

## Stellungnahme

### Referentenentwurf „Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren“ vom 22.12.2025

Unter Bezugnahme auf den am 22.12.2025 veröffentlichten Entwurf eines **Gesetzes zur „Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren“** möchten wir als betroffene Netzbetreiber wie folgt **Stellung** nehmen:

Der Gesetzesentwurf **beachtet im Wesentlichen** die durch den **EuGH** aufgezeigten **rechtlichen Grenzen**. Das begrüßen wir. Des Weiteren ermöglicht der Entwurf eine **technologieoffene** und **verhältnismäßige** Umsetzung und **löst** viele **Probleme** der **vormaligen Regelungen** zur Vorratsdatenspeicherung. Insbesondere bewerten wir als **positiv**, dass die **angefochtenen** und außer **Kraft gesetzten Regelungen** der **alten anlasslosen Vorratsdatenspeicherung** im TKG nach Maßgabe des Referentenentwurfes („Ref-E“) **vollständig gestrichen** wurden.

#### 1. Anmerkungen zur Einführung einer Mindestspeicherung von IP-Adressen

##### 1.1 Formulierungsanforderungen an die Speicherdauer

**Datenschutzrechtlich kritisch** erachten wir die in **§ 176 Abs. 1** TKG Ref-E enthaltene Forderung zur Speicherung der Daten **mit Beginn der Zuweisung** und **Löschung nach drei Monaten ab dem Zeitpunkt des Endes der Zuweisung**. Diese Regelung führt zu einer **Datenspeicherung deutlich über drei Monate** hinaus und **verletzt** somit die **Vorgaben des EuGH**.

In vielen Netzen, insbesondere bei modernen Glasfaseranschlüssen, gibt es **keine Zwangstrennung** mehr. Es kommt nur noch **selten** zu einer **Trennung der Verbindung**, zum Beispiel bei Wartungsarbeiten im Netz. **Verbindungszeiten** von **mehreren Wochen** und **Monaten** sind die Regel. Besteht die **Verbindung** bei einem solchen Anschluss beispielsweise über **zehn Monate**, führt dies zu einer **Speicherdauer** von insgesamt **13 Monaten** bei der **bislang im Gesetzestext formulierten Speicherzeit**.

Bereits die **Nennung der Speicherfrist** von drei Monaten in **§ 176 Abs. 1 S. 1** TKG Ref-E zusätzlich zur Löschvorgabe in **§ 176 Abs. 2 Nr. 4** TKG Ref-E irritiert, da eine **Speicherung über drei Monate** nach Beginn der Zuweisung hinaus bis zum Zeitpunkt der vorgesehenen Löschung **nicht eindeutig vorgegeben** ist. Die **Frist** sollte **ausschließlich** in **§ 176 Abs. 2 Nr. 4** TKG Ref-E aufgeführt werden.

Um die Speicherung von Daten auf höchstens drei Monate zu begrenzen, ist eine **zusätzliche rechtliche Vorgabe notwendig**, nach welcher das Datum und die Uhrzeit vom Beginn der Zuweisung nach drei Monaten zu löschen sind. Der **anschließend fehlende Zeitpunkt** des Beginns der Zuweisung in den entsprechenden **Datensätzen** bedeutet, dass die Zuweisung seit mindestens drei Monaten besteht, ohne die **konkrete Dauer zu benennen**, so dass eine **Auskunft** zu einem **länger zurückliegenden Zeitpunkt unmöglich** ist.

**Alternativ** könnte § 176 Abs. 1 TKG Ref-E derart geändert werden, dass anstelle einer Auflistung zu **speichernden Daten technologieneutral** der eigentliche **Zweck** beschrieben wird:

*Anbieter von Internetzugangsdiensten müssen die Identifizierung von Teilnehmern basierend auf öffentlicher IP-Adresse, Portnummer und sekundengenauer Zeitangabe für einen Zeitraum von drei Monaten ermöglichen. Hierzu dürfen sie dafür notwendige Verkehrsdaten speichern.*

Diese **vorgeschlagene Gesetzesanpassung** ist aus unserer Sicht **essenziell**, um das Gesetz rechtssicher zu gestalten. **Rechtssicherheit** steht für uns als Netzbetreiber bei einer **Neuregelung** und dem **dritten Versuch** einer anlasslosen Speicherung von Daten auf Vorrat im **Vordergrund**.

