung widerspricht klar den Vorgaben des EuGHs nach objektiven Anknüpfungspunkten, die es ermöglichen Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern.[12]

Neben der mangelnden Einschränkung in Bezug auf die betroffenen Personen ist die Bestimmung auch in zeitlicher Hinsicht überschießend, indem Daten auf staatsanwaltschaftliche Anordnung für bis zu 12 Monate gespeichert werden müssen. Sofern Daten zum Zeitpunkt der Anordnung bereits

[10] EuGH 16.5.2014, C-293/12, *Digital Rights Ireland* Rz 51, EuGH 21.12.2016, C 203/15 *Tele2 Sverige* Rz 103
[11] EuGH 21.12.2016, C 203/15 *Tele2 Sverige* Rz 108, 110
[12] Ibid. Rz 111

für Verrechnungszwecke aufbewahrt wurden, kann sich damit – je nach Auslegung der Gesetzesbestimmung[13] - eine Speicherdauer von über einem Jahr ergeben. Damit sieht die Bestimmung eine mehr als doppelt so lange Speicherdauer vor als jene nach der aufgehobenen Vorratsdatenspeicherung in Österreich. Auch eine solche Vorgabe ist ohne Angabe weiterer Kriterien um die maximal zulässige Speicherdauer zu bestimmen überschießend und unverhältnismäßig.

Hieraus folgt, dass die vorgesehene Bestimmung zur Einführung von „quick-freeze“ in keiner Weise den Vorgaben des EuGHs zu einer angemessenen Vorratsdatenspeicherung entspricht, weder hinsichtlich der Einschränkung auf die Verfolgung schwerer Kriminalität, noch hinsichtlich der objektiven Kriterien welche eine Limitierung der Daten auf das absolut Notwendigste gewährleisten sollen. Die ISPA spricht sich daher grundsätzlich gegen eine Aufnahme der Bestimmung aus, fordert jedoch bei dessen Beibehaltung jedenfalls eine Adaptierung, um den Anforderungen der EuGH Rechtsprechung zu entsprechen. Andernfalls riskiert man wiederum ein zeit- und kostenaufwändiges Verfahren vor dem Verfassungsgerichtshof und in letzter Instanz möglicherweise wieder vor dem EuGH, welches am Ende zur Aufhebung der Bestimmung führt.

6) Die Anordnung, bestimmte Daten nicht zu löschen darf zu keiner Speicherverpflichtung zusätzlicher Daten führen

Der Gesetzesentwurf lässt es in seiner aktuellen Form völlig offen, welche Daten die Staatsanwaltschaft von der Löschungsverpflichtung ausnehmen kann. Aus dem Wortlaut der Bestimmung folgt lediglich, dass jene Daten die in einer staatsanwaltschaftlichen Anordnung angeführt werden von der grundsätzlichen Löschpflicht nach § 99 Abs. 1 TKG ausgenommen sind. Nach letzterer Bestimmung dürfen Verkehrsdaten „*außer in den in diesem Gesetz geregelten Fällen nicht gespeichert oder übermittelt werden und sind vom Anbieter nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren*“. Bislang bestand eine entsprechende Ausnahme gemäß Abs. 2 u. 3 leg. cit. generell nur für solche Verkehrsdaten, die zur Verrechnung von Endkunden- oder Vorleistungsentgelten erforderlich sind für maximal drei Monate, sowie im Einzelfall zur Behebung von Störungen, bei Kundenanfragen, zur Betrugsermittlung oder zur Vermarktung der Kommunikationsdienste sowie für die Bereitstellung von Diensten mit Zusatznutzen. Da sich die Geschäftsmodelle der einzelnen Betreiber zum Teil stark unterscheiden, wurden demnach auch Verkehrsdaten bislang in unterschiedlichem Ausmaß gespeichert.

Da sich § 99 Abs. 1a jedoch augenscheinlich auf die generelle Löschverpflichtung sämtlicher Verkehrsdaten und nicht auf die gemäß den bisherigen Ausnahmeregelungen gespeicherten Daten bezieht, liegt der Schluss nahe, dass der Gesetzgeber offenbar eine Anordnung zur Speicherung sämtlicher Verkehrsdaten nach Beendigung der Verbindung vorsehen möchte, unabhängig davon ob diese bislang als Betriebsdaten gespeichert wurden oder nicht.

