



POSTANSCHRIFT Bundesministerium der Justiz und für Verbraucherschutz, 11015 Berlin

Herrn
Michael Ebeling

HAUSANSCHRIFT Mohrenstraße 37, 10117 Berlin
POSTANSCHRIFT 11015 Berlin

BEARBEITET VON Referat Z A 4
TELEFON (+49 30) 18 580 -0
FAX (+49 30) 18 580-9525
E-MAIL poststelle@bmjv.bund.de
AKTENZEICHEN Z A 4 - 1451/6 II - Z3 740/2015

DATUM Berlin, 19. Oktober 2015

BETREFF Auskunft nach dem Informationsfreiheitsgesetz (IFG)
HIER Stellungnahme der EU-Kommission zum Gesetzentwurf zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten
BEZUG 1. Ihr Antrag vom 12. September 2015 per E-Mail
2. Meine Zwischennachricht vom 9. Oktober 2015
ANLAGE 4 Seiten

Sehr geehrter Herr Ebeling,

ich nehme Bezug auf den bisherigen Schriftverkehr und gebe Ihrem Antrag nach dem Informationsfreiheitsgesetz (IFG) vom 12. September 2015 statt.

Die von Ihnen erbetene Stellungnahme der EU-Kommission zum Gesetzentwurf zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten füge ich diesem Schreiben als Anlage bei.

Mit freundlichen Grüßen

Im Auftrag

Mitteilung 317

Mitteilung der Kommission - TRIS/(2015) 02810
Richtlinie 98/34/EG
Notifizierung: 2015/0288/D

Ausführliche Stellungnahme der Kommission im Hinblick auf die Dienste (Artikel 9 Absatz 2 dritter Gedankenstrich der Richtlinie 98/34/EG). Diese ausführliche Stellungnahme verlängert die Stillhaltefrist bis zum 06-10-2015.

Comunicado detallado - Podrobné vyjádření - Udførlig udtalelse - Ausführlichen Stellungnahme - Üksikasjalik arvamus - Επιπεριστατωμένη γνώμη - Detailed opinion - Avis circonstancié - Parere circostanziato - Detalizēts atzinums - Detali nuomonė - Részletes vélemény - Opinioni dettaljata - Uitvoerig gemotiveerde mening - Opinia szczegółowa - Parecer circunstanciado - Podrobný úsudok - Podrobno mnenje - Yksityiskohtainen lausunto - Detaljerat yttrande - Подробно становище - Aviz detaliat - Aviz detaliat.

Abre el plazo de statu quo - Zahájení doby pozastavení prací - Fristen for proceduren indledes - Beginn der Verfahrensfrist - Ooteaja avamine - Έναρξη της προθεσμίας διαδικασίας - Opening of the standstill period - Ouvrir le délai de statu quo - E aperto il termine di procedura - Bezdarbības perioda sākums - Atidėjimo periodo pradžia - A halasztási időszak megnyitása - Ftuħ tal-perijodu ta' waqfien - Begin van de termijn voor de procedure - Otwarcie okresu odroczenia - Abre o prazo de procedimento - Otvorenie pozastavenej periódy - Uvedba obdobja mirovanja - Menettelyn määraaika alkaa - Inleder förfarandets frist - Откриване на периода на прекъсване - Deschiderea perioadei de stagnare - Deschiderea perioadei de stagnare.

Die Kommission hat diese ausführliche Stellungnahme am 07-09-2015 empfangen.
The Commission received this detailed opinion on the 07-09-2015.
La Commission a reçu cet avis circonstancié le 07-09-2015.

