Stellungnahme der Verbände BREKO, BUGLAS und VATM zum Entwurf eines Anforderungskataloges nach § 113f TKG zur Umsetzung des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Nach § 113 f. des Gesetzes zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten ("Vorratsdatenspeicherung") vom 10.12.2015 , BGBl. I S.2218) erstellt die Bundesnetzagentur (BNetzA) im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Anforderungskatalog zur Einhaltung der in §§ 113 b bis 113 e genannten Standards für die Datensicherheit und Datenqualität. Einen entsprechenden Entwurf für diesen Anforderungskatalog (Stand: 11.05.2016) hat die BNetzA im Amtsblatt veröffentlicht.

Die Verbände BREKO, BUGLAS und VATM vertreten mehr als 90 Prozent der im Wettbewerb zur Deutschen Telekom AG stehenden Netzbetreiber und damit einen wesentlichen Teil der Adressaten, an die sich die Speicherpflicht und die Anforderungen an die Datensicherheit und Datenqualität richten.

Die Stellungnahme erhebt schon wegen der für einen technisch sehr komplexen Sachverhalt keinen Anspruch auf Vollständigkeit. Der Anforderungskatalog weist unserer Ansicht nach an vielen Stellen Unschärfen und Widersprüche auf, welche dringend nachgebessert werden müssen. Auch besteht an vielen Stellen noch deutlicher Klärungsbedarf.

I. Allgemeine Ausführungen

1. Kostentragung

Wie bereits in anderen Regelungen, z.B. bei der Umsetzung von Überwachungsmaßnahmen und dem automatisierten Auskunftsverfahren (§ 110 TKG) oder dem automatisierten Auskunftsverfahren (§ 112 TKG) sollen die TK-Unternehmen auch im Rahmen der Vorratsdatenspeicherung die erheblichen Kosten für Anforderungen des Katalogs komplett alleine tragen. Die Anbieter wenden sich natürlich nicht gegen eine notwendige Mitwirkung bei der Erfüllung öffentlicher Aufgaben, wie der Gefahrenprävention oder der Strafverfolgung und gegen die Definition der *erforderlichen* Schnittstellen und Systeme (was nicht bedeutet, dass es immer die in der Regel teure technische Ideallösung sein muss).

Allerdings handelt es sich dabei um die Erfüllung öffentlicher Aufgaben, deren Kosten letztlich auch durch die öffentliche Hand getragen werden müssen. Dies gilt auch insbesondere deshalb, weil inzwischen die Summe der aus der Erfüllung öffentlicher Aufgaben resultierenden Belastungen die TK-Wirtschaft insgesamt überfordern und für kleinere und mittlere Unternehmen existenzgefährdend ist.

Anders als bei der früheren Gesetzgebung werden die Daten für die Vorratsdatenspeicherung gerade nicht mehr für eigene Zwecke und auf ohnehin vorhandenen Infrastrukturen gespeichert, sondern nach den Vorgaben des BVerfG muss eine komplett neue und separate Infrastruktur mit äußerst hohen Sicherheitshürden aufgebaut werden. Daher belasten die im Anforderungskatalog vorgesehenen Maßnahmen die Unternehmen nicht nur mit hohen zusätzlichen Einrichtungskosten, z.B. für die redundanten Speichersysteme für die separate Speicherung von Verkehrsdaten und Abrechnungsdaten, redundante Backup-Systeme mit gleichen Sicherheitsstandards, die Kosten für Firewalls, Kryptosysteme und ggf. notwendige bauliche Maßnahmen, sondern auch mit hohen laufenden Kosten, insb. für das erforderliche Personal (Stichwort: „4-Augen-Prinzip“). Die Einrichtungskosten sollen die Anbieter dabei komplett alleine tragen. Hinsichtlich der laufenden Kosten könnte zwar eine Entschädigung nach § 23 des Justizvergütungs und-Entschädigungsgesetz (JVEG geltend gemacht werden, allerdings stehen die Entschädigungssätze hier in keinem Verhältnis zu den tatsächlich entstehenden Personalkosten und müssten dringend angepasst werden. Insgesamt ist eine angemessene, d.h. kostendeckende, Entschädigung für alle Anbieter sowohl hinsichtlich der Implementierungskosten als auch mit Blick auf die laufenden Kosten vorzusehen.

Den erheblichen verfassungsrechtlichen und moralischen Bedenken gegen die Vorratsdatenspeicherung soll offenbar begegnet werden, indem ein extrem hohes Maß an Sicherheit verlangt wird. Wenn dies so gewünscht wird, dann darf der Gesetzgeber hier die komplette wirtschaftliche Last einer originär staatlichen Aufgabe nicht einer einzelnen Branche zuweisen.

Zudem werden die TK-Unternehmen gegenüber den OTT-Anbietern erheblich benachteiligt, da diese zumindest nach der Praxis von der Vorratsdatenspeicherung ausgenommen sind. Im Wettbewerb gegen die OTT-Dienste verlieren die TK-Unternehmen daher unzulässig durch die Verpflichtung zur Vorratsdatenspeicherung.

Der Kriterienkatalog sieht vor, dass Daten durchgängig verschlüsselt und nur gesichert übertragen werden. Diese Anforderungen erscheinen jedoch nur dann gerechtfertigt, wenn dieses Prinzip auch in den nachgelagerten Schnittstellen und insbesondere beim Zugriff der berechtigten Stellen (bS) auf diese Daten konsequente Anwendung finden. Über entsprechende Standards zur Datensicherung bei den abfragenden Sicherheitsbehörden ist jedoch nichts bekannt. Insofern sollte im Rahmen der TKÜV und TR TKÜV der Zugriff auf die von den Netzbetreibern ohnehin vorgehaltene und von den berechtigten Stellen derzeit kaum genutzte ETSI/ESB-Schnittstelle begrenzt werden.

2. Sicherheit und Vollständigkeit der Daten

Es ist anzumerken, dass TK-Anbieter keine Ermittlungsbehörden sind und die hier eingesetzten Systeme primär der Abwicklung von TK-Diensten dienen. Insofern dürfen an die TK-Unternehmen keine strengeren Anforderungen an die Richtigkeit und Vollständigkeit von Daten gestellt werden, als dies allgemein auf Grund der geltenden Gesetze ohnehin der Fall ist.

3. Einführung einer De-Minimis-Regelungen

§ 113a Abs.2 TKG sieht lediglich eine allgemeine Härtefallregelung vor, nach der eine „angemessene Entschädigung“ an Unternehmen zu zahlen ist, für die Umsetzung der Vorgaben eine „unbillige Härte“ darstellen würde. Über entsprechende Anträge entscheidet die BNetzA. Dies bedeutet aber, dass die hiervon betroffenen Anbieter hinsichtlich der Implementierungskosten und der operativen Kosten zunächst mindestens in Vorleistung gehen müssen. Da zudem keine Kriterien , kein Verfahren und keine Fristen für die Entscheidung über die Anwendung der Härtefallregelung definiert sind und auch nichts zur Höhe der „angemessenen Entschädigung“ ausgesagt wird, werden gerade kleinere und mittlere Unternehmen kaum in der Lage sein, die hohen Anforderungen des Kataloges über wirtschaftlich umzusetzen und über einen längeren Zeitraum vorzufinanzieren. Angesichts der beschriebenen Unsicherheiten über das „Ob“, „Wie“ und „Wann“ einer Härtefall-Entschädigung wird sich auch eine Kreditfinanzierung kaum realisieren lassen (abgesehen von den Kosten für einen entsprechenden Kredit). Die Entscheidung über die Anwendung der Härtefallklausel kann dann gerade für kleinere und mittlere Unternehmen zu spät kommen.

Sinnvoller wäre es daher, Anbieter mit weniger als 10.000 Teilnehmern mindestens von den kostenintensiven Anforderungen des Kataloges auszunehmen. Eine entsprechende De-Minimis-Regelung findet sich mit Blick auf die Umsetzung technischer Maßnahmen zur Überwachung bereits in § 3 Abs.2 Nr.5 TKÜV und hat sich dort bewährt. Eine derartige Ausnahme wäre auch gut vertretbar, weil davon auszugehen ist, dass es gegenüber kleineren Anbietern mit weniger als 10.000 Kunden nur zu sehr wenigen Anfragen kommen wird, so dass der hohe Einrichtungs- und operative Aufwand, den die Umsetzung des Anforderungskataloges bedeutet, hier besonders unangemessen erscheint.

Die Anforderungen des Kriterienkatalogs stellen aber nicht nur kleinere TK-Anbieter vor Herausforderungen, sondern zieht auch für bundesweit agierende Anbieter erhebliche Anforderungen an Implementierung und Betrieb nach sich. Daher wäre auch eine Marginaliengrenze je Dienst wünschenswert, wie dies im Bereich der Gestaltung der Überwachbarkeit implementiert ist.

4. Unterschiedliches Schutzbedürfnis für Telefonie-Verkehrsdaten und IP-Verkehrsdaten

Der Anforderungskatalog berücksichtigt nicht das grundsätzlich unterschiedliche Schutzbedürfnis von Telefonie-Verkehrsdaten und IP-Verkehrsdaten.
Während es sich bei Telefonie-Verkehrsdaten um statische Zuweisungen von Rufnummern handelt, sind IP-Verkehrsdaten zumindest der Internetnutzers zu mehr als 90 % dynamische Adressvergaben bei Nutzung IPV4. Dies gilt auch bei IPV6-Adressen. Inhaber von Telefonnummern lassen sich relativ schnell z. B.im Rahmen einer Google-Suche feststellen. Eine IP-Adresse lässt sich stets nur bis zum LIR (Local Internet Registry) aufgrund der RIPE-Zuweisungen zurückverfolgen. Auch die Benutzerkennung, die in der Regel aus Zahlen kombiniert mit Buchstaben und Sonderzeichen besteht, erlaubt keinen Rückschluss auf den Internetnutzer. Aus diesem Grund wäre mindestens mit Blick auf die IP-Verkehrsdaten eine Überprüfung der Erforderlichkeit des Schutzniveaus vorzunehmen.

5. Auslagerung an externe Dienstleister muss ermöglicht werden

Um die ohnehin schon sehr kritische Unwirtschaftlichkeit der im Anforderungskatalog adressierten Maßnahmen abzumildern, ist es zwingend erforderlich, dass die Möglichkeit der Auslagerung an externe Dienstleister, die § 113 a Abs.1 TKG offensichtlich vorgesehen ist, durch einzelne Anforderungen nicht verhindert wird. Vielen Anbietern wird eine Umsetzung des Anforderungskatalogs, wenn überhaupt, nur möglich sein, wenn über die Einschaltung eines externen Dienstleisters Kosten- und Skalierungseffekte erzielt werden können. Die Maßnahmen sind daher jeweils auf ihre Umsetzbarkeit durch Dritte zu prüfen.

6. Fehlerbehebung: Fehlende Test- und Analysemöglichkeit

Die Systeme zur Vorratsdatenspeicherung sind durch den Gesetzgeber in Ihrer Verwendung streng begrenzt. Ein Einsatz zu Testzwecken oder zur Eingrenzung von Fehlern durch den Netzbetreiber oder Systemhersteller ist durch die Absicherung und die konsequente Verschlüsselung der Daten nahezu unmöglich. Auch die äußerst enge gesetzliche Zweckbindung gibt solche Anwendungsfälle kaum her. Daher stehen die TK-Anbieter sowohl technisch als auch rechtlich vor Herausforderungen, da bei möglichen Fehlern kaum eine Möglichkeit zur Fehleranalyse und –behebung besteht. Hier wären dringend Vorgaben wünschenswert, unter denen zu Testzwecken bzw. zur Fehlerbehebung gesichert auf die Daten zugegriffen werden kann und diese entsprechend genutzt verwendet werden dürfen

7. Einführung angemessener Umsetzungsfristen

Die vorgesehene Frist von einem Jahr zur Umsetzung der hohen Anforderungen aus dem Katalog ist zu kurz bemessen. Da es sich um ausschließlich nationale Anforderungen handelt, stehen zum Teil die erforderlichen Systeme heute noch gar nicht am Markt zur Verfügung und werden wegen der erheblichen Rechtsunsicherheiten im Zusammenhang mit der Einführung der Vorratsdatenspeicherung seitens der Hersteller – nach deren eigener Aussage – vor Abschluss der laufenden verfassungsrechtlichen Prüfung auch nicht entwickelt werden. Es ist daher ein wesentlich großzügigerer Umsetzungszeitraum vorzusehen, der die laufende Verfassungsbeschwerde, die Zeit für die Entwicklung der notwendigen Systeme durch die Hersteller, die Zeit für die Implementierung der Systeme durch die Anbieter und die erforderliche Schulung des Personals angemessen berücksichtigt.

II. Anmerkung zu einzelnen Regelungen

Zu Ziffer 4.1 Gewährleistung eines besonders hohen Standards der Datensicherheit

„Nach dieser Einrichtung stehen dem Unternehmen Verkehrsdaten zur Verfügung, die nach §§ 96 ff. TKG gespeichert werden dürfen (nicht Gegenstand dieses Anforderungskatalogs) und Verkehrsdaten, die nach § 113b TKG gespeichert werden müssen. […]“

Diese Aussage schließt per se die Verwendung irgendwelcher Billingdaten bzw. –systeme als Quelle für VDS-relevante Daten aus, da dort nur Verkehrsdaten nach § 96 TKG gespeichert werden. In Kap. 5.1.1 wird aber das Abrechnungssystem als möglicher Ursprung benannt und im Schaubild auf S. 14 explizit hervorgehoben. Es handelt sich insoweit um widersrpüchliche Regelungsgehalte.

„Diese Verkehrsdaten müssen soweit wie möglich vor Beeinträchtigungen oder Missbrauch bewahrt werden.“

Bedeutet die Formulierung an dieser wie auch anderer Stelle, dass Maßnahmen nach dem aktuellen Stand der Technik gefordert sind oder soll der anderweitig im Text zu findende direkte Verweis auf diesen unbestimmten Rechtsbegriff (wie bspw. in Kap. 5.1.5, S.13 oben) implizieren, dass sonst gerade ein höherer oder weniger hoher Maßstab anzuwenden ist?

Zu Ziffer 5.1.1 Allgemeine Anforderungen

„speicherpflichtige Verkehrsdaten nach §113b TKG“

Sollen diese nach Abs. 2 Satz 5 auch irgendwie geartete OTT-Internettelefoniedienste (z.B. Skype, Whatsapp, WebRTC, …) enthalten?

Dies hätte zur Folge, dass das Gesetz nicht in dieser Form umsetzbar wäre, da explizit Inhalte von IP-Kommunikation bzw. Internetzugangsdiensten von der Speicherung und Auswertung ausgenommen sind. Sogenannte Over-The-Top (OTT) Dienste sind jedoch nur mittels Auswertung des Datentraffics auffindbar, was nicht mit deutschen Datenschutzvorschriften vereinbar ist.

Ansonsten müssten die OTT-Dienstleister mit verpflichtet werden, was bei im Ausland beheimateten Anbietern schwer umsetzbar sein wird, sonst aber gegen die Diskriminierungsfreiheit verstoßen würde.

„Es müssen Verkehrsdaten ankommender und abgehender Verbindungen gespeichert werden. Die Verkehrsdaten müssen ihren Ursprung direkt aus den Abrechnungs-, Log- oder Signalisierungsdaten haben."

Abrechnungsdaten im Sinne von CDRs enthalten niemals ankommende Verbindungen und liegen als Auswertung des Billingsystems nur monatlich im Nachhinein vor. Dies ist für kurzfristige Auskunftsersuchen somit unzureichend bzw. ggf. nicht vollständig zulieferbar. Es sollte daher eine Klarstellung dahingehend erfolgen, dass Abrechnungsdaten für ankommende Verbindungen nicht existieren und daher auszunehmen sind.

„Die Speichereinrichtungen müssen über eine ausreichende Leistungsfähigkeit verfügen, um alle anfallenden Verkehrsdaten und eingehenden Abfragen verarbeiten zu können."

Hier ist eine Klarstellung erforderlich, was unter einer „ausreichenden Leistungsfähigkeit" zu verstehen ist. Gibt es hierzu klarere Vorgaben, auch hinsichtl. der Verfahrensweise?

„…ist deren Richtigkeit und Vollständigkeit durch regelmäßige Prüfungen sicherzustellen."

An welche Zeiträume kann man sich hier bezüglich der Regelmäßigkeit anlehnen, was wir als angemessen erachtet?

Zu Ziffer 5.2.1 Grundsätzliche Architektur der Anlagen

Ist es auch möglich bzw. rechtlich legitim das ganze VDS-System oder zumindest Teile davon einschließlich der organisatorischen Verantwortung hinsichtlich der Verwendung und des Betriebs davon an Erfüllungsgehilfen auszulagern? Dies wäre gerade für kleinere Unternehmen zum Teil überlebensnotwendig.

Mit Hinblick auf obige Anmerkungen zu Kap. 5.1.1 wäre es sinnvoll, den Funktionsblock „Billing-Systeme" mit einem Funktionsblock „VDS-Mediation" zu ersetzen, mind. jedoch

darum zu ergänzen. Eine VDS-Mediation-Funktion übernimmt dabei die Aufgabe, (ggf. redundante) Daten aus den Netzelementen des Providers zu sammeln und zu konsolidieren. Im selben Zug werden Filter (z.B. gleiche Filterlisten nach §99, wie vom Billingsystem verwendet) darauf angewendet. Anschließend führt die VDS-Mediation die gefilterten Daten dem VDS-Speicher über die sogenannte Datendiode zu.

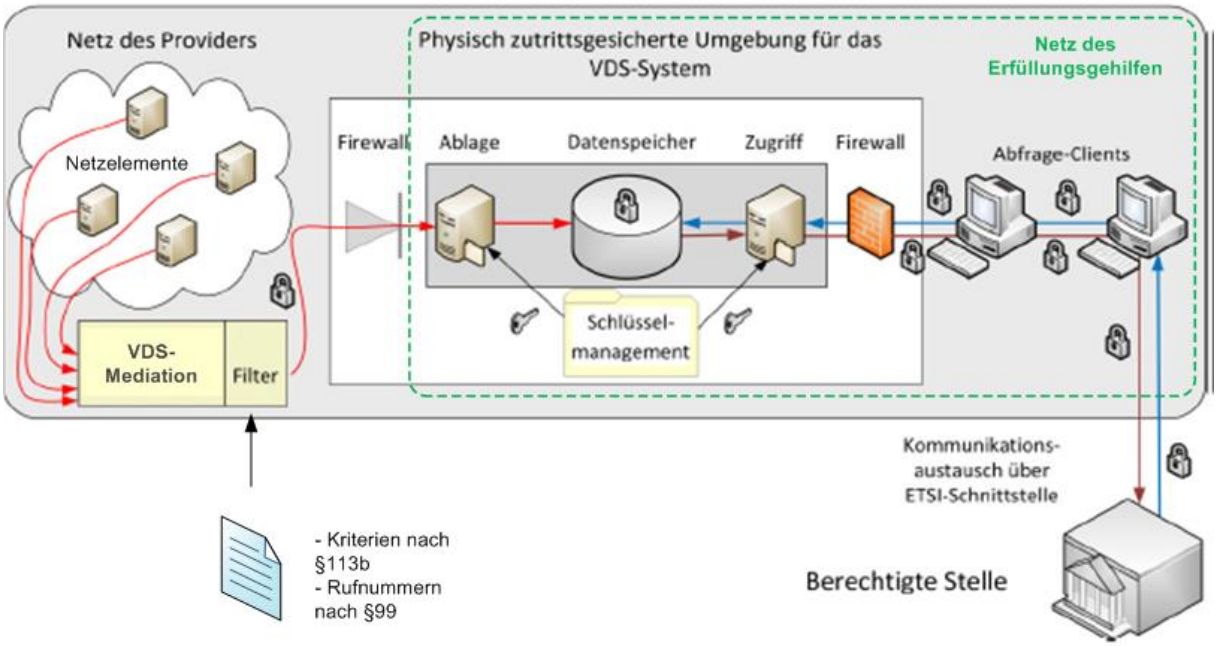
Diese Darstellung ist unserer Einschätzung nach nicht ganz korrekt, aus den folgenden Gründen:

- die VDS speichert nicht das Ergebnis des Billinglaufs

- die VDS speichert Informationen, welche überhaupt nicht abgerechnet werden und somit nach dem Billingprozess auch nicht zur Verfügung stehen (z.B. erfolglose Calls, ankommende Calls)

- bei kleineren Unternehmen wird nur monatlich ein kompletter Abrechnungslauf gemacht, die VDS erfolgt aber kontinuierlich

Siehe zu beiden Kommentaren auch folgende geänderte Abbildung:



Diesbezüglich. könnte eine Zwischenspeicherung im Mediation-Device problematisch sein. §113d TKG bezieht sich auf gespeicherte Daten generell, egal wo. Das könnte ja bedeuten,

dass die VDS-Mediation Teil des VDS-Systems sein müssten. Hier ist eine Klärung der genauen Anforderungen erforderlich.

Weiter stellt sich die Frage, welche Vorgaben es an die Struktur der Daten bei unterschiedlichen Quellsystemen gibt.

Wie erfolgt der Umgang mit redundanten Informationen (z.B. Daten aus mehreren Switchen oder Netzelementen bei einer Verbindung)?

Technische Daten sind ggf. interpretationsfähig (z.B. Gesprächsbeginn oder Rufnummer in lokalem oder globalen Rufnummernformat)

-> bei einer manuellen Auswertung der Anfrage und anschließender Aufbereitung könnte das gefiltert werden

-> bei einer automatisierten Abfrage ist das ggf. problematisch

Zu Ziffer 5.2.2 Besonders sicheres Verschlüsselungsverfahren gemäß §113d Satz 2 Nr. 1 TKG

„Eine Entschlüsselung von Verkehrsdaten ist ausschließlich zum Zwecke der Beauskunftung zulässig […]“

Gilt hier ebenso das Vier-Augen-Prinzip i.S. einer Entschlüsselung durch 2 Mitarbeiter (mit ggf. eigenen Schlüsseln)?

Als Verschlüsselungsverfahren wird eine transparente Datenbankverschlüsselung oder eine Container-Verschlüsselung empfohlen. Hingegen wird zur irreversiblen Löschung von Verkehrsdaten die Löschung der verwendeten Schlüssel als ausreichend betrachtet, wenn diese in ausreichender Granularität (Tagesschlüssel) erzeugt worden sind. Dies ist widersprüchlich: Einerseits wird eine Datensatz-genaue Verschlüsselung mit Tagesschlüsseln gefordert und andererseits transparente Verschlüsselung der gesamten Datenbank.

Zu Ziffer 5.2.3 Speicherung in gesonderten Speichereinrichtungen gemäß §113d Satz 2 Nr. 2 TKG

„Im Datenspeicher des VDS-Systems, auch in einer virtuellen Umsetzung, dürfen darüber hinaus neben den Verkehrsdaten nach § 113b TKG und den notwendigen Systemdateien keine sonstigen Daten gespeichert werden, insbesondere keine Daten für die in § 96 TKG genannten Zwecke."

