Bundesministerium für Inneres
Sektion III - Recht
Herrengasse 7
1070 Wien

Vorab per Mail an bmi-III-1@bmi.gv.at und
begutachtungsverfahren@parlament.gv.at

Ihr Zeichen: BMI-LR1340/0019-III/1/2017 Wien, 18. August 2017

Betreff: Stellungnahme der T-Mobile Austria GmbH zum Begutachtungsentwurf des Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert wird

Sehr geehrte Damen und Herren,

beiliegend übermitteln wir Ihnen die Stellungnahme der T-Mobile Austria GmbH zum Begutachtungsentwurf des Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden.

Wir gehen davon aus, mit den Ausführungen dieser Stellungnahme einen Beitrag zu einer tragbaren gesetzlichen Lösung leisten zu können und stehen auch gerne für ein persönliches Gespräch zur Verfügung.

In diesem Sinne verbleiben wir

mit freundlichen Grüßen,

Mag. Anja Trefbal-Bustori
Vice President Legal, Regulatory & Interception
T-Mobile Austria GmbH

T-Mobile Austria GmbH

Stellungnahme der T-Mobile Austria GmbH zum Begutachtungsentwurf des Telekommunikationsgesetz 2003

Zu den geplanten Änderungen des Telekommunikationsgesetzes erlaubt sich die T-Mobile Austria GmbH wie folgt Stellung zu nehmen:

1. § 97 Abs.1a TKG - Stammdaten – Prepaid Registrierung

Durch diese vorgeschlagene Bestimmung soll erreicht werden, dass es für Teilnehmer künftig nicht mehr möglich sein soll, einen nicht registrierten Anschluss bzw. eine sogenannte anonyme Wertkarte zu verwenden. Durch die unklare Formulierung der Bestimmung werden auch Neuanmeldungen im Postpay-Bereich erfasst.

Wir sprechen uns strikt gegen diese Bestimmung aus - vor allem aus dem Gedanken eines sicherheitsfördernden Aspektes heraus. Das Whitepaper der GSMA (https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_WhitePaper_MandatoryRegistrationofPrepaidSIM-Users.pdf) macht klar, dass durch die Einführung einer verpflichtenden Registrierung von SIM/Prepaid-Karten keine positiven Effekte auf die Verhinderung und Verfolgung auf Straftaten hat. Die in Mexiko 2009 eingeführte obligatorische Registrierung wurde mangels der erwähnten nicht eingetretenen Effekte wieder aufgehoben.

Die Registrierungsverpflichtung bei Vertragsabschluss hätte eindeutige, nachteilige Auswirkungen auf mehrere Vertriebskanäle über die eine solche Verpflichtung schwer, bzw. nicht möglich ist. Exemplarisch sei hier nur der Internetvertrieb, bei dem eine verlässliche Identifizierung nur unter großem Arbeits- und Kostenaufwand möglich wäre, erwähnt. Aber selbst bei solchen hochtechnischen Identifizierungsverfahren würden stets unüberwindbare Zweifel der Datenrichtigkeit bleiben. Auch beim Vertrieb von Prepaid-Karten im klassischen Einzelhandel würde eine solche Verpflichtung nur unter hohem Aufwand realisierbar sein und hohen Sach-

und Personalaufwand verursachen, der letztendlich von den Teilnehmern zu tragen sein wird. Da laut den Erläuterungen zum Begutachtungsentwurf auch der Erwerb von Guthaben von der – hier – Identifizierungsverpflichtung umfasst sein soll, wäre ein solcher Erwerb von Guthaben beispielsweise an Geldautomaten nicht mehr möglich und im Einzelhandel (z.B. in einem Supermarkt oder einer Tankstelle) so gut wie nicht umsetzbar. Ein so massiver Eingriff kann nicht im Sinne des Gesetzgebers liegen.

Die Bestimmung sollte daher dahingehend abgeändert werden, dass hinsichtlich der Registrierungsverpflichtung nicht auf den Verkauf, sondern auf die Aktivierung bzw. Freischaltung des Anschlusses abgestellt wird. Dies würde nachgelagertes Identifikationsverfahren ermöglichen. Ein solches wäre beispielsweise das sogenannte Foto-Ident-Verfahren.

Die Einführung dieser Bestimmung hat das Potential, einen „Secondhand Markt" für registrierte Prepaid-Karten zu schaffen. Die Weitergabe bzw. der Verkauf von solchen registrierten Karten an Dritte kann nicht beschränkt oder unterbunden werden und wird die intendierten Auswirkungen konterkarieren. So wären auch entwendete oder mit gestohlenen Dokumenten (online) registrierte Prepaid-Karten von einem gewissen Wert und es könnte so ein neues Problemfeld geschaffen werden.