ΟΓΡΑΝΙΧΕΗ - OMEZENÝ PRÍSTUP - BEGRÆNSET - ZUGANGSBESCHRÄNKT - ΕΣΩΤΕΡΙΚΗ ΧΡΗΣΗ - LIMITED - LIMITADO - PIIRATUD - RAJOITETTU - LIMITÉ - KORLÁTOZOTT HOZZÁFÉRÉS - RISERVATO - RIBOTO NAUDOJIMO DOKUMENTAS - IEROBEŽOTAS PIEĒJAMĪBAS DOKUMENTS - RĪSTRETT - RESTRITO - LIMITAT - OBMEDZENÝ - OMEJENO - BEGRÄNSAT

ein im Rahmen der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften bearbeitetes Dokument
Dieses Dokument darf nur Mitarbeitern der Europäischen Kommission und der Mitgliedstaaten übermittelt werden, die, wie in Richtlinie 98/34/EG festgelegt, darüber in Kenntnis gesetzt werden müssen.
Ein mit dem Hinweis „LIMITED“ (zugangsbegrenzt) gekennzeichnetes Dokument darf nicht veröffentlicht werden.
Bei der elektronischen Übermittlung des Dokuments innerhalb der Kommission hat diese über SECEM (SECure Email) zu erfolgen.
Empfänger des Dokuments, die nicht über die festgelegte Berechtigung zur Kenntnisnahme wie oben angegeben verfügen, haben den Verfasser, Aussteller oder Absender unverzüglich entsprechend zu informieren und das Dokument auf sichere Weise ungelesen zurückzusenden. Im Fall der Unterlassung stellt dies eine Verletzung der Sicherheit dar, was zu Disziplinarmaßnahmen oder rechtlichen Schritten führen kann.

(MSG: 201502810.DE)

1. MSG 317 IND 2015 0288 D DE 07-09-2015 07-09-2015 COM 9.2(3) 07-09-2015

2. Kommission

3. GD GROW/B/2 - N105 04/63

4. 2015/0288/D - V00T

5. Artikel 9 Absatz 2 dritter Gedankenstrich der Richtlinie 98/34/EG

6. im Rahmen des in der Richtlinie 98/34/EG festgelegten Notifizierungsverfahrens notifizierten die deutschen Behörden der Kommission am 5. Juni 2015 den Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten.

Durch den Gesetzentwurf wird Erbringern öffentlich zugänglicher Telekommunikationsdienste in Deutschland die Speicherung von Verkehrsdaten vorgeschrieben. Die Verkehrsdaten, wie Rufnummer, internationale Kennung, Datum und Uhrzeit des Anrufs/der Internetnutzung, Internetprotokolladresse, Benutzerkennung sind 10 Wochen lang zu speichern, während die Standortdaten 4 Wochen lang aufbewahrt werden sollen.

Die Prüfung des Entwurfs hat die Kommission zur Abgabe der folgenden ausführlichen Stellungnahme und Bemerkungen veranlasst.

1. Ausführliche Stellungnahme

Vorratsspeicherungspflicht in Deutschland

Gemäß § 113b des notifizierten Entwurfs einer Verordnung würden Erbringer von elektronischen Kommunikationsdiensten verpflichtet, die laut dem notifizierten Entwurf auf Vorrat zu speichernden Daten in Deutschland zu speichern.

Jegliche Maßnahme auf nationaler Ebene, die die Ausführung der Dienstleistungserbringung verbietet, verhindert oder weniger attraktiv macht, stellt eine Einschränkung dieser Grundfreiheit dar, auch wenn sie ohne Diskriminierung aufgrund der Staatsangehörigkeit anwendbar ist (siehe zum Beispiel die Rechtssache C-65/05, Kommission gegen Hellenische Republik, Randnr. 48).

Eine Verpflichtung für Erbringer von elektronischen Kommunikationsdiensten, die entsprechenden Daten in Deutschland zu speichern, würde zunächst eine Einschränkung hinsichtlich der Erbringung von elektronischen Kommunikationsdiensten darstellen. Als Folge dessen wären Kommunikationsanbieter aus anderen Mitgliedstaaten („MS“), die Zugang zum deutschen Markt haben möchten, im Vergleich zu ihren in Deutschland niedergelassenen Wettbewerbern mit zusätzlichen Kosten konfrontiert, da sie daran gehindert würden, alleinige, zentralisierte Speichereinrichtungen, die bereits in anderen MS (oder an einem sonstigen Ort) vorhanden sind, zu nutzen. Diese Unternehmen würden somit finanziell gegenüber ihren Wettbewerbern mit Niederlassung in Deutschland benachteiligt, da sie auf mehrere Speichereinrichtungen umstellen müssten. Da diese Kosten erheblich sein können, ist diese Beschränkung geeignet, ein Markthemmnis oder einen Wettbewerbsnachteil für diese Erbringer aus anderen MS darzustellen, die noch nicht über solche Einrichtungen vor Ort verfügen. Zweitens würde sie eine Beschränkung im Hinblick auf die Erbringung von Datenspeicherdiensten darstellen, weil eine Nachfrage solcher Dienstleistungen von Anbietern, die über Speichereinrichtungen in anderen MS verfügen, seitens deutscher Erbringer von Telekommunikationsdiensten ausgeschlossen würde.

