

Berlin, 20. Juli 2015

Notifizierungsnummer 2015/0288/D - V00T

Sehr geehrter Herr Präsident Juncker,
sehr geehrte Damen und Herren Kommissare,

zurzeit führt die Kommission ein Notifizierungsverfahren gemäß der Richtlinie 98/34/EC zum „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ durch. Wir wenden uns mit diesem Schreiben an Sie, da wir den Gesetzentwurf für unvereinbar mit dem EU-Recht, insbesondere mit den Grundrechten auf Privatsphäre und den Schutz personenbezogener Daten halten.

Der Digitale Gesellschaft e.V. ist ein gemeinnütziger Verein, der sich seit seiner Gründung im Jahr 2010 für Grundrechte und Verbraucherschutz im Internet einsetzt. Zum Erhalt und zur Fortentwicklung einer offenen digitalen Gesellschaft engagiert sich der Verein gegen den Rückbau von Freiheitsrechten im Netz und für die Realisierung digitaler Potentiale bei Wissenszugang, Transparenz, Partizipation und kreativer Entfaltung.

Anliegend finden Sie eine Darstellung unserer rechtlichen Bedenken gegen den vorliegenden Gesetzentwurf. Wir bitten Sie, diese Einwände bei der Durchführung des Notifizierungsverfahrens zu berücksichtigen.

Mit freundlichen Grüßen,



Digitale Gesellschaft e.V.

A handwritten signature in black ink, appearing to read "A. Sander", is positioned to the right of the logo.

Alexander Sander, Geschäftsführer

Mit dem verfahrensgegenständlichen Gesetzentwurf werden die Erbringer öffentlich zugänglicher Telekommunikationsdienste dazu verpflichtet, Verkehrsdaten aus der elektronischen Kommunikation für zehn Wochen und Standortdaten für vier Wochen anlasslos zu speichern¹. Die Daten dürfen zum Zwecke der Verfolgung besonders schwerer Straftaten und zur Abwehr konkreter Gefahren für Leib, Leben, Freiheit der Person oder für den Bestand des Bundes oder eines Landes an die zuständigen Behörden übermittelt werden². Des Weiteren dürfen die Daten für sogenannte Bestandsdatenauskünfte i.S.d. § 113 Abs. 1 Satz 3 TKG verwendet werden³.

Die vorgesehenen Regelungen der §§ 113a – 113g TKG-E verletzen die EU-Grundrechte auf Schutz der Privatsphäre (Art. 7 EU-GR) und den Schutz personenbezogener Daten (Art. 8 EU-GR). Entgegen Art. 52 Abs. 1 S. 2 EU-GR wahren die Normen nicht den Grundsatz der Verhältnismäßigkeit.

Die Anwendbarkeit der EU-Grundrechte ergibt sich aus Art. 15 Abs. 1 S.3 E-Privacy-Richtlinie (2002/58/EG).

1. Eingriff in Artf. 7, 8 EU-GR

Dass bereits die Verpflichtung zur Speicherung der Verkehrs- und Standortdaten in besonders schwerwiegender Weise in die Grundrechte aus Artf. 7, 8 EU-GR eingreift, hat der Europäische Gerichtshof in seiner Entscheidung vom 8. April 2014 (C-293/12 u.a.) in Bezug auf die Richtlinie 2006/24/EG ausführlich dargelegt⁴. Diese Beurteilung trifft in gleicher Weise auf die in dem verfahrensgegenständlichen Gesetzentwurf vorgesehene Speicherpflicht zu.

2. Unverhältnismäßigkeit

Die Unverhältnismäßigkeit dieser Eingriffe ergibt sich insbesondere aus zwei Gesichtspunkten. Zum Einen soll die Speicherung nach dem vorliegenden Entwurf anlasslos und undifferenziert erfolgen. Des Weiteren beschränkt sich die Speicherpflicht nicht auf das absolut Notwendige. Beide Umstände hatte der EuGH auch in seinem Urteil vom 8. April 2014 bezüglich der Richtlinie 2006/24/EG ausdrücklich als Gründe für die Unverhältnismäßigkeit hervorgehoben.

