schal abgegoltenen Verbindungen mitgeteilt werden dürfen, so gewährt dies keinen Anspruch gegen den Anbieter (zu § 45e und § 99 TKG aF s. BT-Drs. 16/3635, 45).

Die Regelungen zur **Auskunft** über **Verkehrsdaten** nach § 11 mit Erteilung des Einzelverbindungsnachweises und des Nachweises bei nachträglichen Beanstandungen gegen die Rechnung sind abschließend und **vorrangig vor** dem **allgemeinen Auskunftsrecht der Betroffenen** nach **Art. 15 DS-GVO.** Die bisherige Rechtslage gegenüber dem allgemeinen Auskunftsanspruch nach § 34 BDSG aF darf die Spezialregelungen und deren Voraussetzungen nicht umgehen (zu § 34 BDSG aF und § 99 TKG aF *AG Bonn* ZD 2014, 148f.; *Bäcker* MMR 2009, 803 (805) (kein allgemeiner Auskunftsanspruch für Abrechnungsdaten, wohl aber für sog. Vorratsdaten nach § 113b TKG aF); *Wehr/Ujica* MMR 2010, 667 (670)). **15**

3. Ausschluss von Verbindungen nach Abs. 5 und Abs. 6

Der Einzelverbindungsnachweis darf **keine Verbindungen** zu **Anschlüssen erkennen** lassen, die in **Abs. 5 aufgezählt** sind. Dies sind insbesondere die dort genannten **Beratungsstellen.** Die entsprechenden Stellen werden in einer Liste aufgenommen, welche die BNetzA zum Abruf bereithält. Die entsprechende Liste ist zumindest vierteljährlich abzurufen und muss deshalb bei der Erteilung eines Einzelverbindungsnachweises automatisiert berücksichtigt werden. **16**

Abs. 6 enthält zudem **Besonderheiten** für bestimmte **Berufsträger** wie Rechtsanwälte oder Ärzte. Diese können sich auf Antrag in die Liste der BNetzA eintragen lassen, sodass dann Anrufe zu ihren Anschlüssen nicht in Einzelverbindungsnachweisen aufgeführt werden dürfen. **17**

Diese **Beschränkungen** bei dem Ausweis der Verbindungen im Einzelverbindungsnachweis bedeuten gleichzeitig, dass die Höhe der in Rechnung gestellten **Entgelte** sich nicht **vollständig** mit den Einzelverbindungen **abgleichen** lässt, wenn auch Verbindungen zu einem der in der Liste genannten Anschlüssen entgeltpflichtig stattgefunden haben. Dies bedeutet, dass sich in diesem Fall scheinbar ein Widerspruch zwischen der Abrechnung und der Auflistung ergibt. Der Gesetzgeber hat entschieden, dass dieser Widerspruch in diesem Falle hinzunehmen ist. **18**

Gesetzlich nicht geregelt ist, ob die **Einschränkung des Abs. 5** zum Ausweis dieser bestimmten Anschlüsse im Einzelverbindungsnachweis auch für den Fall des § 11 Abs. 2 gilt, wenn dem Endkunden aufgrund seiner **Einwendungen nachträglich** die **Verkehrsdaten** aufzuschlüsseln sind. Auch in diesem Falle stehen sich das Interesse des Endnutzers an der Prüfung der Entgelte und Verbindungen und die Datenschutzinteressen entgegen. Da es an einem ausdrücklichen Verbot fehlt, auch diese Verbindungen aufzuschlüsseln, hat hier der Vorgang an der Prüffähigkeit der Rechnung den Vorrang. Denn das Recht des Endnutzers nach § 65 Abs. 1 TKG auf Erteilung eines Einzelverbindungnachweises ist gesetzlich nicht ausdrücklich eingeschränkt und diese Wertung ist nachvollziehbar als Interessensausgleich iSv Art. 7 Abs. 2 ePrivacy-RL. **19**

4. Sonderfall des Abs. 4 bei 0800-Anschlüssen

Einen **Sonderfall** der Erteilung eines **Einzelverbindungsnachweis** regelt § 11 **Abs. 4.** Soweit ein Anschlussinhaber zur vollständigen oder teilweisen Übernahme der Entgelte für Verbindungen verpflichtet ist, die bei seinem Anschluss ankommen, dürfen ihm in dem für ihn bestimmten Einzelverbindungsnachweis die Nummern der Anschlüsse, von denen die Anrufe ausgingen, nur unter Kürzung um die **20**

letzten drei Ziffern mitgeteilt werden. Dies bedeutet, dass die Aufnahme dieser Verbindungen in den Einzelverbindungsnachweis zulässig ist, hierbei die sog. A-Rufnummer aber um die letzten drei Ziffern zu kürzen ist.

21 Diese **Regelung** wird insbesondere in der **Praxis bedeutsam,** wenn ein Nutzer **0800-Rufnummern** bei einem Netzbetreiber geschaltet hat, für die er dann entsprechend der Rufnummerngasse selbst die Entgelte tragen muss, während diese Verbindungen für den Anrufer kostenfrei sind. Abs. 5 bestimmt hierbei, dass der Nutzer (Anschlussinhaber und B-Teilnehmer) zwar in gewisser Weise alle Verbindungen entsprechend hinsichtlich der Entgeltpflicht überprüfen kann, dies aber nur eingeschränkt durch Kürzung der A-Rufnummern um die letzten drei Ziffern. Dies soll dem Interesse der Anrufenden an der Vertraulichkeit der Kommunikation dienen. Diese Vorschrift ist in der Praxis im Regelfall nicht sehr bedeutsam, da auch unter 0800-Rufnummern im Regelfall unter vollständiger Signalisierung der A-Rufnummer angerufen wird. Dennoch ist diese Regel bei der Erteilung des Einzelverbindungsnachweises zu beachten, unabhängig davon, ob die Anrufer die vollständigen Rufnummern bei den Verbindungen signalisieren oder nicht.

22 **Abs. 5** findet hingegen in der Praxis und im Ergebnis **keine Anwendung bei sog. Shared-Cost-Diensten** oder entgeltfreien Mehrwertdiensten (aA Taeger/Gabel/*Munz* TTDSG § 11 Rn. 5). Historisch wurden zwar Rufnummern in der 01080-Gasse als sog. „Shared-Cost-Dienste" eingeführt, bei denen die Entgelte zwischen Anrufer und Angerufenem aufgeteilt wurden. Solche Dienste gibt es aber in der Praxis nicht mehr und insbesondere die Rufnummern in der Gasse 0180 betreffen nun auch entgeltpflichtige **Servicedienste,** bei denen nur der Anrufer das Entgelt zu zahlen hat (siehe *BNetzA* Verfügung Nr. 46/2012 Amtsblatt 15/2012 v. 8.8.2012).

23 Nach der Rechtsprechung darf ein **Verbindungsnetzbetreiber,** der für einen Anbieter von Servicediensten dessen Servicerufnummer (zB 0180, 0900) realisiert und über den Teilnehmernetzbetreiber des Anrufers das Entgelt einzieht, diesem **nicht die vollständigen A-Rufnummern mitteilen** (aA *Schmitz* ZD 2012, 8ff.). Dieses Verbot sieht die Rechtsprechung jedenfalls so lange als einschlägig an, wie die Entgelte eingezogen werden können. Diese Rechtsprechung überzeugt nicht, da der Anbieter des Servicedienstes der Vertragspartner des Anrufers und Forderungsinhaber ist. Warum dieser die A-Rufnummern seines entgeltpflichtigen Kunden nicht kennen dürfen soll, überzeugt nicht (s. zur Kritik *Schmitz* ZD 2012, 8ff.). Gleichwohl hat sich diese Aufsichtspraxis bislang durchgesetzt.

III. Praxis und Ausblick auf ePrivacy-VO-E(KOM)

24 Die Regeln zum **Einzelverbindungsnachweis** haben sich im Großen und Ganzen **bewährt.** Die Bedeutung ist im Zeitalter der Nutzung von Flatrates zwar etwas geringer geworden. Es gibt aber immer noch Leistungen, die verbindungsabhängig abgerechnet werden. Diesbezüglich hat die Regelung ihre Bedeutung gewahrt. In der **Praxis** weitaus **wichtiger** sind jedoch die Regelungen zur Erhebung nachträglicher **Beanstandungen** bzw. Einwendungen gegen die Rechnung. Diesbezüglich enthalten TTDSG und TKG wiederum im Großen und Ganzen **bewährte Regelungen.**

25 Zum **Entwurf der ePrivacy-VO-E(KOM)** ist wiederum zu **kritisieren,** dass die erforderlichen Detailregelungen zu Einzelverbindungsnachweis und Bearbeitung von Einwendungen fehlen. Damit drohen Rückschritt und Verlust an Rechts-

sicherheit. Der Verordnungsgeber bleibt aufgefordert, die Regelungstiefe zu vergrößern oder ausreichend Öffnungsklauseln für nationale Zusatzregeln vorzusehen. Dies bedeutet, dass der bisherige Entwurf selbst für klassische Dienste unzureichend ist (*Schmitz* ZRP 2017, 172 (174)) und neuartige Dienste auch nicht angemessen regelt.

§ 12 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

(1) **[1]Soweit erforderlich, dürfen Verpflichtete nach § 3 Absatz 2 Satz 1 Verkehrsdaten der Endnutzer sowie die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind, verarbeiten, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. [2]Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Telekommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. [3]Eine Verarbeitung der Verkehrsdaten und Steuerdaten zu anderen Zwecken ist unzulässig. [4]Soweit die Verkehrsdaten nicht automatisiert erhoben und verwendet werden, muss der Datenschutzbeauftragte des Verpflichteten nach § 3 Absatz 2 Satz 1 unverzüglich über die Verfahren und Umstände der Maßnahme informiert werden. [5]Betroffene Endnutzer sind von dem nach § 3 Absatz 2 Satz 1 Verpflichteten zu benachrichtigen, sofern sie ermittelt werden können.**

(2) **Die Verkehrsdaten und Steuerdaten sind unverzüglich zu löschen, sobald sie für die Beseitigung der Störung nicht mehr erforderlich sind.**

(3) **[1]Zur Durchführung von Umschaltungen sowie zum Erkennen und Eingrenzen von Störungen im Netz ist dem Betreiber von Telekommunikationsnetzen oder seinem Beauftragten das Aufschalten auf bestehende Verbindungen erlaubt, soweit dies betrieblich erforderlich ist. [2]Eventuelle bei der Aufschaltung erstellte Aufzeichnungen sind unverzüglich zu löschen. [3]Das Aufschalten muss den betroffenen Kommunikationsteilnehmern durch ein akustisches oder sonstiges Signal zeitgleich angezeigt und ausdrücklich mitgeteilt werden. [4]Sofern dies technisch nicht möglich ist, muss der betriebliche Datenschutzbeauftragte des Betreibers des Telekommunikationsnetzes unverzüglich detailliert über die Verfahren und Umstände der Maßnahme informiert werden. [5]Diese Informationen hat der betriebliche Datenschutzbeauftragte für zwei Jahre aufzubewahren.**

(4) **[1]Wenn tatsächliche Anhaltspunkte für die rechtswidrige Inanspruchnahme eines Telekommunikationsnetzes oder Telekommunikationsdienstes vorliegen, insbesondere für eine Leistungserschleichung oder einen Betrug oder eine unzumutbare Belästigung nach § UWG § 7 des Gesetzes gegen den unlauteren Wettbewerb, darf der Verpflichtete nach § 3 Absatz 2 Satz 1 zur Sicherung seines Entgeltanspruchs sowie zum Schutz der Endnutzer vor der rechtswidrigen Inanspruchnahme des Telekommunika-**

tionsdienstes oder des Telekommunikationsnetzes Verkehrsdaten verarbeiten, die erforderlich sind, um die rechtswidrige Inanspruchnahme des Telekommunikationsnetzes oder Telekommunikationsdienstes aufzudecken und zu unterbinden. [2]Die Anhaltspunkte für die rechtwidrige Inanspruchnahme des Telekommunikationsnetzes oder Telekommunikationsdienstes hat der nach § 3 Absatz 2 Satz 1 Verpflichtete zu dokumentieren. [3]Der nach § 3 Absatz 2 Satz 1 Verpflichtete darf aus den Verkehrsdaten nach Satz 1 einen pseudonymisierten Gesamtdatenbestand bilden, der Aufschluss über die von einzelnen Endnutzern erzielten Umsätze gibt und unter Zugrundelegung geeigneter Kriterien das Auffinden solcher Verbindungen des Netzes ermöglicht, bei denen der Verdacht einer rechtswidrigen Inanspruchnahme besteht. [4]Die Verkehrsdaten anderer Verbindungen sind unverzüglich zu löschen. [5]Die Aufsichtsbehörde ist über Einführung und Änderung eines Verfahrens nach Satz 1 unverzüglich in Kenntnis zu setzen.

Literatur: *Assion* (Hrsg.), TTDSG, 2022; *Geppert/Schütz,* Beck'scher TKG-Kommentar, 4. Aufl., 2013; *Kiparski,* Die Telekommunikations-Datenschutzregelungen im neuen TTDSG, CR 2021, 482; *Riechert/Wilmer* (Hrsg.), TTDSG, 2022; *Schmitz,* E-Privacy-VO – unzureichende Regeln für klassische Dienste, ZRP 2017, 172; *Spindler/Schmitz* (Hrsg.), TMG, 2. Aufl., 2018; *Schwartmann/Jaspers/Eckhard* (Hrsg.), TTDSG, 2022; *Taeger/Gabel* (Hrsg.), DSGVO – BDSG – TTDSG, 4. Aufl., 2022; *Wehr/Ujica,* „Alles muss raus!" – Datenspeicherungs- und Auskunftspflichten der Access-Provider nach dem Urteil des BVerfG zur Vorratsdatenspeicherung, MMR 2010, 667.