Darüber hinaus würde diese Bestimmung Menschen, die sich nicht ausweisen können oder wollen stark benachteiligen. Nicht jeder Teilnehmer der anonym bleiben möchte verfolgt mit seinem Verhalten strafrechtlich relevante Ziele. Auch außereuropäische Touristen wären von der Einführung einer Registrierungsverpflichtung besonders stark betroffen.

Die Formulierung der Bestimmung ist zu allgemein und unklar und lässt einen großen Auslegungsspielraum. Vor allem werden zulässigen Identifizierungsverfahren nicht ausdrücklich normiert.

Da durch die Registrierung von Prepaid-Karten sicherheitspolitische Zwecke verfolgt werden, wären daher auf jeden Fall die für die Einführung notwendigen Sach- und Personalaufwendungen zu ersetzen. Im Übrigen kann zum Kostenersatz und Inkrafttreten der Registrierungsverpflichtung sinngemäß auf die Ausführungen zur Aussetzung der Löschungsverpflichtung hinsichtlich Verkehrsdaten („Quick Freeze") verwiesen werden.

2. §§ 97 Abs. 1a ff Verkehrsdaten / Ausnahme von der Löschungsverpflichtung „Quick Freeze"

Umfang der Daten

Die Bestimmung, dass die Löschungsverpflichtung hinsichtlich der „den Bestimmungen der StPO bezeichneten Daten" durchbrochen wird, ist zu unpräzise formuliert und ermöglicht mehrere Varianten der Auslegung. Es ist nicht eindeutig definiert, welchen Daten für welchen Zeitraum von einer solchen staatsanwaltlichen Anordnung umfasst sein sollen.

Es kann davon ausgegangen werden, dass mit diesem Pauschalverweis auf die StPO Verkehrsdaten iwS (daher Verkehrsdaten ieS, Zugangsdaten (§ 92 Abs. 3 Z 4a TKG) und Standortdaten (§ 92 Abs. 3 Z 6 TKG)) erfasst sein sollen. Dies würde dem Umfang der zu speichernden Daten der Legaldefinition der „Auskunft über Daten einer Nachrichtenübermittlung" in der StPO (§ 134 Z 2 StPO) entsprechen.

Es wäre dem Verständnis und der Rechtssicherheit förderlich, die Bestimmung des Abs. 1a dahingehend abzuändern, dass sie wie folgt lautet: „gemäß der in § 134 Z 2 StPO bezeichneten Daten".

Es ist auch anzumerken, dass durch diese Formulierung nicht nur betriebsnotwendige Daten umfasst sind, sondern alle Verkehrsdaten die in der Regel unverzüglich nach Verarbeitung gelöscht werden (vgl. § 99 Abs. 1 TKG).

Die zu Begutachtung vorgeschlagene Bestimmung lässt viel Raum für Auslegungsspielräume und führt somit fast zwangsläufig zu Auffassungsunterschieden, wie der Umfang der von der Löschungsverpflichtung ausgenommenen Daten zu verstehen ist.

Speicherdauer und Löschungsverpflichtungen

Die durch die staatsanwaltliche Anordnung von der Löschungsverpflichtung ausgenommen Daten dürfen gemäß der Bestimmung für maximal 12 Monate aufbewahrt werden bzw. eine solche Anordnung „für höchstens 12 Monate" erteilt werden. Diese Formulierung wirft eine Vielzahl von Fragen auf.

Es ist unklar, ob dieser zwölfmonatige Zeitraum auch historische (d.h. schon angefallene und somit gespeicherte) Verkehrsdaten mitumfassen kann oder nur zukünftig anfallende erfassen soll.

Wenn man davon ausgeht, dass neben zukünftigen Verkehrsdaten auch historische erfasst sein können, stellt sich die Frage, ob der höchstzulässige zukünftige Zeitraum von 12 Monaten neben den historischen tritt oder von diesem miterfasst ist. Mit anderen Worten: Ist ein historischer Zeitraum von der zwölfmonatigen Maximalspeicherdauer bzw. Ausnahme von der Löschungsverpflichtung abzuziehen oder tritt dieser hinzu? Sollten historische Verkehrsdaten nicht zu diesen 12 Monaten zählen, wäre es somit möglich, dass Verkehrsdaten länger als 12 Monate aufzubewahren sind – eine Ausdehnung der Höchstspeicherdauer von maximal 12 Monaten ist jedoch klar abzulehnen.