1 Vgl. §§ 113a, 113b Abs. 1 – 3 TKG-E

2 Vgl. § 113c Abs. 1 Nr. 1, 2 TKG-E

3 Vgl. § 113c Abs. 1 Nr. 3 TKG-E

4 Vgl. EuGH, Urt. v. 8. April 2014, C-293/12, Rn. 32 - 37

a. Anlasslosigkeit der Speicherung

So betrifft die im Gesetzentwurf vorgesehene Verpflichtung zur Speicherung von Verkehrs- und Standortdaten in umfassender Weise alle Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Die Speicherverpflichtung gilt daher auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte.⁵

Des Weiteren soll die Speicherverpflichtung zwar dazu beitragen, schwere Straftaten zu verhindern und zu verfolgen, gleichwohl verlangt der Gesetzentwurf an keiner Stelle einen Zusammenhang zwischen den zu speichernden Daten einerseits und einer konkreten Gefahr für die öffentliche Sicherheit oder einen konkreten Verdacht einer Straftat andererseits. Insbesondere beschränkt sich die Speicherverpflichtung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geographischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.⁶

b. keine Beschränkung auf das absolut Notwendige

Nach ständiger Rechtsprechung des EuGH verlangt das Grundrecht auf Schutz der Privatsphäre außerdem, dass Eingriffe in das Recht auf den Schutz personenbezogener Daten stets auf das absolut Notwendige beschränkt sein müssen⁷.

aa. Berufsgeheimnisträger

Gegen diese Vorgabe verstößt der vorliegende Entwurf bereits deswegen, weil er in unzureichender Weise Ausnahmen von der Speicherverpflichtung für Berufsgeheimnisträger vorsieht. Während die Daten der Mitarbeiter von Behörden, von kirchlichen und sozialen Einrichtungen gänzlich von der Speicherung ausgenommen sind⁸, werden die Daten anderer Berufsgeheimnisträger (z.B. Rechtsanwälte, Steuerberater, Wirtschaftsprüfer, Ärzte, Pharmazeuten, Psychotherapeuten, Journalisten) vollumfänglich gespeichert. Lediglich ihr Abruf und ihre Verwendung in Strafverfahren sind nach dem Entwurf untersagt⁹. Damit

5 Vgl. entsprechend zur RL 2006/24/EG EuGH, Urt. v. 8. April 2014, C-293/12, Rn. 58.

6 Vgl. entsprechend zur RL 2006/24/EG EuGH, Urt. v. 8. April 2014, C-293/12, Rn. 59.

7 Vgl. EuGH Urteil IPI, C-473/12, EU:C:2013:715, Rn. 39 und die dort angeführte Rechtsprechung

8 Vgl. § 113b.6 TKG-E, § 99.2 TKG

9 Vgl. § 100g.4 StPO-E

beschränkt sich die Speicherpflicht nicht auf das absolut Notwendige, sondern erstreckt sich auch auf Daten, deren spätere Verwendung sogar gesetzlich ausgeschlossen ist.

Demgegenüber verfährt nicht das Argument, dass der Schutz sämtlicher Berufsheimnisträger eine umfassende zentrale Datenbank aller Personen mit Verschwiegenheitspflichten erforderlich machen würde. Viele berufsständische Organisationen, wie etwa die Bundesrechtsanwaltskammer, führen in ihrem Bereich bereits vollständige Verzeichnisse ihrer Mitglieder¹⁰. Zumindest bei Berufsgruppen, für die derartige Listen existieren, könnte für Ausnahmen von der Speicherpflicht auch auf diese zurückgegriffen werden. Es wäre daher ohne Weiteres möglich, die Speicherpflicht zugunsten des Schutzes von Berufsheimnisträgern noch weiter einzugrenzen, ohne eine umfassende zentrale Datenbank aller Personen mit Verschwiegenheitspflichten zu erstellen. Die Speicherpflicht beschränkt sich deshalb nicht auf das absolut Notwendige.

Im Übrigen beschränkt sich die Speicherpflicht auch bereits deswegen nicht auf das absolut Notwendige, weil ein sachlicher Grund für die in dem Entwurf konkret vorgenommene Unterscheidung zwischen den Daten bestimmter Gruppen von Berufsheimnisträgern fehlt. Es ist vollkommen willkürlich, behördlichen, kirchlichen und sozialen Einrichtungen größeren Schutz ihrer Kommunikation zukommen zu lassen als etwa Rechtsanwälten oder Journalisten. Sämtliche dieser Berufsgruppen erfüllen in vergleichbarer Weise wichtige gesamtgesellschaftliche und rechtsstaatliche Aufgaben und dienen der Verwirklichung von Grundrechten. Sie sind daher auch alle in gleicher Weise schutzwürdig.