Beschränkungen des freien Dienstleistungsverkehrs sind nur in dem Maße zulässig, in dem sie notwendig und angemessen zum Schutz spezifischer öffentlicher Interessen sind (wie beispielsweise der öffentlichen Ordnung oder öffentlichen Sicherheit, die ausdrücklich in Artikel 52 AEUV erwähnt werden, oder anderer zwingender Gründe des Allgemeininteresses, die durch die Rechtsprechung des Gerichtshofs anerkannt sind).

In der dem notifizierten Entwurf beigefügten Begründung wird zugestanden, dass die Speicherpflicht für Daten in Deutschland eine Beschränkung des freien Dienstleistungsverkehrs darstellt. Es wird darin jedoch die Ansicht vertreten, dass eine solche Beschränkung aufgrund des öffentlichen Interesses zur Gewährleistung des Datenschutzes und der Datensicherheit gerechtfertigt sei. Die deutschen Behörden erklären: „Eine Beschränkung auf das Inland ist notwendig, um die grundrechtlichen Erfordernisse des Datenschutzes und der Datensicherheit zu gewährleisten, die gespeicherten Vorratsdaten wirksam vor Missbrauch sowie vor jedem unberechtigten Zugang und jeder unberechtigten Nutzung zu schützen und das durch eine unabhängige Stelle zeitnah und effizient überwachen zu können.“ Gemäß der ständigen Rechtsprechung sind Ausnahmen von den Grundfreiheiten des Vertrags eng auszulegen und restriktiv anzuwenden (siehe z. B. Rechtssache C-483/99, Kommission gegen Französische Republik, Randnummer 48). Rechtfertigungen aufgrund von administrativen oder technischen Unterschieden zwischen Mechanismen, die dem Schutz des gleichen öffentlichen Interesses dienen sollen, wie es im vorliegenden Fall der Fall zu sein scheint, werden nicht gewährt. Die von einem Mitgliedstaat geltend gemachten Rechtfertigungsgründe müssen somit von einer Untersuchung zur Zweckmäßigkeit und zur Verhältnismäßigkeit der von diesem Staat angenommenen Maßnahme und von spezifischen Nachweisen, durch die die Argumente bekräftigt werden, begleitet werden (siehe Rechtssache C-8/02 Leichtle, Randnummer 45). Die von Deutschland im Rahmen der Notifizierung vorgelegten Informationen und Rechtfertigungen genügen den oben genannten Anforderungen nicht.

In diesem Zusammenhang ist zu beachten, dass die Datenlokalisierung allein selbst keine zusätzliche Sicherheit schafft, wenn man berücksichtigt, dass die Erbringer gemäß der Richtlinie 2002/58/EG (Artikel 6) Verkehrsdaten, zu Gebührenabrechnungs- und Übertragungszwecken ohne geografische Beschränkungen speichern dürfen. Die inhaltlichen Anforderungen hinsichtlich der Sicherheit der Datenverarbeitung wurden allerdings im Rahmen von Artikel 17 Absatz 1 der Richtlinie 95/46/EG und Artikel 4 der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten in der elektronischen Kommunikation harmonisiert. Es wird verdeutlicht, dass es sich bei diesen harmonisierten Anforderungen um Pflichten handelt, die dem für die Verarbeitung der Daten Verantwortlichen (d. h. im vorliegenden Zusammenhang dem Telekommunikationsanbieter) obliegen. Darüber hinaus muss der für die Verarbeitung der Daten Verantwortliche, wenn die Speicherung von einem anderen Anbieter als dem „für die Verarbeitung der Daten Verantwortlichen“ durchgeführt wird, sicherstellen, dass der Speicheranbieter („Auftragsverarbeiter“ im Sinne der Richtlinie 95/46/EG) an die Einhaltung derselben inhaltlichen Pflichten gebunden ist wie der „für die Verarbeitung der Daten Verantwortliche“ (Artikel 17 Absatz 3, 2. Gedankenstrich der Richtlinie 95/46/EG). Der für die Verarbeitung der Daten Verantwortliche muss im Hinblick auf die Auswahl und weitere Überwachung des Auftragsverarbeiters ebenfalls bestimmte zusätzliche Pflichten und Schutzmaßnahmen einhalten (Artikel 17 Absatz 2 und 3, 1. Gedankenstrich der Richtlinie 95/46/EG).

Gemäß der ständigen Rechtsprechung ist eine nationale Maßnahme in einem Bereich, der Gegenstand einer vollständigen Harmonisierung auf EU-Ebene war, angesichts der Bestimmungen der Harmonisierungsmaßnahme und nicht der des Vertrags zu bewerten (siehe zuletzt C-265/12, Citroën Belux, Randnummer 31). Darüber hinaus werden nach Artikel 1 Absatz 2 der Richtlinie 95/46/EG die Mitgliedstaaten daran gehindert, „den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des [...] gewährleisteten Schutzes [der Grundrechte natürlicher Personen bei der Verarbeitung personenbezogener Daten]“ zu beschränken oder untersagen. Es sind keine Ausnahmen von diesem Artikel oder Beschränkungen dessen durch die nationalen Maßnahmen, die gemäß Artikel 15 der Richtlinie 2002/58/EG angenommen werden, gestattet. Aus den obigen Ausführungen folgt, dass ein Mitgliedstaat nicht den freien Dienstleistungsverkehr beschränken darf, indem er den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des Schutzes der Grundrechte natürlicher Personen bei der Verarbeitung personenbezogener Daten beschränkt oder untersagt.

Gemäß Artikel 17 Absatz 1 der Richtlinie 95/46/EG hat Deutschland das Recht, Erbringern von elektronischen

Kommunikationsdiensten (für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern), die im Sinne von Artikel 4 der Richtlinie in Deutschland niedergelassen sind, spezifische Pflichten im Hinblick auf technologische Mittel zur Gewährleistung der Datensicherheit (wie z. B. starke Verschlüsselung) aufzuerlegen. Solche spezifischen Sicherheitsmaßnahmen können Anbietern unabhängig davon auferlegt und durchgesetzt werden, an welchem Ort die Daten gespeichert sind. Darüber hinaus könnte der deutsche Gesetzgeber unter denselben Bedingungen (der Verantwortliche oder Verarbeiter ist in Deutschland ansässig) zur Gewährleistung einer effektiven Überwachung der Einhaltung der Vorschriften in Bezug auf den Datenschutz und die Datensicherheit durch die nationalen Aufsichtsbehörden besondere Bedingungen einführen, selbst wenn die Daten in einem anderen Mitgliedstaat gespeichert werden. Dies könnte beispielsweise Verpflichtungen zur Bereitstellung spezifischer Informationen und/oder Erfüllung bestimmter Bedingungen, regelmäßige Berichterstattung und Rechenschaftspflichten; Verpflichtungen, sich freiwilligen Prüfungen durch die deutschen Behörden zu unterziehen oder unabhängige Beauftragte zu ernennen sowie abschreckende Strafen im Falle der Nichteinhaltung umfassen. Außerdem sind gemäß Artikel 28 der Richtlinie 95/46/EG die Aufsichtsbehörden verschiedener Mitgliedstaaten zur Zusammenarbeit verpflichtet.

Diesbezüglich ist ebenfalls zu beachten, dass der Gerichtshof im Urteil in der Rechtssache C-293/12 Digital Rights Ireland die Richtlinie 2006/24/EG unter anderem mit der Begründung aufgehoben hat, dass die Richtlinie nicht vorschreibt, dass die fraglichen Daten innerhalb der Europäischen Union auf Vorrat gespeichert werden müssen, sodass es nicht als vollumfänglich gewährleistet angesehen werden kann, dass die Einhaltung der Erfordernisse des Datenschutzes und der Datensicherheit, wie in Artikel 8 Absatz 3 der Charta ausdrücklich gefordert, durch eine unabhängige Stelle überwacht wird (siehe Randnummer 68). Der Gerichtshof machte jedoch keinen Unterschied in Bezug auf das in jedem Mitgliedstaat gewährleistete Schutzniveau, da jeder Mitgliedstaat in der Lage sein sollte, ein gleichwertiges Schutzniveau zu gewährleisten, das dem zur Umsetzung der Datenschutzlinie vorgeschriebenen entspricht. Stattdessen wird durch die Entscheidung eine allgemeinere Vorschrift zur Speicherung der Daten innerhalb der Europäischen Union insgesamt eingeführt, ohne eine Beschränkung des freien Datenverkehrs zwischen Mitgliedstaaten zu rechtfertigen.

Angesichts der obigen Ausführungen fordert die Kommission Deutschland auf, die Verpflichtung in § 113b des Entwurfs des Telekommunikationsgesetzes zur ausschließlichen Speicherung der Vorratsdaten in Deutschland zu streichen oder andernfalls weitere Informationen in Bezug darauf vorzulegen, wie eine solche Verpflichtung mit den oben erwähnten Bestimmungen des EU-Rechts vereinbar sein könnte, insbesondere mit Artikel 56 AEUV und Artikel 1 Absatz 2 der Richtlinie 95/46/EG.

Diese Gründe veranlassen die Kommission, die vorliegende ausführliche Stellungnahme nach Artikel 9 Absatz 2 der Richtlinie 98/34/EG abzugeben und darin festzustellen, dass der betreffende Entwurf einer Verordnung eine Verletzung von Artikel 56 AEUV sowie Artikel 1 Absatz 2 der Richtlinie 95/46/EG darstellen würde, wenn er ohne Berücksichtigung der hier gemachten Ausführungen angenommen würde.

Die Kommission erinnert Ihre Regierung daran, dass die Abgabe einer ausführlichen Stellungnahme nach Artikel 9 Absatz 2 der vorgenannten Richtlinie 98/34/EG den Mitgliedstaat, der den betreffenden Entwurf der technischen Vorschrift verfasst hat, verpflichtet, diesen nicht vor Ablauf von vier Monaten nach seiner Notifizierung anzunehmen.

Diese Frist endet demnach am 6. Oktober 2015.

Die Kommission weist Ihre Regierung des Weiteren darauf hin, dass der Mitgliedstaat, an den die ausführliche Stellungnahme gerichtet wurde, nach dieser Bestimmung ebenfalls verpflichtet ist, die Kommission über die von ihm beabsichtigten Folgemaßnahmen zu informieren.

Sollte der Wortlaut des betreffenden Entwurfs von technischen Vorschriften ohne Berücksichtigung der oben genannten Einwände angenommen werden, könnte sich die Kommission zur Übersendung eines Mahnschreibens gemäß Artikel 258 des Vertrags über die Arbeitsweise der Europäischen Union gezwungen sehen. Des Weiteren behält sie sich die Möglichkeit zur Übersendung eines Mahnschreibens für den Fall vor, dass ihr die Antwort Ihrer Regierung zum Zeitpunkt der Annahme des infrage stehenden Entwurfs von technischen Vorschriften nicht zugegangen ist.

Die Kommission fordert Ihre Regierung auf, ihr den endgültigen Wortlaut des betreffenden Entwurfs von technischen Vorschriften unverzüglich nach Annahme mitzuteilen. Die Nichtübermittlung dieses Wortlauts würde eine Verletzung von Artikel 4 Absatz 3 des Vertrags über die Europäische Union und von Artikel 8 Absatz 3 der Richtlinie 98/34/EG darstellen, gegen die vorzugehen sich die Kommission vorbehalten.

2. Bemerkungen

Die Kommission nimmt ebenfalls die Gelegenheit wahr, die folgenden Bemerkungen an die deutschen Behörden zu übermitteln.

Speicherdauer (Entwurf § 113b Absatz 1 des Telekommunikationsgesetzes)

Die faktischen Elemente und Nachweise (d. h. statistische Daten oder Studien), die der Bewertung zugrunde liegen, dass eine Speicherfrist von 4 bzw. 10 Wochen unbedingt notwendig ist, um das verfolgte Ziel des Allgemeininteresses zu erreichen, sollten bereitgestellt und erläutert werden.

Verschiedene Kategorien von Verkehrsdaten

Die Kommission stellt fest, dass in § 100g der Strafprozessordnung zwischen den Verkehrsdaten unterschieden wird, die gemäß § 96 Absatz 1 des Telekommunikationsgesetzes gespeichert werden, und den Verkehrsdaten, die gemäß Entwurf § 113b des Telekommunikationsgesetzes gespeichert werden. Die Kommission bittet um eine Bestätigung, ob die Daten gemäß § 96 Absatz 1 des Telekommunikationsgesetzes nur zum Zwecke der Gebührenerhebung und -abrechnung der Teilnehmer gespeichert werden.

Zugang zu Verkehrsdaten zum Zwecke der Strafverfolgung und Funkzellenabfragen (Entwurf § 100g Absatz 1 und Entwurf § 100g Absatz 3 Satz 1 der Strafprozessordnung)

Die Kommission stellt fest, dass der Entwurf § 100g Absatz 1 der Strafprozessordnung besagt, dass

Verkehrsdaten (§ 96 Absatz 1 des Telekommunikationsgesetzes) von Strafverfolgungsbehörden erhoben werden dürfen, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten für die Bedeutung der Sache angemessen ist, sowie wenn eine Person als Täter oder Teilnehmer eine Straftat von erheblicher Bedeutung begangen hat, insbesondere eine in § 100a Absatz 2 der Strafprozessordnung bezeichnete Straftat. Da keine weitere Definition einer Straftat von erheblicher Bedeutung angegeben wird, führt dies möglicherweise zu einer Einschränkung des Grundrechts auf den Schutz personenbezogener Daten, die nicht eindeutig abgegrenzt ist, damit sie als „gesetzlich vorgegeben“ angesehen werden kann und gewährleistet werden kann, dass die Einschränkung auf den unbedingt nötigen Umfang beschränkt ist. Der gleiche Einwand besteht hinsichtlich des Zugangs von Strafverfolgungsbehörden zu Verkehrsdaten über Funkzellenabfragen (Entwurf § 100g Absatz 3 Satz 1 der Strafprozessordnung), bei dem Bezug auf den Entwurf § 100g Absatz 1 dieser Ordnung genommen wird.

Vorherige Prüfung des Zugangs zu Daten

Die Kommission möchte die deutschen Behörden auffordern, zu klären, ob der Zugang zu Vorratsdaten für Strafverfolgungsbehörden einer vorherigen Prüfung durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegt, und falls ja, die entsprechenden Bestimmungen anzugeben und zu erläutern.

Überwachung und Prüfung der Verwendung von Daten (Entwurf § 113c Absatz 1 des Telekommunikationsgesetzes)

Die Kommission stellt fest, dass in den notifizierten Bestimmungen keine (Ex-post-)Instrumente festgelegt werden, um eine juristische Prüfung der Entscheidungen, die eine Übermittlung von gemäß Entwurf § 113c Absatz 1 des Telekommunikationsgesetzes gespeicherten Daten verlangen, zu erwirken.

In Anbetracht der wesentlichen Bedeutung einer Gewährleistung des Rechts auf Zugang zu wirksamen Rechtsmitteln (Artikel 47 der Charta) in diesem Bereich möchte die Kommission die deutschen Behörden auffordern, Informationen in Bezug auf den Zugang zu Rechtsmitteln zur Erwirkung einer juristischen Prüfung der Entscheidungen, die eine Übermittlung von gemäß dem Entwurf von § 113c Absatz 1 des Telekommunikationsgesetzes gespeicherten Daten verlangen, vorzulegen.

Anordnungen und Verlängerungen von Maßnahmen - § 101a Absatz 2 der Strafprozessordnung

§ 101a Absatz 2 der Strafprozessordnung besagt, dass wenn eine Maßnahme in einem spezifischen Fall nach § 100g angeordnet oder verlängert wird, in der Begründung die wesentlichen Erwägungen zur Erforderlichkeit und Angemessenheit der Maßnahme, auch hinsichtlich des Umfangs der zu erhebenden Daten und des Zeitraums, für den sie erhoben werden sollen, darzulegen sind. Die Kommission stellt fest, dass ungeachtet der Verpflichtung zur Angabe von Gründen für die Erforderlichkeit und Angemessenheit der Maßnahme die Tatsache, dass in den Bestimmungen keine Höchstfrist für die Gesamtdauer der Anordnungen oder Verlängerungen festgelegt ist, Zweifel in Bezug auf die Verhältnismäßigkeit der Maßnahme aufwerfen kann. Die Kommission würde Informationen in Bezug darauf begrüßen, ob solche Anordnungen und Verlängerungen gesetzlich den Höchstfristen unterliegen und falls nicht, in welchem Maße die deutschen Behörden davon ausgehen, dass die oben genannte Bestimmung ausreichenden Schutz in Bezug auf die Verhältnismäßigkeit von Anordnungen und Verlängerungen gewährt.

Personen, deren Kommunikation gemäß § 53 Absatz 1 Satz 1 Nummer 1 bis 5 der Strafprozessordnung der Pflicht des Berufsgeheimnisses unterliegt – § 100g Absatz 4 der Strafprozessordnung

Die Kommission geht davon aus, dass die Vorratsdatenspeicherung auch für Personen gilt, deren Kommunikation gemäß § 53 Absatz 1 Satz 1 Nummer 1 bis 5 der Strafprozessordnung der Pflicht des Berufsgeheimnisses unterliegt. Infolgedessen werden solche Daten als Beweismittel ausgeschlossen, aber die Daten von Personen, deren Kommunikation der Pflicht des Berufsgeheimnisses unterliegt, werden dennoch auf Vorrat gespeichert. Gleichzeitig stellt die Kommission fest, dass gemäß § 113b Absatz 6 des Telekommunikationsgesetzes, der wiederum auf § 99 Absatz 2 des Telekommunikationsgesetzes Bezug nimmt, eine Ausnahme hinsichtlich der Speicherung und Vorratsspeicherung von bestimmten Kategorien von Datensubjekten vorgesehen ist. Die Kommission nimmt die Erläuterung der deutschen Behörden zur Kenntnis, dass es nicht möglich wäre, alle Personen zu registrieren, deren Kommunikation gemäß § 53 Absatz 1 Satz 1 Nummer 1 bis 5 der Strafprozessordnung der Pflicht des Berufsgeheimnisses unterliegt. Dennoch würde die Kommission weitere Informationen dahingehend begrüßen, warum Personen, deren Kommunikation der Pflicht des Berufsgeheimnisses unterliegt, anders als die Behörden und Institutionen behandelt werden, die von der Ausnahme nach § 113b Absatz 6 des Telekommunikationsgesetzes umfasst werden, wenn sie sich in einer vergleichbaren Situation befinden.

Außerdem ist unklar, ob verfahrenstechnische Anforderungen bestehen, um zu gewährleisten, dass die Daten von Personen, deren Kommunikation gemäß § 53 Absatz 1 Satz 1 Nummer 1 bis 5 der Strafprozessordnung der Pflicht des Berufsgeheimnisses unterliegt, wirksam vor dem Risiko des Missbrauchs und vor rechtswidrigem Zugriff auf die Daten und deren Nutzung geschützt werden. Die Kommission würde weitere Angaben zu diesem Punkt begrüßen.

Mitglied der Kommission
Europäische Kommission

Allgemeine Kontaktinformationen Richtlinie 98/34
Fax: +32 229
email: grow-dir83-189-central@ec.europa.eu