In diesem Zusammenhang ist auch unklar, ob Folgeanordnungen zulässig sind. Eine solche Folgeanordnung bzw. Verlängerung würde bedeuten, dass nach Ablauf der höchstzulässigen Vorhaltedauer weitere 12 Monate, unter einer fortlaufender Löschung (rollierende Löschung) der bereits vorgehaltenen Verkehrsdaten die älter alter als 12 Monate sind, von der Löschungsverpflichtung ausgenommen sind (Bespiel: Die Daten sind ab sofort, bis 2020 jeweils 12 Monate vorzuhalten).

Es sollte auch klargestellt werden, dass sich die punktuelle Durchbrechung der Löschungsverpflichtung auf einzelne bestimmte Teilnehmeranschlüsse beziehen muss und für geografgische Örtlichkeiten (im Sinne einer Funkzellenauswertung) eine solche Anordnung nicht möglich ist.

Es ist nicht klar, ob die von der Löschungsverpflichtung ausgenommenen Daten nach dem von der Staatsanwaltschaft bestimmten Zeitraum – der sich aus dem in der Anordnung nach Abs. 1a 1. Satz bestimmten (Start-)Zeitpunkt und der Höchstdauer von 12 Monaten (Endzeitpunkt) – ergibt, oder für den Zeitpunkt der Löschung ein eigenständiger Zeitpunkt bestimmt werden kann (Frist).

Konkret: Müssen die Daten nach dem Ablauf des durch die Anordnung bestimmten Endzeitpunkts (höchstens 12 Monate) sofort gelöscht werden, oder kann für die Löschung der von der Löschungsverpflichtung ausgenommen – und daher gespeicherten - Daten ein viel späterer Zeitpunkt („Frist") vorgesehen werden, beispielsweise 36 Monate.

Um Klarheit zu schaffen wird vorgeschlagen die Bestimmung dahingehend abzuändern, dass sie zu lauten hat:

„Nach Ablauf des in der staatsanwaltschaftlichen Anordnung bestimmten Zeitpunkts der Aussetzung der Löschungsverpflichtung nach Abs. 1, spätestens jedoch gemäß Abs. 1a nach 12 Monaten, sind die von der Löschungsverpflichtung nach Abs. 1a ausgenommen Daten zu löschen."

Durch diese Formulierung ist eindeutig klargestellt, dass die Daten nach Ablauf des von der Staatsanwaltschaft bestimmten Zeitraumes, der insgesamt 12 Monate nicht überschreiten darf, zu löschen sind.

Form der Anordnung

Die formellen sowie inhaltlichen Voraussetzungen der Anordnungen nach § 99 Abs. 1 sollten an jene zur Überwachung von Nachrichten und Auskunft über Daten einer Nachrichtenübermittlung angeglichen werden. Durch die weiter unten vorgeschlagene Ergänzung wird ausdrücklich festgehalten, dass für Anordnungen nach § 99 Abs. 1a dieselben strikten formellen sowie inhaltlichen Voraussetzungen (mit Ausnahme der gerichtlichen Bewilligung) zu erfüllen sind wie für Anordnungen nach §§ 134 ff StPO. Der § 138 Abs. 1 StPO sieht vor, dass Anordnungen grundlegende – zum Teil zur Durchführung bzw. Mitwirkung notwendige – Angaben zu enthalten haben, wie beispielsweise die genaue Bezeichnung des betroffenen Anschlusses (d.h. die Rufnummer) oder den Zeitpunkts des Beginns und Beendigung der angeordneten Maßnahme.

Ebenso sollte klargestellt werden, dass eine Mitwirkungsverpflichtung (§ 138 Abs. 2 StPO) und Geheimhaltungsverpflichtung (§ 138 Abs. 3 StPO) besteht. Ohne einen Verweis auf diese Bestimmungen ist nicht ersichtlich, woraus sich derartige Verpflichtungen für Anordnungen gemäß § 99 Abs. 1a sonst ergeben sollten.

Die Bestimmung sollte daher wie folgt ergänzt werden:
„Eine derartige Anordnung hat schriftlich zu erfolgen und den Anforderungen des § 138 Abs. 1 bis 3 StPO zu entsprechen und kann höchstens für 12 Monate erteilt werden."

Durch diese Formulierung wäre eindeutig klargestellt welche formellen und inhaltlichen Mindestvoraussetzungen einzuhalten sind.

Ohne Klärung der offenen Fragen kann eine Planung des notwendigen, separaten und hochsicheren Einzeldatenhaltungssystems nicht geplant und eine Bestellung in Auftrag gegeben werden – eine Implementierung ist bis zum Inkrafttreten der Bestimmung daher nicht möglich (siehe auch weiter unten zum Inkrafttreten).