Eine solche Auslegung wird von der ISPA in jedem Fall abgelehnt und sich gegen jegliche Speicherverpflichtung zusätzlicher Daten ausgesprochen. Dies gilt insbesondere hinsichtlich jener

[13] Vgl hierzu Punkt 8

Daten welche aktuell nur zwischengespeichert werden da es hierzu zudem an der notwendigen Infrastruktur fehlt. Eine Beauskunftung sowie eine Übermittlung dieser Daten als „Comma-separated Value (CSV)"-Datei über die Durchlaufstelle wäre für diese Daten derzeit auch nicht möglich, da dies technisch nicht implementiert ist.

Aus diesem Grund wäre nach Ansicht der ISPA § 99 Abs. 1a zu adaptieren um klarzustellen, dass die Anordnung der Staatsanwaltschaft sich jedenfalls nur auf solche Daten beziehen kann, welche der Betreiber bereits bisher als Betriebsdaten aufbewahrt, es somit ausschließlich zu einer Verlängerung bereits bestehender Speicherfristen und zu keiner Etablierung neuer Speicherverpflichtungen kommt. Dies entspricht auch den Vorgaben des EuGHs nach einer Limitierung der Daten auf das für die Bekämpfung schwerer Kriminalität absolut Notwendigste.

Dabei ist zudem hinsichtlich der Anwendung von CGN-Technologie festzuschreiben, dass von der Speicherverpflichtung in keinem Fall die Speicherung der intern vergebenen Portnummern erfasst wäre. Diese Ausnahme war zwar in den Erläuterungen zur Vorratsdatenspeicherung klar definiert, da § 102a TKG mittlerweile jedoch aufgehoben wurde, wäre die neuerliche Aufnahme entsprechender Ausführungen jedenfalls notwendig.[14]

Zudem ist im Sinne der Rechtssicherheit auch eine Anpassung der Datensicherheitsverordnung (TKG-DSVO) sowie der Technischen Richtlinie zur CSV-Datei für die Beantwortung von Auskunftsbegehren gemäß § 94 Abs. 4 TKG 2003 vorzunehmen.

Gerade kleine und mittelgroße Betreiber verfügen außerdem nicht über die notwendigen Kapazitäten, den vorgegebenen Speicherverpflichtungen in der Praxis nachzukommen. Aufgrund dessen sahen bereits die aufgehobenen Bestimmungen zur Vorratsdatenspeicherung eine Ausnahme für KMUs vor und sollte diese auch nun übernommen werden.

7) Die einzelnen Bestimmungen zur Auskunftspflicht und Protokollierungspflicht (§ 99 Abs. 1b – 1e) sind widersprüchlich und erfordern Klarstellung

Gemäß § 99 Abs. 1b TKG des Gesetzesentwurfs, darf eine Auskunft über nach Abs. 1a leg. cit. gespeicherte Daten ausschließlich nach gerichtlicher Bewilligung der staatsanwaltschaftlichen Anordnung erfolgen. Bei Verletzung dieser Vorgabe ist nach § 109 Abs. 4 Z 11 TKG eine Verwaltungsstrafe von bis zu EUR 58,000 vorgesehen.

§ 99 Abs. 1e sieht jedoch die Übermittlung der Protokolldaten, welche gemäß Abs. 1c leg cit. auch Name und Anschrift des von der Auskunft betroffenen Teilnehmer umfassen, bereits auf schriftliche Anfrage an die Datenschutzbehörde vor. Es erscheint zweifelhaft ob es tatsächlich im Sinne des Gesetzgebers ist, dass Anordnungen der Staatsanwaltschaft einer gerichtlichen Bewilligung bedürfen, Anfragen der Datenschutzbehörde hingegen nicht. Eine entsprechende Klarstellung durch den Gesetzgeber ist nach Ansicht der ISPA daher zwingend erforderlich.

[14] Vgl. Erläuterungen zu § 102a Abs. 2 Z1 TKG

Ebenso verweist § 99 Abs. 1d TKG auf das Auskunftsrecht des Betroffenen nach allgemeinen datenschutzrechtlichen Bestimmungen[15] wonach diesem die verarbeiteten Daten, die Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, der Zweck der Datenverwendung sowie die Rechtsgrundlagen zu beauskunften sind. Die im Rahmen des Datenschutz-Anpassungsgesetzes 2018 neu aufgenommenen Bestimmungen zur Datenverarbeitung im Rahmen der Strafverfolgung sehen dabei für den Fall, dass durch eine solche Beauskunftung Ermittlungsergebnisse gefährdet werden können, die Möglichkeit zur Verweigerung bzw. Einschränkung der Auskunft vor.[16] Zwar bezieht sich dies in diesem Fall auf die Auskunftsverpflichtung der Strafbehörden gegenüber dem Betroffenen, jedoch wäre ein entsprechendes Recht zur Einschränkung bzw. Verweigerung der Auskunft auch für den Betreiber in § 99 Abs. 1d TKG aufzunehmen, da ein darauf basierendes Auskunftsrecht des unter (Anlass)Verdacht stehenden Kunden den Zweck der Bestimmung des § 44 Abs 2 DSAG 2018 andernfalls geradezu konterkarieren würde. Auch hier ist daher nach Ansicht der ISPA eine Klarstellung bzw. Ergänzung durch den Gesetzgeber notwendig.

