Positionierung zur VERPFLICHTUNG VON MINDESTSPEICHERFRISTEN VON IP-ADRESSEN sowie zur EINFÜHRUNG EINER SICHERUNGSANORDNUNG

Wir bedanken uns für die Möglichkeit, unsere Überlegungen zur Einführung einer Speicherverpflichtung von IP-Adressen und Sicherungsanordnung einbringen zu dürfen. Es ist uns ein **sehr großes Anliegen**, dass nach den **erheblichen Fehlinvestitionen** zweier vor den Gerichten **gescheiterten Vorratsdatenspeicherungen** ("VDS") jeglicher neuer Regelungsansatz vor allem **Rechtssicherheit** bietet. Darüber hinaus sind auch die **wirtschaftlichen** und **technischen Rahmenbedingungen** zu berücksichtigen. Unsere Überlegungen beziehen sich auf die vorliegenden Gesetzesentwürfe:

- *Gesetzentwurf der Fraktion der CDU/CSU "Entwurf eines Gesetzes zur Verbesserung der Verbrechensaufklärung – Einführung einer Mindestspeicherung von IP-Adressen und Wiederherstellung der Funkzellenabfragemöglichkeit" (Drs. 20/13366),*
- *Gesetzentwurf des Bundesrates "Entwurf eines Gesetzes zur Einführung einer Mindestspeicherung von IP-Adressen für die Bekämpfung schwerer Kriminalität" (Drs. 20/13748) und*
- *Gesetzentwurf "Entwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung" (Drs. 20/14022).*

1. Anmerkungen zur Einführung einer Mindestspeicherung von IP-Adressen

Aus unserer Sicht ist es **nicht sinnvoll**, die derzeitigen Regelungen **§§ 176- 181 TKG nachzubessern** oder **möglichst minimale Anpassungen** vorzunehmen, um eine Speicherverpflichtung für IP-Adressen einzuführen.

Die derzeit **vorliegenden Entwürfe** zur IP-Datenspeicherung sehen **im Wesentlichen** nur eine **Eingrenzung der Speicherverpflichtung** auf die Speicherung von **IP-Adressen und Portnummern** vor. Alle weiteren Rahmenbedingungen bleiben größtenteils unverändert bestehen. Uns als potenziell Verpflichtete werden damit **überbordende Sicherheitsvorgaben** auferlegt. Im Hinblick auf eine Neuregelung zur Speicherung von IP-Adressen-Zuordnungen durch den Internet Service Provider ("ISP") sprechen wir uns für die **ersatzlose Streichung der alten Gesetzesregelungen zur VDS und eine Neuformulierung der entsprechenden Vorschriften im TKG** aus.

1.1 Technologieoffenheit

Die Gesetzentwürfe **verkennen**, dass es **unterschiedliche Technologien** gibt, um einem Anschluss eine **IP-Adresse zuzuweisen**. Aufgrund des **bekannten IP-Adressenmangels im IPv4 Bereich** wenden alle ISPs **unterschiedliche Verfahren** an, um den Kunden **IP-Verbindungen zu ermöglichen**. Auf Grundlage der **unterschiedlichen Technologien für den Internetzugang** (Festnetz, Mobilfunk, Satellit) **existieren** ebenso **diverse technische Realisierungen der IP-Adresszuordnungen** für einen Internetanschluss.

Hintergrundinformationen zur Vergabe von IP-Adressen durch einen ISP

Bei der Vergabe von IP-Adressen gibt es drei zu unterscheidende Szenarien:

1. Der IP-Anschluss hat eine **fest (statisch) zugewiesene öffentliche** IP-Adresse. Die IP-Adresse wird mit dem Vertragsabschluss dem Anschluss fest zugewiesen. Die statische Zuteilung kommt daher nur bei einem verschwindend geringen Anteil der Anschlüsse zum Einsatz. Die **statisch** zugewiesene **IP-Adresse gilt als Bestandsdatum**. **Anhand der IP-Adresse ist nicht erkennbar, ob diese statisch zugeordnet ist**.
2. Der IP-Anschluss erhält für die Dauer der Einwahl ins Internet **eine dynamisch zugewiesene** IP-Adresse zur exklusiven Nutzung. Bei jeder neuen Einwahl, bei einer möglichen Zwangstrennung, bei Verbindungsabbrüchen oder Wartungsarbeiten im Netz des ISPs wird **dem Kunden eine andere IP-Adresse zugewiesen**.
3. Der IP-Anschluss erhält, bedingt durch die **wenigen verfügbaren IPv4 Adressen**, für die Dauer der Einwahl **nur eine IP-Adresse aus dem internen Netz des ISPs**. Die interne IP-Adresse wird nach außen nicht sichtbar und kann auch von außen nicht direkt angesprochen werden. Bei jeder Kommunikation ins Internet wird die interne IP-Adresse über verschiedene Verfahren umgerechnet. Es kommt so zu einer internen Verbindung des Anschlusses ins Netz des ISPs. Gleichzeitig kommt es zu einer zweiten durch den ISP aufgebauten Verbindung ins Internet zu der vom Kunden gewünschten Zieladresse. Bei jeder **einzelnen Kommunikation** können die **öffentlich sichtbaren IP-Adressen und Ports** dabei **variieren**.

Für Details verweisen wir auf den ETSI Technical Report 103 829 - „IP address retention and traceability“ (online abrufbar).

Das Ziel des Gesetzes ist es, den Ursprung bzw. den **Teilnehmer einer Kommunikation im Internet identifizieren** zu können. Die bisherigen regulatorischen Ansätze haben hierzu eine **Speicherverpflichtung der öffentlichen IP-Adresse vorgesehen**. Letzte Entwürfe **erweitern diese Verpflichtung um die zusätzliche Speicherung der Port-Adresse**. Diese Ansätze verkennen aber wesentliche **technische Zusammenhänge**. Eine Speicherpflicht für „**eine gegebenenfalls zugewiesene Port-Nummer**“ ist **unzureichend für alle Technologien**, durch die **einem Anschluss Port-Nummern** bzw. **ganze Port-Bereiche zugewiesen** werden. Im Internet ist **nicht erkennbar**, um **welche Art des Zugangs** es sich handelt und **wer hinter** der **sichtbaren IP-Adresse des ISPs** steht. Um eine Verbindung

einem **Anschluss** und damit einem **Anschlussinhaber zuzuordnen**, sind daher **zwei Aspekte** zu beachten:

- **Parameter der Anfrage**: Die **Verbindung** wird **unabhängig** von der **durch den ISP eingesetzten Technologie** durch die IP-Adresse der Quelle, dem durch die Quelle genutzten Port der Verbindung und der Uhrzeit eindeutig **definiert**. Jede IP-Verbindung ist die Verbindung von einer Source IP-Adresse über einen hier genutzten Port zu einer Destination IP-Adresse und einen hier adressierten weiteren Port. Der Aufruf nur einer Internet-Seite erzeugt dabei schon dutzende kurze Internetverbindungen (Cookies, Banner, Adds, Bilder, Frames). Eine **Anfrage an den ISP zur Zuordnung einer IP-Verbindung** zu einem Kundenanschluss muss daher die **Source IP-Adresse**, den **Source Port** sowie den **Zeitpunkt der Verbindung** enthalten.
- **Duch den ISP zu speichernden Daten**: Der Zugang ins Internet wird durch unterschiedliche technische Verfahren ermöglicht. Die für eine **Zuordnung einer angefragten IP-Verbindung** durch den **ISP zu speichernden Daten** können - je nach eingesetzter **Technologie** - **unterschiedlich** sein. Diese legt der ISP basierend auf dem von ihm eingesetzten Verfahren fest.

Eine Neuregelung zur IP-Adressenspeicherung könnte möglicherweise so gestaltet werden, dass ein ISP in der Lage sein muss, eine im Internet **sichtbare IP-Verbindung** zu einem **bestimmten Zeitpunkt** einem **konkreten Anschluss zuzuordnen**. Eine entsprechende Norm sollte demnach die zuvor erwähnten Punkte in der Art berücksichtigen, dass:

- sofern **dynamische** (nicht fest vergebene) IP-Adressen vergeben werden, sollten für das Auskunftsverfahren nach § 174 TKG diejenigen Daten **technologieoffen erhoben** und **gespeichert** werden, die **eine eindeutige Zuordnung** des genutzten Anschlusses **ermöglichen**.
- Zur **Identifikation des Anschlusses** benötigt der **Provider von der berechtigten Stelle** die öffentlich von diesem Anschluss für diese **Verbindung genutzte** und im Internet **sichtbare IP-Adresse** und **Por**t sowie den **Zeitpunkt der Verbindung**.

Als Verpflichtete sehen wir folgende **weitere Aspekte** als **notwendig** an, um eine **datenschutzkonforme Umsetzung** zu erreichen:

- Daten, die die **adressierte Gegenseite der Kommunikationsverbindung** betreffen, wie etwa die IP-Adresse und der Port der Gegenseite, **dürfen nicht gespeichert** werden. Diese Daten könnten **sonst Rückschlüsse auf Inhalte der Kommunikation** ermöglichen.