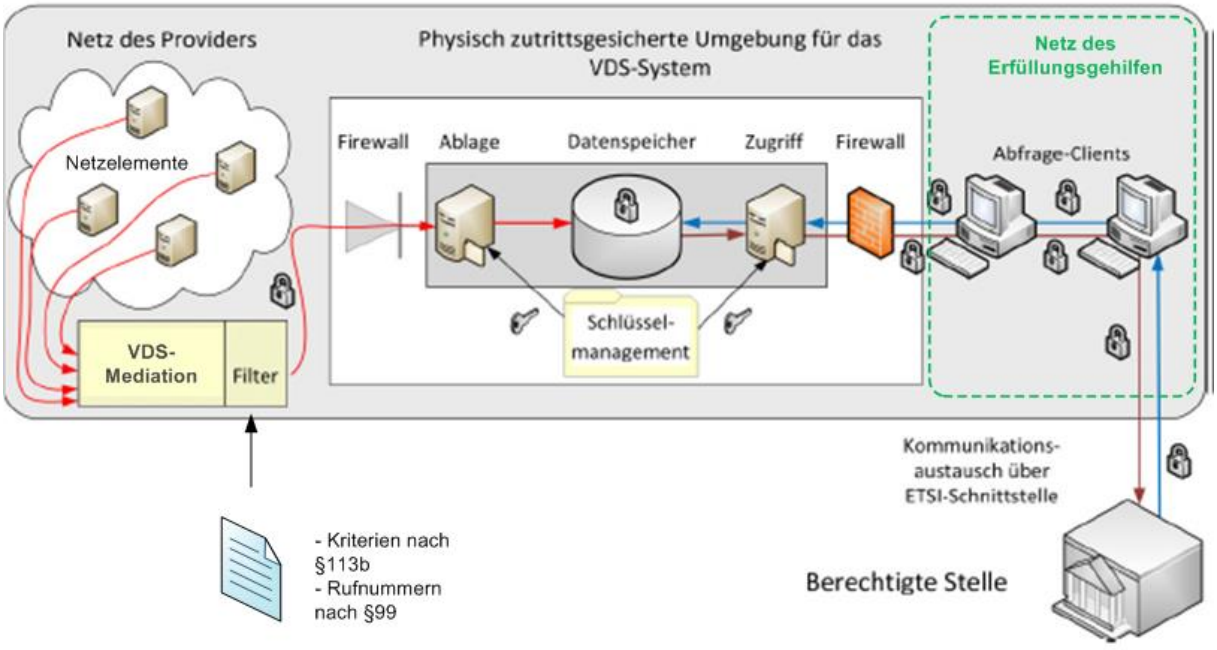
Bezieht sich diese Aussage auf die physikalische Festplatte, die von allen virtuellen Gast-Systemen genutzt wird oder nur die logische HD der dedizierten virtuellen Maschine?

Zu Ziffer 5.2.4 Hoher Schutz vor dem Zugriff aus dem Internet nach § 113d Satz 2 Nr. 3 TKG

„Um die Anfragen der berechtigten Stellen durch ermächtigte Mitarbeiter des Verpflichteten bearbeiten zu können, muss im Vier-Augen-Prinzip ein kontrollierter Zugriff auf den Datenspeicher erfolgen können. […] Die ermächtigten Mitarbeiter müssen aus ihrem Netz verschlüsselt auf das Zugriffssystem zugreifen können."

Darf diese Ermächtigung an Erfüllungsgehilfen i.S. eines externen Dienstleisters erteilt werden?

Diese Frage ist vor allem dann relevant, wenn z.B. nur die Abfragesysteme einschließlich der organisatorischen Aufwände jedoch nicht die Speicherung von Verkehrsdaten nach §113b an externe Erfüllungsgehilfen ausgelagert werden dürfen. Das Bild auf S. 14 würde dann wie



folgt abgewandelt werden müssen:

Gleichermaßen gilt diese Schärfung auch für Kap. 5.2.7, ob die organisatorischen Vorkehrungen komplett ausgelagert werden können an externe Erfüllungsgehilfen.

Köln/Bonn, den 04.Juli 2016