8) Es ist fraglich ob in der Strafprozessordnung eine ausreichende Rechtsgrundlage für eine Anordnung nach § 99 Abs. 1a existiert

Die Charakteristik der Mitwirkung von Betreibern im Rahmen der Strafverfolgung ist, dass diese jeweils auf einer Rechtsgrundlage im Telekommunikationsgesetz (als Rechtsgrundlage für die Tätigkeit der Betreiber) sowie auch in der Strafprozessordnung (als Rechtsgrundlage für die Befugnisse der Staatsanwaltschaft) fußt.

Das nunmehr vorgesehene „quick-freeze“ Modell wird durch den Gesetzgeber im Rahmen der Novelle jedoch ausschließlich im Telekommunikationsgesetz festgesetzt. Dabei bezieht sich der Gesetzgeber in § 99 Abs. 1a TKG auf eine „staatsanwaltschaftliche Anordnung gemäß den Bestimmungen der StPO“ ohne dabei die entsprechende Rechtsgrundlage einer solchen Anordnung oder deren Formvorschriften näher zu spezifizieren. Lediglich in Abs. 1b leg cit. verweist der Gesetzgeber auf eine konkrete Anordnung nach der StPO (§ 135 Abs. 2 Z 2 bis 4), dabei jedoch ausschließlich um den Strafrahmen der Anwendungsfälle von quick-freeze zu umschreiben. In der StPO selbst wiederum existiert keine Rechtsnorm, welche als Grundlage für eine Anordnung gemäß Abs. 1a dienen könnte. Insbesondere eine Anordnung zur Auskunft über Daten einer Nachrichtenübermittlung iSd § 134 Z 2, 138 Abs. 1 StPO bezieht sich ausschließlich auf Zugang zu den bereits aufbewahrten Daten gemäß Abs. 1b leg cit., nicht jedoch auf die ursprüngliche Verlängerung der Speicherdauer.

Die ISPA möchte daher anmerken, dass mangels entsprechender Rechtsgrundlage in der StPO es fraglich ist, inwiefern eine solche Anordnung an einen Betreiber zulässig wäre und dieser – trotz der Rechtsgrundlage im TKG - nachgekommen werden dürfte. Sofern sich der Gesetzgeber folglich dazu entschließt tatsächlich – und entgegen der vorgebrachten Bedenken - eine ähnliche Bestimmung aufzunehmen, sollte daher in jedem Fall eine Rechtsgrundlage für eine Anordnung

[15] § 26 DSG 2000 bzw. nach dessen Außer-Krafttreten ab 25. Mai 2018 Art 15 DSGVO
[16] § 44 Abs. 2 DSAG 2018

der Staatsanwaltschaft auf Aufhebung der Löschpflicht iSd § 99 Abs. 1a in der Strafprozessordnung geschaffen werden.

Zudem wird in Abs. 1a leg cit. festgelegt, dass in der Anordnung der Zeitpunkt bestimmt werden kann ab dem die Löschpflicht nicht mehr besteht, der Betreiber also aus dem Umkehrschluss der vorgesehenen Strafbestimmung in § 109 Abs. 4 Z 9 TKG heraus zur weiteren Aufbewahrung verpflichtet ist. Es ist dabei jedoch unklar, ob sich das Löschverbot ausschließlich auf die ab diesem Zeitpunkt anfallenden Daten beziehen darf, oder auch auf die bereits zu diesem Zeitpunkt als Betriebsdaten aufbewahrten Daten, eine entsprechende Klarstellung wäre nachzuholen. Zudem ist unklar, ob eine Anordnung auch verlängert werden könnte, oder die Daten jedenfalls nach zwölf Monaten zu löschen wären.

