Bundesministerium für Justiz
Museumstraße 7
1070 Wien
Tel.: +43 1 52152 302753

Vorab per Mail an team.s@bmj.gv.at und
begutachtungsverfahren@parlament.gv.at

Ihr Zeichen: BMJ-S578.031/0008-IV 3/2017

Wien, 18. August 2017

Betreff: Stellungnahme der T-Mobile Austria GmbH zum Begutachtungsentwurf des Strafprozessrechtsänderungsgesetz 2017

Sehr geehrte Damen und Herren,

beiliegend übermitteln wir Ihnen die Stellungnahme der T-Mobile Austria GmbH zum Begutachtungsentwurf des Bundesgesetzes, mit dem die Strafprozessordnung 1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017).

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. Silvia Fretbar-Bustorf
Vice President Legal, Regulatory & Interception
T-Mobile Austria GmbH

T-Mobile Austria GmbH

Stellungnahme der T-Mobile Austria GmbH zum Begutachtungsentwurf des Strafprozessrechtsänderungsgesetz 2017

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

1. § 76a Abs. 1 StPO - PUK-Code

Die geplante Erweiterung des bereits bestehenden §76a StPO verpflichtet Anbieter auf bloßes Ersuchen von kriminalpolizeilichen Behörden den PUK-Code bekannt zu geben.

Bei PUK-Codes handelt es sich um **besonders sensible Daten**, mit denen von Teilnehmern zum Schutz vor unbefugten Zugriffen gesetzte Sperren (PIN) überwunden werden können (Zugangssicherungscode). Durch überwinden dieser Sperre kann auf noch nicht zugestellte bzw. abgehörte Kurz- und Sprachboxnachrichten (d.h. grundsätzlich geschützte Kommunikationsvorgänge) zugegriffen werden und Kenntnis von künftigen Kommunikationsvorgängen (d.h. eingehende Anrufe und Kurznachrichten) erlangt werden. Der PUK-Code kann daher beispielsweise mit dem Passwort eines E-Mail Postfaches verglichen werden. Aus diesem Grund kann nicht, wie in den Erläuterungen zu diesem Begutachtungsentwurf, von einer „vergleichbaren Eingriffsintensität" gesprochen werden.

Das Bundesverfassungsgericht in Deutschland hat eine ähnliche Bestimmung - insbesondere das Fehlen von gesetzlichen Voraussetzungen für die Nutzung Zugangssicherungscodes (zu denen neben PIN-Codes und allgemein Passwörtern, auch der PUK-Code zählt) - als verfassungswidrig erkannt und die betroffenen Bestimmungen aufgehoben (1 BvR 1299/05).

Eine Einordnung als Stammdatum oder Angleichung der verfahrensrechtlichen Voraussetzung und der damit zusammenhängenden ausufernden Beauskunftungsverpflichtung ist daher grundsätzlich abzulehnen.

Es könnte jedoch eine eigenständige Bestimmung (z.B. §76b StPO) geschaffen werden, die es kriminalpolizeiliche Behörden ausschließlich auf Grund einer staatsanwaltlichen Anordnung und

somit **ohne Offenlegung der in den Erläuterungen erwähnten Verdachts- und Beweislage** erlaubt den PUK-Code bei Betreibern anzufragen.

Da durch die Bekanntgabe eines PUK-Codes durch den Netzbetreiber somit die Möglichkeit von Zugriffen auf (noch) dem Fernmeldegeheimnis unterliegenden, durch Art 10a StGG und § 93 TKG 2003 geschützte Verkehrs- und Inhaltsdaten gewährt wird, könnte die Verpflichtung bzw. Ermächtigung zur Beauskunftung von PUK-Codes alternativ in die §§ 134 ff StPO aufgenommen werden: so wäre eine Beauskunftung auf Grund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft – bzw. die vorgesehene Betreiberausfertigung/-anordnung – möglich und wäre daher mit dem Überwachen von Nachrichten und der Auskunft über Daten einer Nachrichtenermittlung gleichgestellt. Auch in diesem Fall ist im Rahmen der Betreiberausfertigung keine Offenlegung der Verdachts- und Beweislage (Begründung) erforderlich. Der in der Überwachungskostenverordnung (ÜKVO) bereits bestehende Kostenersatz für die Beauskunftung von PUK-Codes im Rahmen einer Anordnung nach §§ 134ff StPO spricht ebenfalls für diese Lösungsvariante.

2. § 134 Abs. 2a StPO - Lokalisierung einer technischen Einrichtung / IMSI-Catcher

Richtig ist, dass der Einsatz von technischen Mitteln zur Lokalisierung von Endeinrichtungen (IMSI-Catcher) bereits in § 53 Abs. 3b zur Gefahrenabwehr geregelt ist. Die Ausdehnung der Ermächtig bzw. Einsatzmöglichkeit auf die Bestimmungen der StPO soll wohl den bereits tatsächlichen Gegebenheiten Rechnung tragen.

Der Einsatz von IMSI-Catchern sollte außerhalb der sicherheitspolizeilichen Gefahrenabwehr äußerst restriktiv erfolgen, da es technisch bedingt zu schweren Netzstörungen und lokalen Netzausfällen von bis zu mehreren Minuten kommt bei denen u.a. auch keine Notrufe getätigt werden können. Darüber hinaus bieten IMSI-Catcher technisch bedingt auch die Möglichkeit Telefonate und Kurznachrichten direkt abzufangen und somit Kenntnis vom Inhalt dieser zu erlangen. Es muss daher sichergestellt werden, dass IMSI-Catcher ausschließlicher zur Lokalisierung von technischen Einrichtungen (d.h. Endgeräte) eingesetzt werden.

3. § 134 Abs. 3 StPO - Überwachung von Nachrichten / Nachrichtenbegriff

Das Loslösen der Legaldefinition der „Überwachung von Nachrichten" von den Begrifflichkeiten des Telekommunikationsgesetzes (§ 92 Abs. 3 Z 7 TKG) und der damit einhergehenden Schaffung einer eigenständigen Begriffsbestimmung, schafft – anders als in den Erläuterungen dargelegt – Unklarheit und Rechtsunsicherheit für die Adressaten der Norm.

Nach den Erläuterungen zum Begutachtungsentwurf soll damit ausdrücklich klargestellt werden, dass neben dem gesamte Internetverkehr auch ausschließlich maschinenbasierte Kommunikation (Maschine to Maschine; M2M) und erfasst sein soll. Die vorgeschlagene Legaldefinition des Nachrichtenbegriffs geht zu weit und umfasst jede nur denkmögliche elektronische Kommunikation - wo doch nur jene der verschlüsselten Nachrichten erfasst werden soll - und führt zu einer gesetzlich normierten Möglichkeit einer allumfassenden Überwachung von Kommunikation und Informationsaustausch.

Es sollte im Sinne einer normenklaren Regelung daher eine eigenständige Bestimmung (§ 134 Abs. 3a, „Überwachung von verschlüsselten Nachrichten") geschaffen werden, die neben die unveränderte, bereits bestehende Bestimmung des § 134 Abs. 3 tritt, welche die Überwachung von Nachrichten iSd. § 92 Abs. 3 Z 7 TKG regelt.

T-Mobile Austria GmbH