Insgesamt ist die Bestimmung sehr vage, lässt einen zu großen Auslegungsspielraum zu und sollte eindeutig und mit mehr Detailgenauigkeit neu verfasst werden. Auch die vergleichsweise knappen Erläuterungen zu dieser einzelfallbezogenen Vorratsdatenspeicherung lassen vermuten, dass diese nicht zu Ende gedacht wurde. Zum jetzigen Zeitpunkt sollte man daher von der Einführung dieser Bestimmung in seiner aktuellen Form absehen.

Investitionskostenersatz

Bestehende Massenspeichersysteme sind in der Regel nicht für eine hochgesicherte und individuelle Datenhaltung ausgelegt und müssen erweitert bzw. neu angeschafft werden. Durch die besondere Qualität der Daten und die dadurch strengeren Protokollierungsverpflichtungen ist eine Datenhaltung in getrennten System erforderlich.

Die Anschaffungskosten der technischen Einrichtungen die notwendig sind, um den gesetzlichen Verpflichtungen zur Speicherung von Verkehrsdaten nachzukommen, sind wie bisher (vgl. VfGH G37/02 vom 27.02.2003 zur Vorratsdatenspeicherung) im Ausmaß von mindestens 80% zu ersetzen. Eine Bestimmung die einen Investitionskostenersatz regelt fehlt und ist daher zu schaffen.

Da die Investitionen im Rahmen sicherheitspolitischer Anforderungen getätigt werden müssen und somit dem öffentlichen Interesse dienen, ist ein Ersatz der Kosten zwingend notwendig.
Es muss daher eine gesetzliche Verordnungsermächtigung zum Ersatz der Investitionskosten geschaffen werden, wie dies bereits in der Investitionskostenersatzverordnung (IKEV) für die Umsetzung der damaligen Vorratsdatenspeicherung geschehen ist.

Kostenersatz

Neben den bereits erwähnten Investitionskosten entstehen besonders durch die punktuelle Durchbrechung der Löschungsverpflichtung auch operative Kosten. Diese Kosten entstehen im gleichen Ausmaß wie bei der Verpflichtung zur Auskunft über Daten eine Nachrichtenübermittlung und werden daher im gleichen Umfang zu ersetzen sein.

Es sind allerdings nicht nur die Kosten im Falle einer Auskunft zu ersetzen – diese wären wohl ohnehin bereits durch die bestehenden Bestimmung abgedeckt – sein, **sondern auch jene, die die Speicherung ohne anschließende Auskunft betreffen.** Eine Ungleichbehandlung des Kostenersatz der tatsächlich beauskunfteten Verkehrsdaten mit jenen, die zwar gespeichert, aber in Folge wieder gelöscht werden, ist aufgrund der erheblichen Aufwände nicht gerechtfertigt.

Wie bereits bezüglich des Investitionskostenersatzes erwähnt, erfolgt die Umsetzung der Bestimmungen ausschließlich zur Erreichung sicherheitspolitischer Ziele und ist daher im öffentlichen Interesse. Es ist daher erforderlich, eine Bestimmung in der Überwachungskostenverordnung (ÜKVO) vorzusehen, um somit einen angemessen Kostenersatz zu schaffen.

Umsetzungsfrist

Erst wenn das Sicherheitspaket abschließend beschlossen ist, kann mit der System- und Umsetzungsplanung begonnen, Bestellungen bei Systemlieferanten abgegeben und bestehende Prozesse angepasst und neue geschaffen werden. Die Frist zur Umsetzung der Bestimmungen des Sicherheitspaktes ist vor allem in Anbetracht des notwendigen Eingriffs in die Speicherlogik und besonderen Protokollierungs- und Löschungsverpflichtungen nicht realisierbar.

Des Weiteren ist davon auszugehen, dass aufgrund der neuen Datenschutzgrundverordnung jedenfalls eine umfangreiche Datenschutzfolgeabschätzung durchzuführen sein wird und daher eine zeitintensive Zusammenarbeit mit der Datenschutzbehörde bezüglich der konkret zu treffenden Sicherheitsmaßnahmen erforderlich sein wird, damit Unternehmen rechtssicher arbeiten können. Die bloße Meldung einer Anwendung beim Datenverarbeitungsregister genügt in Zukunft nicht mehr.

Auch die für die Registrierungsverpflichtung notwendigen System- und Prozessanpassungen können bis zum Inkrafttreten der geplanten Änderungen keinesfalls fristgerecht durchgeführt werden.

Es wird daher vorgeschlagen den Zeitpunkt des Inkrafttretens der Bestimmungen um zumindest neun Monate nach Verlautbarung zu verschieben. Nur so kann sichergestellt werden, dass den gesetzlichen Bestimmungen im notwendigen Ausmaß entsprochen werden kann und die Betreiber Rechtssicherheit haben.

T-Mobile Austria GmbH