9) Der vorgesehene Rechtschutz soll ausgebaut werden

Wie bereits dargelegt ist die vorgesehene „quick-freeze“ - Maßnahme dazu geeignet, empfindlich in die Grundrechte zahlreicher Unbeteiligter einzugreifen, ohne dass diese zunächst darüber informiert sind. In solchen sensiblen Materien obliegt dem Rechtschutzbeauftragten des BMJ gemäß § 147 StPO die Prüfung und Kontrolle solcher Ermittlungsmaßnahmen. Aufgrund der mangelnden Rechtsgrundlage für eine staatsanwaltschaftliche Anordnung nach Abs. 1a ist jedoch unklar ob auch diese der Kontrolle des Rsb unterliegt, die ISPA spricht sich in jedem Fall dafür aus, speziell um den nach aktuellem Gesetzesentwurf drohenden ausufernden Speicheranordnungen entgegenzuwirken.

Zudem wäre nach Ansicht der ISPA auch eine Novellierung des § 147 StPO notwendig, mit der die Rechte des Rsb ausgeweitet werden, um eine effektive Kontrolle sowohl der Anordnung als auch der Durchführung der Maßnahme zu ermöglichen. Hierzu wäre insbesondere der Zugang zu den Protokolldaten gemäß § 99 Abs. 1c des Gesetzesentwurfs vorzusehen. Die im Entwurf vorgesehene Übermittlung der Protokolldaten lediglich an die Datenschutzbehörde ist nicht ausreichend um den Rechtschutz zu gewährleisten.

10) Die technische Umsetzung des „quick-freeze“ Modells erfordert einen enormen Aufwand der zu ersetzen ist

Die vorgesehene Bestimmung würde Accessprovider zur Speicherung von weitaus mehr Daten als bisher verpflichten, da bislang grundsätzliche alle Verkehrsdaten spätestens nach drei Monaten – außer bei Zahlungseinspruch – gelöscht werden. Hierzu sind nicht nur zusätzliche Speicherkapazitäten, sondern insbesondere auch ein hoher personeller Aufwand von Nöten.

Speziell der bereits unter Punkt 4. ausgeführten Fall, wonach die Speicherung von Daten aller Nutzerinnen und Nutzer innerhalb einer (oder mehrerer) Funkzellen angeordnet wird, würde die Betreiber vor große Probleme stellen, da schlagartig enorme Speicherkapazitäten verfügbar sein müssten und zudem auch die Daten entsprechend zugeordnet und abgelegt werden müssten.

Daneben ist es für Betreiber in der Praxis technisch schwierig umsetzbar, bei einzelnen Daten die Löschpflicht auszuschalten während die grundsätzliche automatische Löschung der Daten nach spätestens drei Monaten weiterhin besteht.

Die ISPA fordert daher – unter Aufrechterhaltung der grundsätzlichen Ablehnung der Ausweitung der Überwachung gemäß den obigen Erläuterungen – für jedweden zusätzlichen Aufwand, der Betreibern hierbei im Zuge der Erfüllung einer staatlichen Aufgabe entsteht, einen vollständigen Kostenersatz vorzusehen, zumindest jedoch 80 % des personellen und finanziellen Aufwands gemäß geltender Rechtslage nach dem TKG sowie der Rechtsprechung des Verfassungsgerichtshofs[17]. Eine Überwälzung der gesamten Kosten zur Einrichtung bzw. Adaptierung der Schnittstellen auf den Betreiber, welcher hier lediglich seine Mitwirkungspflicht an einer staatlichen Aufgabe erfüllt und in keinster Weise selbst profitiert, wäre jedenfalls klar unverhältnismäßig.

Nach Ansicht der ISPA ist daher sowohl die Aufnahme einer Bestimmung zum Ersatz der laufenden Personal- und Sachaufwendungen in der Überwachungskostenverordnung (ÜKVO) sowie auch zum Ersatz der Investitionskosten in der Investitionskostenverordnung (IKVO) zwingend notwendig.

11) Die Beauskunftung von persönlichen Daten an Privatpersonen im Rahmen der Strafverfolgung wird abgelehnt

Gestützt auf das Projekt „*Gemeinsam.Sicher*“ des BMI, sieht der Gesetzesentwurf in einer Novellierung des § 57 Abs.1 SPG vor, dass in Hinkunft Sicherheitsbehörden personenbezogene Daten an sogenannte „*Teilnehmer von Sicherheitsforen*“ iSd § 25 Abs. 1 SPG sowie an „*Menschen, die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken und wesentlich zur Gefahrenminderung beitragen*“ iSd § 26, der die allgemeine Streitschlichtung behandelt, übermitteln dürfen.

Die ISPA steht grundsätzlich einer Auslagerung sicherheitspolizeilicher Aufgaben an Privatpersonen äußerst kritisch gegenüber, da hierdurch das staatliche Gewaltmonopol untergraben wird.