Hierbei handelt es sich nicht um eine rein formelle Frage, da die Daten allein durch ihre Speicherung einem hohen Missbrauchsrisiko ausgesetzt werden. Auch wenn der Entwurf die Erbringer öffentlicher Telekommunikationsleistung zu verhältnismäßig intensiven Vorkehrungen für die Datensicherheit verpflichtet, so kann niemals vollständig ausgeschlossen werden, dass Unbefugte Zugriff auf die gespeicherten Daten nehmen können. Gerade angesichts der Enthüllungen von Edward Snowden und der Plattform WikiLeaks über die Spähpraktiken der NSA und des GCHQ wird deutlich, dass zumindest diese Nachrichtendienste über faktisch unbegrenzte Ressourcen verfügen, um sensible Infrastrukturen anzugreifen und Daten zu exfiltrieren. Medienberichten zufolge haben gerade britische Nachrichtendienste jahrelang die rechtlich besonders geschützte Kommunikation zwischen Anwälten und ihren

¹⁰ Vgl. beispielsweise Bundesweites Amtliches Anwaltsverzeichnis der Bundesrechtsanwaltskammer: <http://www.rechtsanwaltsregister.org/default.aspx?AspxAutoDetectCookieSupport=1>

Mandanten überwacht¹¹. Nicht zuletzt dieses Beispiel zeigt, dass die Gefahren für die besonders sensiblen Kommunikationsdaten nicht rein hypothetischer oder potentieller Natur sind, sondern tatsächlich und konkret bestehen.

bb. Fehlender Effektivitätsnachweis

Die Notwendigkeit der Speicherung scheitert zudem an dem Umstand, dass es für die Annahme, die Speicherung leiste einen effektiven und unverzichtbaren Beitrag zur Verfolgung schwerer Straftaten oder zur Abwehr erheblicher konkreter Gefahren, bis heute keinerlei Nachweis gibt. Für den Zeitraum von 2008 bis 2010, in dem es in Deutschland bereits ein Gesetz zur Vorratsdatenspeicherung gab, gelangte eine Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht vielmehr zu dem Ergebnis, dass sich keine Belege für eine Steigerung der Aufklärungsquote durch die Vorratsdatenspeicherung finden ließen¹². Ähnlich kritisch wird die Effektivität der Vorratsdatenspeicherung bei der Verfolgung schwerer Straftaten auch in einem Gutachten des Wissenschaftlichen Dienstes des Bundestages bewertet¹³. Selbst Vertreter der Bundesregierung und des federführenden Bundesministeriums der Justiz und für Verbraucherschutz waren auf Nachfragen von Presse¹⁴ und Abgeordneten¹⁵ des Deutschen Bundestages außer Stande, irgendwelche belastbaren Fakten oder Zahlen zur Wirksamkeit des Instruments der Vorratsdatenspeicherung zu benennen. Auch in einer von der EU-Kommission herausgegebenen Datensammlung mit dem Titel „Evidence for the necessity of data retention in the EU“ gelingt der Nachweis der Notwendigkeit nicht¹⁶. Evident wird allenfalls, dass es eine äußerst geringe Zahl von Einzelfällen gibt, in denen die Vorratsdatenspeicherung bei der Aufklärung hilfreich, aber keineswegs notwendig gewesen wäre.

11 Vgl. <http://www.theguardian.com/uk-news/2015/feb/18/uk-admits-unlawfully-monitoring-legally-privileged-communications>

12 Vgl. <https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf>

13 Vgl. https://www.vorratsdatenspeicherung.de/images/Sachstand_036-11.pdf

14 Vgl. <https://netzpolitik.org/2015/justizminister-maas-zur-vorratsdatenspeicherung-die-notwendigkeit-kann-ich-nicht-beweisen/>

15 Vgl. <http://dip21.bundestag.de/dip21/btd/18/050/1805062.pdf>, S. 17 (Frage d. Abg. Wawzyniak)

16 Vgl. http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf