

Fragenkatalog zum Expertenworkshop „Erfüllungsaufwand Verkehrsdaten- speicherung“

Vorbemerkung

Wir bedanken uns für die Einladung zur Anhörung des Nationalen Normenkontrollrates und für Ihre Fragen zu den mit dem geplanten Gesetz zur Vorratsdatenspeicherung einhergehenden Kosten für die zur Umsetzung verpflichteten Unternehmen.

Hinweisen möchten wir in diesem Zusammenhang jedoch darauf, dass die konkreten Aufwendungen letztlich in hohem Maße von den Anforderungen des Katalogs der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation und Eisenbahnen (BNetzA) abhängig sein werden. Nichts desto trotz sind auch schon im Gesetzentwurf viele Regelungen enthalten, die zu zusätzlichen Kosten führen werden, auf die wir im Folgenden im Rahmen der Beantwortung Ihres Fragenkatalogs gerne eingehen.

1. Wie viele Telekommunikationsunternehmen sind betroffen, nur solche mit Sitz in Deutschland?

Der Regierungsentwurf für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten verpflichtet ohne jegliche Differenzierung alle Erbringer öffentlich zugänglicher Telekommunikationsdienste. Neben den Netzbetreibern sind daher auch Service Provider vom Gesetzentwurf erfasst.

Gemäß § 6 TKG sind alle Unternehmen, die gewerblich öffentliche Telekommunikationsnetze oder Telekommunikationsdienste betreiben, verpflichtet, sich bei der BNetzA anzumelden. Die auf der Internetseite der BNetzA veröffentlichte Liste mit allen gemeldeten Unternehmen enthält rund 3.500 Firmen:

http://www.bundesnetzagentur.de/cln_1421/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/meldepflicht.html?nn=268208

Nicht ersichtlich ist aus dieser Liste heraus, wie viele Unternehmen Netze und Dienste betreiben, die für die Vorratsdatenspeicherung relevant sind. Eine exakte Zahl der betroffenen Unternehmen müsste jedoch von der BNetzA zu bekommen sein.

An dieser Stelle möchten wir gerne auf das Problem aufmerksam machen, dass die Einbeziehung von Service Providern in den Regelungsbereich des Gesetzentwurfes dazu führt, dass hier eine Verpflichtung zur Beauskunftung von Gesprächsdaten geschaffen wird (z. B. Standortdaten, Verbindungsdaten bei Prepaid-Karten, Verbindungsdaten bei eingekauften Flatrate-Tarifen), die

originär nur bei Betrieb eines eigenen Netzes anfallen und daher gerade nicht bei Service Providern. Insofern sollten Service Provider daher von der Verpflichtung zur Beauskunftung ausgenommen werden und befugt sein, bezüglich dieser Daten an den jeweiligen Netzbetreiber zu verweisen. Ansonsten müssten diese Daten beim jeweiligen Netzbetreiber angefordert werden. Der fortwährende Austausch und die damit einhergehende Doppelspeicherung würden daher zu einem vermeidbaren Mehraufwand sowie zu einer unnötigen Erhöhung des Risikos im Hinblick auf die Datensicherheit führen. Die Regelung in § 113a Abs. 1 Satz 2 TKG-E bedarf daher einer entsprechenden Anpassung.

2. Weshalb und inwieweit hängen der einmalige und/oder der wiederkehrende Aufwand der Telekommunikationsunternehmen von der Größe des jeweiligen Unternehmens ab?

Ein Teil der Kosten entsteht unabhängig von der Größe des Unternehmens, dies gilt insbesondere für gewisse Grund-Investitionskosten. Ein anderer Teil der Kosten ist dagegen abhängig von der Größe des Unternehmens bzw. von der Anzahl seiner Kunden. Je mehr Kunden über die Systeme eines Providers laufen, umso größer sind die Anforderungen an die Hardware und damit steigen die Kosten für die benötigten Systeme und die benötigte Stellfläche. Hinzu kommt, dass je größer die Anzahl der Teilnehmer eines Anbieters ist, desto häufiger werden Auskünfte seitens der Behörden angefragt, die mit entsprechender Personalstärke bearbeitet werden muss. Bei Service Providern ist der Aufwand zudem auch von der Frage abhängig, über wie viele Netzbetreiber die Dienste angeboten werden. Je mehr Netzbetreiber betroffen sind, desto größer ist der Einigungs- und Implementierungsaufwand.

3. Lassen sich Größengruppen bilden und wenn ja, nach welchen Kriterien und mit welchen Aufwandsgrößenordnungen?

Da die anfallenden Daten aus dem Bereich des Mobilfunk umfangreicher sind (z. B. Standortdaten, Funkzellen), als die Daten der VoIP- und Festnetzanbieter, könnte diesbezüglich eine erste Kategorisierung stattfinden. Eine zweite Kategorisierung könnte dann nach Anzahl der Kunden erfolgen.

4. Unterscheiden sich die Aufwände für Speicherung und Umgang mit Verkehrsdaten von den entsprechenden Aufwänden für Standortdaten?

Jede Ausweitung von Speicherverpflichtungen, zumal in separaten und speziell gesicherten Systemen, erzeugt zusätzlichen Aufwand sowohl was Investitionen angeht als auch im laufenden Betrieb. Die zusätzliche Speicherung von Standortdaten bedeutet insofern auch einen zusätzlichen Aufwand, auch wenn über die genaue Relation zu anderen Verkehrsdaten derzeit keine Angabe gemacht werden kann. Grundsätzlich gilt auch: je differenzierter eine Speicherverpflichtung ausgestaltet ist, desto aufwändiger und zeitintensiver wird ihre Umsetzung in den verpflichteten Unternehmen sein.

5. Können Telekommunikationsunternehmen auf eine frühere oder aktuell genutzte Speicherung von Verkehrsdaten und Standortdaten und die dafür vorhandene Technik zurückgreifen?

Die für die kurze Zeit bis zur Entscheidung des Bundesverfassungsgerichts sehr aufwändig implementierten Systeme sind aufgrund der technischen Weiterentwicklung allenfalls zu einem kleinen Teil noch nutzbar. Zu bedenken gilt es auch, dass das Bundesverfassungsgericht insbesondere auch mangelnde Sicherheit gerügt hat. In den §§ 113d-113g TKG-E werden daher erstmals technische Anforderungen formuliert, die vorher so nicht bestanden haben. Weiter erschwerend kommt hinzu, dass die Anforderungen letztlich erst von der Bundesnetzagentur konkretisiert werden sollen, was heutige Aussagen natürlich erschwert. Insgesamt gesehen wird für den weit überwiegenden Teil der Systeme neu investiert werden müssen.

6. Lassen sich die Anforderungen an den Umgang und die Gewährleistung der Sicherheit der gespeicherten Daten bereits konkretisieren (Anforderungskatalog)?

In § 113 f TKG-E ist vorgesehen, dass der Anforderungskatalog erst durch die Bundesnetzagentur im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt wird.

7. Wenn Sicherheit und Umgang mit den gespeicherten Daten dem Stand der Technik entsprechen müssen: Wie ist dieser zu beschreiben und welche Aufwände ergeben sich daraus?

Im Unterschied zu den „anerkannten Regeln der Technik“ meint der Begriff „Stand der Technik“ die „Speerspitze“ der Technik, also sozusagen das Neueste vom Neuen. Logisch hiermit verknüpft sind die Tatsachen, dass sich der „Stand der Technik“ laufend ändert, nicht immer hinreichend bestimmbar ist, sehr teuer und zudem nicht ausreichend erprobt. Insofern sehen wir die Anforderung „Stand der Technik“ als äußerst problematisch und änderungsbedürftig an.

Zudem stellt sich in diesem Zusammenhang die Frage der Verantwortlichkeiten. Aus Sicht des VATM darf die Verantwortung für die Definition der „nach dem Stand der Technik höchstmöglichen Sicherheit“ für die Speicherung der Daten nicht allein den TK-Diensteanbietern übertragen werden. Vielmehr sollte auf Grundlage eines Sicherheitskonzepts, das seitens der jeweiligen Unternehmen entwickelt und bei zuständigen Behörden hinterlegt wird, eine haftungsrechtliche Privilegierung zu Gunsten der TK-Diensteanbieter geschaffen werden, um ökonomische Risiken für die Unternehmen im Zusammenhang mit der Vorratsdatenspeicherung auszuschließen.

Was die zu erwartenden Aufwände angeht, so sind die von Unternehmen zu Unternehmen sehr unterschiedlich. Einige Unternehmen gehen von mittleren sechsstelligen Beträgen aus, andere sogar – abhängig von der genauen Ausgestaltung des Anforderungskataloges der BNetzA – sogar von sieben- bis achtstelligen Eurobeträgen. Grundsätzlich gilt selbstverständlich, dass die Kosten deutlich steigen, je häufiger die Systeme aktualisiert und angepasst werden müssen.

8. Weshalb, inwieweit und wofür entstehen höhere Aufwände gegenüber den bereits bestehenden Anforderungen aus den geltenden §§ 109, 109a, 110, 112 und 113 TKG?

Es gibt eine ganze Reihe von neuen Regelungstatbeständen, die zu deutlich höheren Kosten führen werden:

Ein wichtiger Punkt betrifft den Umstand, dass keine de-minimis-Regelung mehr vorgesehen ist und so auch Unternehmen mit nur sehr kleinem Endkundenkreis genauso verpflichtet werden, wie Unternehmen mit Millionen von Kunden. Darüber hinaus sieht der Gesetzentwurf vor, dass künftig auch Daten gespeichert werden müssen, die nicht entgeltrelevant sind. Hauptursache für

erhöhte Aufwände dürfte jedoch die im TKG-E vorgesehene separate Vorhaltung der erhobenen Daten sein. Je nach gesetzlicher Grundlage sind hier unterschiedliche Vorgaben zu beachten, die für die jeweiligen Daten anzuwenden sind. Die gesamte Umsetzung in großen IT-Systemen ist bereits von Seiten der Programmierung und der Beschaffung von entsprechenden Anlagen her eine große Herausforderung. Darüber hinaus sind auch Prozesse neu zu erstellen, die mit hohem Personalaufwand verbunden sind. Ein Beispiel hierfür ist das **4-Augen-Prinzip** (§113d Nr. 5. TKG-E „Mitwirkung von mindestens zwei Personen beim Zugriff“).

9. Inwieweit folgen aus dem Gebot der Speicherung im Inland neue einmalige und jährliche Aufwände?

Hinsichtlich der EU-Konformität ist die vorgesehene Verpflichtung zur Speicherung der erhobenen Daten allein in Deutschland („im Inland“ §113b (1) TKG-E) kritisch zu bewerten. Es ist fraglich, ob vor dem Hintergrund des EU-Binnenmarktes eine solche Regelung EU-rechtlich Bestand haben kann. Jedenfalls wäre eine sichere Speicherung ohne Frage auch zumindest innerhalb der EU ohne weiteres realisierbar. Insbesondere aus Sicht der paneuropäisch agierenden Unternehmen dürfte diese Regelung einen unverhältnismäßigen Eingriff in Unternehmergrundrechte darstellen. Die in der Gesetzesbegründung (S. 43) ausgeführten Erwägungen zur Rechtfertigung dieser Regelungen sind in Anbetracht des harmonisierten Rechtsrahmens für Datenschutz, und insbesondere nach Start der Trilogverhandlungen zur Datenschutzverordnung, nicht überzeugend. Unabhängig von diesen rechtlichen Überlegungen würde die Verpflichtung zur Speicherung im Inland gegenüber einer paneuropäischen Lösung für einige große Unternehmen zu laufenden Mehraufwendungen führen.

10. Inwieweit folgen aus dem Gebot einer Speicherung getrennt vom Internet – wenn auch nicht physikalisch – neue einmalige und jährliche Aufwände?

Die in § 113d Nr. 3 TKG-E vorgesehene Speicherung auf „vom Internet entkoppelten Datenverarbeitungssystemen“, wirft große Fragen hinsichtlich der datenmäßigen Anbindung auf, um überhaupt speichern und ggf. beaskunften zu können. So werden die Daten einerseits zunächst in Netzen aggregiert, die nicht vom Internet entkoppelt sind. Ferner müssen die Verkehrsdatensätze

dann aber auch in Systemen gespeichert werden, auf welche über Netzwerke und sichere VPN-Verbindungen standortunabhängig zugegriffen werden kann. Andernfalls wäre eine Beauskunftung im Sinne des § 113 c Abs. 1 TKG-E nur am Standort des Rechenzentrums möglich, in dem die Daten gespeichert sind. Zuletzt würde eine solche Regelung auch durch die Übermittlung nach § 1 Abs. 3 TKG-E iVm § 110 Abs. 3 TKG ad absurdum geführt werden, da eine solche Übertragung von Daten gerade über gesicherten VPN-Internetverbindungen im Sinne der „Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftersuchen für Verkehrsdaten“ realisiert wird. Die in dieser Regelung angelegte Komplexität führt in der konkreten Umsetzung auf jeden Fall zu deutlichen zusätzlichen Aufwänden. Entscheidend wird hier jedoch letztlich der Anforderungskatalog der BNetzA sein, aus dem sich alle Details des aufzubauenden Systems ergeben werden.

11. Inwieweit folgen aus den gebotenen Protokollierungen besondere Aufwände?

Auch hier hängt der genaue Aufwand vom Anforderungskatalog der BNetzA ab. Relevant sind die Fragen, auf welche Weise die Daten gesichert werden müssen, wer Zugriff auf die Daten hat und wie genau die Abläufe festgeschrieben werden.

12. Inwieweit folgen aus dem Gebot der irreversiblen Löschung nach Ablauf der Speicherfristen besondere Aufwände?

Wegen der unterschiedlichen Speicherfristen entsteht ein erhöhter Programmieraufwand für eine entsprechende Löschroutine. Da ein einfaches „Löschen“ oder „Überschreiben“ der Daten vermutlich nicht ausreichend sein wird, wird eine von der BNetzA näher zu spezifizierende Software oder ein zu spezifizierendes Verfahren notwendig sein, dass dann von den Unternehmen implementiert werden muss.

13. Erscheinen die im Justizvergütungs- und -entschädigungsgesetz vorgesehenen Pauschalen für Auskünfte über Verkehrsdaten kostendeckend?

Auch wenn die entstehenden Kosten nicht exakt beziffert werden können, ist absehbar, dass die vorgesehenen Pauschalen nicht kostendeckend im Hinblick auf die Erhebung, Speicherung und Beauskunftung von Daten sein werden. Erst recht ist natürlich eine Refinanzierung der Investitionskosten sowie der laufenden Kosten nicht möglich. Ein weiterer heute noch nicht bekannter Umstand betrifft das zu erwartende Anfragevolumen. Angesichts der steigenden Komplexität der Systeme, der deutlich erhöhten Anforderungen an die Prozesse (z. B. 4-Augen-Prinzip) und eines grundsätzlich zu erwartenden steigenden Anfragevolumens wäre eine Erhöhung der Pauschalen zur Kostendeckung voraussichtlich notwendig.

14. Welche zusätzlichen – einmaligen und/oder wiederkehrenden – Aufwände erwarten die BNetzA, das BSI, das BAMt für Justiz und die BfDI, um den ihnen übertragenen Aufgaben gerecht zu werden?

Diese Frage ist nicht an den VATM gerichtet.

15. Lassen sich die Mehraufwände der Gerichte, Staatsanwaltschaften und Gefahrenabwehrbehörden der Länder durch die neuen Auskunftsfälle und die gesteigerten Anforderungen an die Begründungen von Auskunftersuchen sowie die Begründung der Zurückstellung von Benachrichtigungen der Beteiligten abschätzen (wahrscheinliche Fallzahlen und Zeitaufwand je Fall)?

Diese Frage ist nicht an den VATM gerichtet.

Berlin, 17. Juli 2015