Insbesondere wäre gemäß § 25 SPG die Heranziehung von Sicherheitsforen nicht nur zur Abwehr gefährlicher Angriffe auf Leib und Leben vorgesehen, sondern auch zur Abwehr von Angriffen auf das Vermögen. Hierdurch wird der Anwendungsbereich immens ausgeweitet und erlaubt die Übermittlung personenbezogener Daten an Teilnehmer der Sicherheitsforen bereits bei drohenden Sachbeschädigungen, etwa im Rahmen von größeren Veranstaltungen.

Die Definition von „Sicherheitsforen“ ist darüber hinaus äußerst unbestimmt, da gemäß dem Gesetzeswortlaut davon sämtliche Menschen „*die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken*“ umfasst sein können. Gemäß den Erläuterungen zählen hierzu unter anderem private Vereine, NGOs, Wohnpartner oder auch Menschen die im Rahmen von sogenannten

[17] Verfassungsgerichtshof, 27.02.2003, G 37/02 ua, V 42/02

„Community Policing Projekten“ an der Präventionsarbeit teilnehmen. Dies lässt keinen Überblick über die tatsächlich berechtigten Personen zu. Es wäre darum bei Beibehaltung dieser Bestimmung zwingend eine Legaldefinition aufzunehmen, welche den Begriff „Sicherheitsforum“ klar absteckt und einschränkt.

Ferner ist die Verarbeitung personenbezogener Daten im Rahmen der Strafverfolgung im neuen Datenschutzgesetz in dessen 3. Hauptstück gesondert geregelt. Davon erfasst ist zum einen die Verarbeitung durch staatliche Behörden, zum anderen durch andere Stellen oder Einrichtungen, welchen die Ausübung öffentlicher Gewalt und hoheitliche Befugnisse zur Strafverfolgung übertragen wurden. Die angeführten Sicherheitsforen verfügen jedoch über keine hoheitlichen Befugnisse, sondern sollen lediglich unterstützend in der Prävention und Aufklärung von Straftaten tätig werden. Bei den übertragenen Daten handelt es sich jedoch um die gleichen sensiblen, personenbezogenen Daten dessen Verarbeitung durch das 3. Hauptstück geregelt werden soll. Mangels Anwendbarkeit der Bestimmungen des 3. Hauptstücks auf Sicherheitsforen entstehen somit ungerechtfertigte Rechtschutzlücken für den Betroffenen, da ihm keine dem 3. Hauptstück entsprechenden Rechte gegenüber der Datenverarbeitung durch Sicherheitsforen zur Verfügung stehen.

Darüber hinaus ist der vorgesehene Strafrahmen für einen Verstoß gegen die Verpflichtung zur vertraulichen Behandlung der personenbezogenen Daten überaus niedrig angesetzt. Die entsprechende Verwaltungsübertretung ist in § 84 Abs. 1 vorgesehen, welcher sonst im Wesentlichen Verstöße gegen Betretungsverbote behandelt. Die Aufnahme dieser Verwaltungsübertretung im Rahmen von § 84 ist mangels jeglichen Anknüpfungspunktes oder Gleichwertigkeit mit den darin vorgesehenen Verwaltungsübertretungen unverständlich und nicht nachvollziehbar.

Vergleicht man es etwa mit den entsprechenden Bestimmungen im neuen Datenschutzgesetz, so zeigt sich, dass dieses Strafen von bis zu 50.000 Euro für den Fall einer Verletzung des Datengeheimnisses vorsieht.[18] Diese eklatant unterschiedliche Ahndung desselben Fehlverhaltens widerspricht augenscheinlich dem Gleichheitsgrundsatz und ist auch nicht durch die Mitwirkung der Personen an der Strafverfolgung zu rechtfertigen. Speziell da es sich wie bereits ausgeführt um sensible Daten handelt, ist eine Ahndung für Verletzungen des Datenschutzes entsprechend hoch anzusetzen.

Die in § 84 Abs. 1 Z 8 vorgesehene Verwaltungsübertretung ist sohin eigenständig in einer separaten Bestimmung, der Gliederung des SPG folgend als § 83c, mit einem dem Datenschutz angepassten Strafrahmen festzusetzen. Als Anhaltspunkt sollte hierzu der Strafrahmen nach § 69 Abs. 1 DSG dienen.

[18] § 69 Abs. 1 Z 2 DSG

Für Rückfragen oder weitere Auskünfte stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria

Dr. Maximilian Schubert

Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von über 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.

ISPA – Internet Service Providers Austria
Währinger Straße 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675