## 1.2 Zielgerichtete Anforderungen an die Datensicherheit

In §§ 175 Abs. 2 Nr. 4, 176 Abs. 2 Nr. 4 TKG Ref-E wird eine **unverzügliche und irreversible Löschung** der gespeicherten Daten gefordert. Diese Anforderung wird mithin sowohl für die Sicherungsanordnung als auch für die IP-Datenspeicherung formuliert. Mit üblichen **Datenbanksystemen und skalierbaren Speicherlösungen** ist diese Verpflichtung **schlichtweg technisch nicht umsetzbar**. Das BSI schreibt im IT Grundschutz Kompendium in CON.6:

*„Gewöhnliche Löschvorgänge über die Funktionen des Betriebssystems bewirken in der Regel kein sicheres Löschen der Informationen, das verhindert, dass die Daten wieder rekonstruiert werden können. Um Informationen sicher zu löschen, bedarf es daher spezieller Verfahren. Datenträger können jedoch nur effektiv in ihrer Gesamtheit sicher gelöscht werden und dies ist bei einzelnen Dateien meist nur mit Einschränkungen möglich.“*

Darüber hinaus würde ein „**unverzügliches und irreversibles Löschen**“ das **Anlegen** von **Backups unmöglich** machen. Zusätzlich **erhöhen** sich dadurch die **Implementierungs-** und **Betriebskosten** dramatisch. Vor diesem Hintergrund **regen** wir an, den **Löschbegriff** der **DS-GVO** hier zu verwenden.

**Technische Einzelheiten** zur Umsetzung sollten ferner besser in der **Technischen Richtlinie** geregelt werden.

### 1.3 Erfordernis einer längeren Umsetzungsfrist

Die **Umsetzungsfrist** einer Speicherverpflichtung nach § 230 Abs. 16 TKG Ref-E von sechs Monaten ist **zu kurz bemessen**. Dies ergibt sich aus folgenden Erwägungen:

- **Erstens** sollten zwingend erst die **Anpassungen der TKÜV** und **TR TKÜV** vorliegen, bevor eine entsprechende Frist anfängt zu laufen (vgl. § 175 Abs. 3 TKG Ref-E). Gerade vor dem Hintergrund, dass eine Vorratsdatenspeicherung **gleich zwei Mal gescheitert** ist und die **Adressaten** der Speicherverpflichtungen entsprechende **finanzielle Belastungen** zu tragen hatten, können **Implementierungsmaßnahmen erst** dann getroffen werden, wenn die **rechtlichen Vorgaben erlassen** sind.
- **Zweitens** ist die Frist von sechs Monaten ebenfalls aus **technischen Gründen unmöglich**. Die Umsetzung der **rechtlichen Verpflichtungen** hätte Vorrang; andere Vorhaben mit **direkten Auswirkungen auf den Kunden** müsste zurückstehen. Dies führt **zwangsläufig** zu einem **verzögerten Netzausbau, geringeren Kapazitäten** und **massiven Wettbewerbsnachteilen**. Insbesondere bei den länger am Markt tätigen Netzbetreibern sind erhebliche Anpassungen an der **Netzinfrastruktur** erforderlich.

Wir würden im Hinblick auf die **notwendige Planungssicherheit** die Inkraftsetzung der **Speicherverpflichtung mit der Bereitstellung** der TKÜV und TR TKÜV mit den relevanten Vorgaben **koppeln** und eine **Implementierungszeit von mindestens einem Jahr** ansetzen.

### 1.4 Klarstellungsbedarf Position 201 Justizvergütungs- und entschädigungsgesetz (JVEG)

Wir verstehen **Position 201 JVEG Ref-E** so, dass basierend auf der Gesetzesbegründung **in Abgrenzung** zur **Position 200** bei **Anfragen zu Bestandsdaten** zu einer IP-Adresse nur die **Bestandsdaten beauskunftet** werden, die nach **§ 173 TKG gespeichert** sind. Umfangreichere und **aufwendig zu erhebende Daten**, die im Rahmen eines Ersuchens nach § 174 TKG angefragt werden können, sind **hiervon nicht erfasst**. Sollten weitere Daten basierend auf § 174 TKG abgefragt werden, wäre die **Position 200 JVEG zusätzlich** je Datensatz basierend auf dem **manuell / höheren Aufwand zu berechnen**. Dies ist aus unserer Sicht **äquivalent zur Identifizierung** eines Teilnehmers über die **Abfrage**

mittels AAV zu einer **bekannten MSISDN** zu verstehen. Daher gilt ein **reduzierter Satz zur Vergütung** nur bei der **reinen Identifizierung** eines Teilnehmers über Verkehrsdaten zu einer IP-Adresse.