- Die **Speicherung, der für die Zuordnung benötigten Daten**, **erfolgt getrennt** von den zu **betrieblichen Zwecken gespeicherten Daten**. Eine Verwendung der Daten für andere Zwecke als die zur Identifikation eines Anschlusses im Rahmen eines Auskunftsverfahren nach § 174 TKG ist nicht zulässig.
- Wir empfehlen eine auf das **nötigste begrenzte Speicherfrist**, etwa 30 Tage.
- Die **Kriterien** zur **Absicherung der Daten und Zugriff**e sollten in der **Rechtsverordnung** nach § 170 Abs. 5 TKG und der TR nach § 170 Abs. 6 TKG **geregelt** werden.

1.2 Zielgerichtete Anforderungen an die Datensicherheit

Anders als in der – ausgesetzten – Regelung **gemäß § 176 TKG** sind die, **für die Zuordnung einer Internetverbindung zu speichernden Date**n, zwar **Verkehrsdaten** im Sinne des TKG. Allerdings werden diese als qualitativ **weniger** "**sensitiv**" bewertet und weisen insofern einen **geringeren Schutzbedarf** auf (vgl. EuGH Urt. v. 06.10.20, C-511/18, C-512/18 und C-520/18, Rn. 152). Sie lassen insbesondere **keine Rückschlüsse auf die Inhalte der Kommunikation, die Privatsphäre und Persönlichkeit des Teilnehmers** zu. Die für eine IP-Adressen-Zuordnung erforderlichen Daten **unterliegen somit nicht dem erhöhten Schutzbedarf von Verkehrsdaten**. Aus diesem Grund sind die Anforderungen in **§ 180 TKG**, die für **anlasslos und auf Vorrat gespeicherten Verkehrsdaten aller Teilnehmer** galten, **nicht notwendig und sinnvoll** für die hier beabsichtigte IP-Datenspeicherung. Vielmehr sind die **Anforderungen an die Datensicherheit ausreichend**, die bereits **im Auskunftsverfahren nach § 170 TKG gelten** und **dort normiert sind**.

1.3 Umsetzungsfrist

Mit einer **erneuten Speicherverpflichtung von IP-Adressen** und den **damit im Zusammenhang stehenden Daten** sind **zwingend umfangreiche technische Änderungen** an der Infrastruktur bei den einzelnen ISPs verbunden. Inhaltlich handelt es sich **folglich mitnichten um eine einfache Ausdehnung der bisherigen IP-Adressenspeicherung zu betrieblichen Zwecken**. Insbesondere bei den **etablierten Netzbetreibern** werden **erhebliche** und **kostenintensive technischen Anpassungen** aufgrund der unterschiedlichen eingesetzten Technologien notwendig. Die Umsetzungsfrist sollte, insbesondere im Mobilfunk, **mindestens zwei Jahre** betragen.

2. Anmerkungen zur Einführung einer Sicherungsanordnung

2.1 Anforderungen an die Verwendung und Herausgabe der Daten

Bedingt durch die **Notwendigkeit einer Sicherungsanordnung für Herausgabeverlangen** gemäß der **E-Evidence-Verordnung** bedarf es einer Regelung für die Sicherung von Verkehrsdaten. Wir bitten bei der **Formulierung des Gesetzes** zu berücksichtigen, dass die **gesicherten Daten getrennt** von **anderen Daten zu speichern** sind und nur in dem **Verfahren zum Abruf zur Verfügung** stehen, für das die Sicherungsanordnung erlassen wurde. Eine **Verwendung der Daten** für andere als die in der **Sicherungsanordnung benannten Zwecke** (z. B. Auskunftsersuchen eines Kunden nach der DS-GVO), sollte **ausgeschlossen** sein.

Sollten die **Daten vor einer Herausgabe** gegenüber der **ursprünglichen Sicherungsanordnung** weiter **eingegrenzt** werden, so ist der **Aufwand höher**. Dies sollte sich im **Entschädigungssatz** entsprechend **wiederfinden.** Wir würden hier eine **Entschädigung** wie bei der **ursprünglichen Sicherungsanordnung vorschlagen**. Nur wenn die gesicherten **Daten unverändert** und **vollständig** herauszugeben sind, ist der **Aufwand entsprechend geringer** und **rechtfertigt** einen **reduzierten** Entschädigungssatz.

2.2 Umsetzungsfrist

Die Umsetzungsfrist sollte **ausreichend bemessen** sein, um die **notwendigen IT-Systeme** zur Abfrage und Speicherung **zu entwickeln** und im Netz **zu implementieren**. **Die Umsetzungsfrist** sollte **mindestens ein Jahr** betragen.