FAQ zur Verkehrsdatenspeicherung

Nr.	FAQ	Antwort

Allgemeine Fragen zur Verpflichtung nach § 113a TKG

1	Gelten sogenannte Reseller als Erbringer öffentlich zugänglicher TK Dienste für Endnutzer?	Ja dann, wenn der sogenannte Reseller öffentlich zugängliche Telefondienste oder Internetzugangsdienste gegenüber Endkunden als Vertragspartnern erbringt.
2	Muss das für die Systemadministration zuständige Personal die deutsche Staatsangehörigkeit besitzen oder einen Wohnsitz in der Bundesrepublik Deutschland haben?	Nein
3	Mit welchen Änderungen am Anforderungskatalog der BNetzA ist aufgrund des EuGH-Urteils zur Verkehrsdatenspeicherung in Schweden und Großbritannien vom 21.12.2016 Aktenzeichen C-203/15, C-698/15 zu rechnen?	Die gesetzlichen Regelungen nach § 113 a bis f TKG haben sich nicht geändert, somit besteht derzeit auch kein Änderungsbedarf am Anforderungskatalog.
4	Muss der Verpflichtete nach § 113a TKG oder der Auftragsdatenverarbeiter (sogenannter Erfüllungsgehilfe) das Sicherheitskonzept nach § 113g TKG bei der BNetzA vorlegen?	Der Verpflichtete nach § 113a TKG muss das Sicherheitskonzept nach § 113g TKG dem Referat IS17 der BNetzA vorlegen. Will der Verpflichtete davon abweichen und einen Dritten mit der Vorlage des Sicherheitskonzeptes nach §109 Abs. 4 TKG, bzw. des erweiterten Sicherheitskonzeptes nach § 113g TKG beauftragen, so hat er die Beauftragung zur Vorlage gegenüber der BNetzA in geeigneter Form nachzuweisen (Erstellungs- und Vorlage-, ggf. auch Umsetzungvollmacht).
5	Wer ist zur Speicherung und Beauskunftung der Verkehrsdaten verpflichtet, wenn die Verkehrsdaten bei einem Betreiber einer Telekommunikationsanlage erzeugt werden, dieser selbst aber kein Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer ist?	Wenn der Betreiber einer Telekommunikationsanlage keine öffentlich zugänglichen Telekommunikationsdienste für Endnutzer erbringt, dann besteht für diesen auch keine Verpflichtung nach §§ 113a bis g TKG.

Nr.	FAQ	Antwort
6	Wie erhält der sogenannte Erfüllungsgehilfe die Liste nach § 99 TKG?	Der sogenannte Erfüllungsgehilfe kann mangels Berechtigung von der BNetzA unmittelbar keine Liste nach § 99 TKG erhalten. Diese Liste erhalten nur die Verpflichteten nach § 113a TKG über ein automatisiertes Verfahren (s. Abschnitt 5.1.2 des Anforderungskatalogs). Falls erforderlich, kann der nach §§ 113a ff. TKG Verpflichtete die Liste nach § 99 TKG an den Auftragsdatenverarbeiter (sogenannten Erfüllungsgehilfen) weiterleiten.

Fragen zum Sicherheitskonzept nach § 113g TKG

7	Was muss durch den nach § 113a Telekommunikationsgesetz (TKG) Verpflichteten bei der Erstellung des Sicherheitskonzeptes gemäß § 113g TKG berücksichtigt werden?	Der nach § 113a Absatz 1 Verpflichtete hat in das Sicherheitskonzept nach § 109 Absatz 4 zusätzlich aufzunehmen, 1. welche Systeme zur Erfüllung der Verpflichtungen aus den §§ 113b bis 113e betrieben werden, 2. von welchen Gefährdungen für diese Systeme auszugehen ist und 3. welche technischen Vorkehrungen oder sonstigen Maßnahmen getroffen oder geplant sind, um diesen Gefährdungen entgegenzuwirken und die Verpflichtungen aus den §§ 113b bis 113e zu erfüllen. Das Sicherheitskonzept ist der Bundesnetzagentur unverzüglich nach dem Beginn der Speicherung nach § 113b und unverzüglich bei jeder Änderung vorzulegen. Bleibt das Sicherheitskonzept unverändert, hat der nach § 113a Absatz 1 Verpflichtete dies gegenüber der Bundesnetzagentur im Abstand von jeweils zwei Jahren schriftlich zu erklären. Das Sicherheitskonzept senden Sie schriftlich an: *Bundesnetzagentur* *Referat IS17* *An der Trift 40* *66123 Saarbrücken* Weitere Hinweise zur Erstellung des Sicherheitskonzeptes im Zusammenhang mit der Verpflichtung zur Speicherung von Verkehrsdaten finden sich im Anforderungskatalog nach § 113g TKG.

FAQ zur Verkehrsdatenspeicherung

Nr.	FAQ	Antwort
8	Gibt es Ausnahmeregelungen bei der Erstellung und Vorlage des Sicherheitskonzeptes?	Es gibt keine Ausnahmen bei der Erstellung und Vorlage des Sicherheitskonzeptes. Alle Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer unterliegen der Verpflichtung.
9	Müssen alle Anforderungen des Anforderungskataloges nach § 113f TKG umgesetzt werden?	Bei der Umsetzung der Verpflichtungen gemäß den §§ 113b bis 113e TKG ist ein besonders hoher Standard der Datensicherheit und Datenqualität zu gewährleisten. Die Einhaltung dieses Standards wird vermutet, wenn alle Anforderungen des Anforderungskataloges erfüllt werden. Sofern einzelne oder mehrere technische Vorkehrungen und sonstige Maßnahmen im Sicherheitskonzept nicht entsprechend des Anforderungskataloges umgesetzt sind, muss der Verpflichtete die Gleichwertig-keit der technischen Vorkehrungen und sonstiger Maßnahmen nachweisen. Änderungen im Anforderungskatalog müssen im Sicherheitskonzept berücksichtigt werden. Das geänderte Sicherheitskonzept ist der Bundesnetzagentur unverzüglich vorzulegen.
10	Gibt es ein Formular als Vorlage zum Erstellen des Sicherheitskonzeptes nach § 113g TKG?	Nein, es gibt keine Vorlage. Zur grundsätzlichen Struktur des Sicherheitskonzeptes wird auf die Anlage zum Anforderungskatalog nach § 113f TKG hingewiesen.
11	Gibt es die Möglichkeit ein Musterkonzept als Typmusterprüfung vorzulegen?	Nein, die Möglichkeit für eine Typmusterprüfung hat der Gesetzgeber weder im Zusammenhang mit der Vorlage eines Sicherheitskonzeptes nach § 109 Abs. 4 TKG noch nach § 113g TKG vorgesehen. Der jeweilige Erbringer des öffentlich zugänglichen Telekommunikationsdienstes für Endnutzer muss in seinem Sicherheitskonzept nach § 113g TKG alle Systeme, die zur Erfüllung der Verpflichtungen aus den §§ 113b bis e TKG betrieben werden, aufnehmen, auch die Systeme des sogenannten Erfüllungsgehilfen.

FAQ zur Verkehrsdatenspeicherung

Nr.	FAQ	Antwort
12	Überprüft die BNetzA das Sicherheitskonzept der Verpflichteten?	Ja, die Überprüfung der Umsetzung des Sicherheitskonzeptes nach § 109 Abs. 4 Satz 7 TKG wird in der Regel vor Ort durchgeführt. Der Prüftermin und der Umfang der Prüfung werden mit dem Verpflichteten vorher abgestimmt.
13	Wird bei dem sogenannten Erfüllungsgehilfen die Umsetzung des Sicherheitskonzeptes geprüft?	Ja, die Überprüfung der Umsetzung des Sicherheitskonzeptes nach § 109 Abs. 4 Satz 7 TKG wird in der Regel vor Ort durchgeführt. Damit die Überprüfung durchgeführt werden kann, muss der nach § 113a TKG Verpflichtete in seinem Sicherheitskonzept nach § 113g TKG eine vertragliche Regelung auf der Grundlage des § 11 BDSG mit dem sogenannten Erfüllungsgehilfen aufnehmen und den Zutritt zu den technischen Einrichtungen des VDS-System und zur Prüfung der Protokolle darin regeln. Diese zusätzliche Regelung ist notwendig, da der sogenannte Erfüllungsgehilfe unter Umständen weder Betreiber eines öffentlichen Telekommunikationsnetzes noch Erbringer eines öffentlichen Telekommunikationsdienstes sein kann.
14	Wie wird mit möglichen Mängeln im Sicherheitskonzept umgegangen?	Werden bei der Prüfung des Sicherheitskonzeptes nach § 113g TKG oder bei dessen Umsetzung Sicherheitsmängel festgestellt, so wird der Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer aufgefordert diese Sicherheitsmängel unverzüglich zu beseitigen.
15	Wird bei möglichen Sicherheitsmängeln der gesamte Dienst stillgelegt oder ist nur der Netzbetrieb betroffen?	Wenn der Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer innerhalb einer gesetzten Frist der Aufforderung zur Beseitigung der Sicherheitsmängel nicht nachkommt, kann die Bundesnetzagentur zunächst von der Möglichkeit Gebrauch machen ein Bußgeld zu verhängen und/oder ein Zwangsgeld festzusetzen. Kommt der Verpflichtete der Anordnung auch dann nicht nach, kann die Bundesnetzagentur den Betrieb der betreffenden Telekommunikationsanlage oder das geschäftsmäßige Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise untersagen. Jede Maßnahme muss jedoch verhältnismäßig sein, was stets im Einzelfall zu prüfen ist.

Nr.	FAQ	Antwort

Fragen zur Mandantenfähigkeit des VDS-Systems

16	Können die Speicherpflichten nach §§ 113b ff. TKG auch auf andere Stellen durch Auftrag übertragen werden und was ist dabei zu beachten?	Grundsätzlich ist die Auslagerung des gesamten Verkehrsdatenspeichersystems inkl. dem Abfragesystem oder Einzelkomponenten davon an einen Auftragnehmer im Inland einschließlich der damit verbundenen operativen Tätigkeiten möglich. Die Verantwortung für die Sicherstellung des besonders hohen Standards an Datenqualität und Datensicherheit sowie für die Erstellung, Modifizierung und Einreichung des Sicherheitskonzeptes (§ 113g TKG) verbleibt jedoch bei dem nach § 113a TKG Verpflichteten (= Auftraggeber). Gemäß den Vorgaben des § 11 BDSG (Bundesdatenschutzgesetzes) bleibt der Verpflichtete/Auftraggeber für die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit verantwortlich. Der Verpflichtete/Auftraggeber hat den Auftragnehmer daher insbesondere unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Dies hat er regelmäßig dann erfüllt, wenn sich der Auftragnehmer einer Überprüfung durch eine qualifizierte unabhängige Stelle unterzogen hat und dabei bescheinigt wurde, dass die von ihm zur Verfügung gestellten Systeme und Verfahrensabläufe den Anforderungen an einen besonders hohen Standard der Datensicherheit und Datenqualität nach Maßgabe des § 113f TKG entsprechen. Der Verpflichtete muss hierbei sicherstellen, dass die Bundesnetzagentur und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als zuständige Behörden die Umsetzung der Verpflichtungen der §§ 113b bis 113e TKG und den dabei geforderten besonders hohen Standard der Datensicherheit und Datenqualität überprüfen können. Hierzu zählen neben der Vorlage des Sicherheitskonzepts durch den Verpflichten auch, dass diesen auf Verlangen alle notwendigen Informationen bereitgestellt und ggf. auch Zutritts- und Kontrollrechte beim Auftragnehmer eingeräumt werden. Im Übrigen gelten die Vorgaben des § 11 Abs. 2 BDSG.

Nr.	FAQ	Antwort
17	Muss der Betreiber der VDS-Systems im Rahmen der Auftragsdatenverarbeitung dafür Sorge tragen, dass nur Verkehrsdaten von den sogenannten Resellern gespeichert werden, zu denen ein Auftragsdatenvertragsverhältnis besteht?	Der sogenannte Erfüllungsgehilfe darf im Rahmen der Auftragsdatenverarbeitung nur diejenigen Verkehrsdaten nach § 113b TKG der sogenannten Reseller speichern, die diesem den Auftrag zur Datenverarbeitung auf der Grundlage des § 11 BDSG erteilt haben. Alle anderen Verkehrsdaten anderer sogenannter Reseller ohne einer vertraglichen Regelung nach §11 BDSG dürfen nicht gespeichert werden.
18	Dürfen in einem VS-NfD zertifizierten Netzwerkspeicher auch Verkehrsdaten nach § 113b TKG getrennt von anderen Daten logisch gespeichert werden?	Nein, die nach §113b TKG zu speichernden Verkehrsdaten müssen in physisch gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen gespeichert werden. Diese Anforderung gilt auch beim Einsatz von virtuellen Systemen.
19	Welche sogenannten Erfüllungsgehilfen können durch Verpflichtete ausgewählt werden?	Es gibt keine Einschränkung auf bestimmte sogenannte Erfüllungsgehilfen. Darüber hinaus führt das Referat IS17 der BNetzA keine entsprechende Liste.
20	Wer ist verantwortlich, wenn Fehler bei dem sogenannten Erfüllungsgehilfen vorliegen?	Die Verantwortung für die Umsetzung des Anforderungskatalogs verbleibt bei dem Verpflichteten.

Fragen zum VDS-System (Verkehrsdatenspeicher-System)

21	Darf ein zusätzliches System für die Speicherung der Verkehrsdaten nach § 96 TKG innerhalb des gesicherten Bereichs untergebracht werden in dem auch das VDS-System steht?	Ja, wenn die Speichersysteme für die Speicherung der Verkehrsdaten nach § 113b und § 96 TKG physisch getrennt sind und sich im gleichen Sicherheitsbereich befinden, gelten für beide Systeme die erhöhten Schutzanforderungen nach Kapitel 5.2.6 und 5.2.7 des Anforderungskatalogs.
22	Muss das 4-Augen-Prinzip auch für die Systemadministration umgesetzt werden?	Ja, für den betrieblichen Zugriff auf das VDS-System gilt das 4-Augen-Prinzip nach Abschnitt 5.2.7.2 des Anforderungskatalogs.
23	Muss die VDS-Lösung hochverfügbar sein? Was sind die Anforderungen an Verfügbarkeit- und Wartung?	Die zur Speicherung von Verkehrsdaten betriebenen Systeme müssen über eine nach dem Stand der Technik ausreichende Leistungsfähigkeit und Verfügbarkeit verfügen, um alle anfallenden Verkehrsdaten und

Nr.	FAQ	Antwort
		eingehenden Abfragen verarbeiten zu können. Eine Redundanz ist nicht konkret vorgeben, kann aber unter bestimmten Bedingungen notwendig werden, wenn das Unternehmen durch das Ergebnis der Risikoanalyse im Sicherheitskonzept zu diesem Ergebnis kommt (vgl. Kapitel 4.1, 5.1.1 des Anforderungskatalogs).
24	Kann das VDS-System virtualisiert werden?	Das virtuelle VDS-System muss sich mit allen zugehörigen Komponenten *(Firewall, Ablagesystem, Datenspeicher, Zugriffssystem und dem Schlüsselmanagement)* in einer physisch zutrittsgesicherten Umgebung befinden. Es ist zu beachten, dass das Schlüsselmanagement vom eigentlichen Datenspeicher und anderen Komponenten des VDS-Systems ausschließlich getrennt gehalten und administriert werden soll.
25	Wird durch den Einsatz von Zugangskarte und PIN-Eingabe die 2-Faktor-Authentikation sichergestellt?	Ja, dies wäre eine Möglichkeit der Umsetzung (siehe hierzu Kapitel 5.2.6.2 des Anforderungskatalogs)
26	Der Zutritt zum Rack mit den Komponenten zur Verkehrsdatenspeicherung erfolgt mittels zusätzlichen Schlüssels, der unter Anwendung des 4-Augenprinzips bei einer zentralen Stelle abgeholt wird und dies auch dort dokumentiert wird. Erfüllen diese Anforderungen den Anforderungskatalog?	Vorausgesetzt, dass die Zutrittsberechtigung durch eine 2-Faktor-Authentifikation z.B. durch den Einsatz von einer Zugangs-Chipkarte mit PIN-Eingabe erfolgt, dann kann das Vier-Augen-Prinzip z.B. auch durch den Pförtner angewandt werden, der den Schlüssel zum VDS-System verwaltet. Der Schlüssel darf nur an die Personen ausgehändigt werden, die besonders ermächtigt sind.
27	Welche Mitarbeiter des Unternehmens dürfen den Fernzugriff auf das VDS-System nutzen?	Nach Kapitel 5.2.7.2 des Anforderungskatalogs ist die Nutzung des Fernzugriffs für den betrieblichen Zugriff z.B. für Wartungszwecke ausschließlich im Vier-Augen-Prinzip und den besonders ermächtigten Personen des Unternehmens (Systemadministrator) erlaubt. Der Betrieb der Clientsysteme für den Fernzugriff ist nur in den in Deutschland gelegenen Räumen des Unternehmens gestattet. Zur

Nr.	FAQ	Antwort
		Unterstützung der besonders ermächtigten Systemadministratoren dürfen unternehmensfremde Personen, auch Personen außerhalb Deutschlands, maximal nur lesenden Zugriff auf die Management-Konsole entsprechend der Regelungen nach Kapitel 5.2.7.2, Abschnitt B des Anforderungskatalogs nach § 113f TKG erhalten.
28	Wie lange sollen Systemlogs gespeichert bleiben?	Grundsätzlich sind die Protokolldaten nach § 113e TKG mit dem Zeitpunkt des Zugriffs, die Daten der zugreifenden Person, der Zweck und die Art des Zugriffs für ein Jahr zu speichern. Die systembedingten Protokolldaten (z.B. Firewall-Logs) sind für 3 Monate zu speichern.

Fragen zur Verschlüsselung der VDS-Daten

29	Wenn der Auftragsdatenverarbeiter Verkehrsdaten nach § 113b TKG verschiedener Verpflichteter auf einem Speichersystem in logisch oder physisch voneinander getrennten Speicherbereichen entsprechend Kapitel 5 des Anforderungskataloges speichert, müssen dann auch für unterschiedliche Verpflichtete unterschiedliche Schlüssel verwendet werden?	Ja, nach Abschnitt 5.2.2 des Anforderungskataloges muss die Speicherung der Verkehrsdaten nach § 113d TKG so realisiert werden, dass der Schutz gegen unbefugte Kenntnisnahme und Verwendung der Verkehrsdaten sichergestellt ist. Die Verkehrsdaten müssen vor Eingang in den Datenspeicher mit einem geeigneten Verschlüsselungsverfahren verschlüsselt werden. Sofern die Verkehrsdaten nach § 113b TKG nicht bereits durch den Verpflichteten mit seinen Schlüsseln verschlüsselt wurden, sollten diese zum Schutz gegen unbefugte Kenntnisnahme und Verwendung mit einem eigenen von den der anderen Verkehrsdaten der anderen Verpflichteten unterschiedlichen Schlüssel verschlüsselt werden (jeder Verpflichtete hat seinen eigenen Schlüssel).

Nr.	FAQ	Antwort
30	Müssen die Verkehrsdaten nach § 96 TKG auch tageweise verschlüsselt werden, wenn diese im gleichen Sicherheitsbereich wie die Verkehrsdaten nach § 113b TKG gespeichert werden?	Nein, eine zwangsweise Pflicht zur Verschlüsselung der Verkehrsdaten nach § 96 TKG besteht nicht. Für die Speicherung der Verkehrsdaten nach § 96 TKG gelten die technischen Schutzmaßnahmen nach § 109 TKG. Inwieweit eine Verschlüsselung der Verkehrsdaten nach § 96 TKG notwendig wäre, ergibt sich aus der Beurteilung des Restrisikos der getroffenen Schutzmaßnahmen nach IT-Grundschutz, bzw. dem Katalog der Sicherheitsanforderungen nach § 109 TKG.
31	Wird die Schlüsselverwaltung des VDS-Systems nur für die Speicherung der Verkehrsdaten oder auch für die Übermittlung der Antworten verwendet?	Die Schlüsselverwaltung wird nur für die Verschlüsselung der Verkehrsdaten nach §113b TKG im VDS-System benötigt.
32	Muss es im Rahmen des Schlüsselmanagements einen eindeutigen Tagesschlüssel geben, der mit der täglichen Speicherung der Verkehrsdaten verbunden ist?	Nein, die Ausgestaltung des Schlüsselmanagements lässt nicht nur den Einsatz von Tagesschlüssel zu. Kapitel 5.2.2 des Anforderungskataloges enthält hierzu nähere Ausführungen und Beispiele.

Bei weiteren Fragen zum Sicherheitskonzept wenden Sie sich an:

Referat IS17
E-Mail: IS17.Postfach@bnetza.de