## **2. Anmerkungen zur Einführung einer Sicherungsanordnung**

### **2.1 Entschädigungssatz bei Auskünften nach vorausgegangener Sicherungsanordnung**

Beim Abruf der gesicherten Daten sieht die **Position 600 JVEG Ref-E** einen gegenüber den **Positionen 500-506 JVEG Ref-E** für die Sicherung von Daten **deutlich reduzierten Entschädigungssatz** vor. Dies ist aus unserer Sicht **ausschließlich gerechtfertigt**, wenn die **Daten vollständig abgerufen** werden. **Anders** ist dagegen mit dem **Fall** umzugehen, wenn nur eine (mit weiteren Suchkriterien eingegrenzte) **Teilmenge der gesicherten Daten** zur **Herausgabe** angefordert wird.

Für **diesen Fall** sollte - entsprechend der zur Eingrenzung verwendeten Suchkriterien - erneut die **Entschädigungssätze** der **Positionen 500-506 JVEG Ref-E** zur Anwendung kommen. Nur diese Vorgehensweise trägt dem **erneuten und höheren Bearbeitungsaufwand** bei Teilabrufen hinreichend Rechnung.

### **2.2 Anmerkungen zum Adressatenbegriff des § 175 Abs. 1 TKG Ref-E**

**§ 175 Abs. 1 TKG Ref-E** bezieht sich lediglich auf **Anbieter öffentlicher TK-Dienste**. Die **Formulierung** ist mithin **enger** als die **Vorgängerregelung** des § 175 Abs. 1 TKG Ref-E und ebenfalls **restriktiver formuliert** als die **komplementäre**, in **§ 100g Abs. 1 StPO Ref-E** geregelte Befugnis.

Daraus folgt, dass in **Konstellationen**, in denen der **Anbieter** öffentlicher TK-Dienste und der **Netzbetreiber gesellschaftsrechtlich unabhängig** voneinander sind, solche Verkehrsdaten, die nur bei dem Netzbetreiber anfallen, **normativ nicht** von der in **§ 175 Abs. 1 TKG Ref-E** geregelten Befugnis zur **Beauskunftung** erfasst sind. Es sollten also **diejenigen**, die an dem Anbieten von TK-Diensten **mitwirken** als Normadressaten in § 175 Abs. 1 TKG Ref-E **ergänzt** werden oder eine vergleichbare **Öffnung des Adressatenbegriffs** erfolgen.

### **2.3 Bedeutung des unverzüglichen Löschens gemäß § 13a TDDDG Abs. 2 Ref-E**

Der **Gesetzesentwurf fordert**, dass gesicherte Daten nach der **Übermittlung unverzüglich gelöscht** werden. Diese würde nach unserem Verständnis auch bedingen, dass nach einem Teilabruf der **gesicherten Daten**, die **nicht übermittelten Daten** weiter zu **sichern** sind.

Wir interpretieren die **Verpflichtung zur unverzüglichen Löschung** ferner so, dass wie bisher zur Klärung von möglichen **Übermittlungsfehlern** die **übermittelten Daten** noch **für eine kurze Zeit** zur Fehlerbehebung und erneuten Versendung **vorgehalten** werden sollen.

## 2.4 Umsetzungsfrist

Auch bei der **Sicherungsanordnung** können weitere Regelungen in der TKÜV sowie der technischen Richtlinie getroffen werden. Die Regelungen zur Sicherungsanordnung sind dabei **direkt mit der Gesetzesverkündung anwendbar**.

Hier würden wir eine **Übergangszeit** erwarten, die einsetzt, sobald die **notwendigen Rechtsakte erlassen** worden sind. Ansonsten würden die **Verpflichteten** dazu **angehalten** sein, bereits **im Vorfeld ohne Kenntnis** der in der TKÜV / TR TKÜV zu treffenden Vorgaben, **Implementierungsmaßnahmen zu ergreifen**. Dies widerspricht nicht nur der Rechtssicherheit, sondern auch dem Rechtsstaatsprinzip.