Übersicht

	Rn.
I. Allgemeines	1
1. Entstehungsgeschichte	1
2. Sinn und Zweck der Norm	2
3. Systematik, Verhältnis zu anderen Vorschriften	5
II. Einzelkommentierung	8
1. Störungserkennung und -beseitigung	8
2. Erkennen und Unterbindung von Missbrauch	28
3. Verarbeitung von Bestandsdaten	35
III. Praxis und Ausblick auf ePrivacy-VO-E(KOM)	41

I. Allgemeines

1. Entstehungsgeschichte

1 **§ 12 übernimmt** weitgehend die bislang in **§ 100 TKG aF enthaltene Regelung** zur Störungs- und Missbrauchserkennung beim Betrieb von Telekommunikationsanlagen. Auch bei dieser Regelung könnte damit im Grundsatz weitgehend auf die bislang ergangene Rechtsprechung zu § 100 TKG aF sowie die Verwaltungspraxis und Literatur zurückgegriffen werden. Allerdings sind hierbei **Besonderheiten** zu beachten, die eine Anwendung der bisherigen Grundsätze stark einschränken.

2. Sinn und Zweck der Norm

Zunächst enthält § 12 **keine Regelung** mehr zur Verwendung von sog. **Bestandsdaten,** da diese in der ePrivacy-RL nicht konkret geregelt sind und sich nach Art. 95 DS-GVO die Verarbeitung dieser Bestandsdaten somit folglich nur nach der DS-GVO richtet. Es ist allerdings davon auszugehen, dass sich im Vergleich zur bisherigen Regelung im Ergebnis keine durchgreifende inhaltliche Änderung auch hinsichtlich der Verarbeitung von Bestandsdaten zu den genannten Zwecken ergibt (→ Rn. 35). **2**

Zudem ist die **Rechtsprechung des EuGH** (Urt. v. 19.10.2016 – C-582/14) zur Zulässigkeit von Sicherheitsmaßnahmen bei Webseiten (zu § 15 TMG aF) zu beachten und auf die Anwendung von **§ 12 zu übertragen.** Damit verbietet sich im Ergebnis eine zu enge am Wortlaut orientierte Anwendung von § 12, welche es dem Anbieter ohne Abwägung seines berechtigten Interesses verbieten würde, seiner Verpflichtung (§§ 165, 63 Abs. 2 TKG, Art. 4 ePrivacy-RL) zur Gewährung von Funktion und Sicherheit nachzukommen. **3**

§ 12 regelt im Wesentlichen zwei Fälle. Zum einen dürfen **Störungen** gem. der Abs. 1–3 einschließlich einer möglichen Aufschaltung (Abs. 3) erkannt und beseitigt werden. Abs. 4 regelt dann die Erkennung und Unterbindung einer **Leistungserschleichung** und anderer **Missbrauchsfälle** durch Verarbeitung der Verkehrsdaten. Beide Fälle sind voneinander zu unterscheiden und getrennt zu behandeln. In der Praxis kann es allerdings vorkommen, dass ein Anbieter zunächst sowohl eine Störung oder aber einen Missbrauch vermuten muss und damit in beide Richtungen ermittelt. **4**

3. Systematik, Verhältnis zu anderen Vorschriften

§ 12 basiert auf **Art. 15 Abs. 1 der ePrivacy-RL.** Nach **Erwgr. 29** dieser Richtlinie können Dienstanbieter Verkehrsdaten in Bezug auf Teilnehmer und Nutzer in Einzelfällen verarbeiten, „um technische Versehen oder Fehler bei der Übertragung von Nachrichten zu ermitteln. Für Fakturierungszwecke notwendige Verkehrsdaten dürfen ebenfalls vom Diensteanbieter verarbeitet werden, um Fälle von Betrug, die darin bestehen, die elektronischen Kommunikationsdienste ohne entsprechende Bezahlung nutzen, ermitteln und abstellen zu können." **5**

Die Ausführungen des Erwgr. sind aber nicht als Beschränkung zu verstehen. Denn es ist die **EuGH-Rechtsprechung** zur Zulässigkeit von Sicherheitsmaßnahmen bei **Webseiten** (*EuGH* Urt. v. 19.10.2016 – C-582/14) sowie die Verpflichtung nach **Art. 4 ePrivacy-RL** und **§ 165 TKG** zu **beachten.** Hiernach hat der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. Diese Sicherheitsmaßnahmen dienen ausdrücklich auch dem Schutz personenbezogener Daten. Deshalb hat ein Anbieter auch die entsprechenden Rechte zum Aufdecken und Erkennen von Störungen und Missbrauch in entsprechender **richtlinienkonformer Auslegung von § 12.** Gleiches gilt für die Funktionsgewährleistung und damit die Störungsbearbeitung. **6**

Verstöße gegen bestimmte Pflichten in § 12 sind **bußgeldbewehrt,** s. im Einzelnen § 28 Abs. 1 Nr. 4, Nr. 5, Nr. 6 und Nr. 7. Auch hierbei ist allerdings zu bedenken, dass der Wortlaut des § 12 zu eng ist. An der Bestimmtheit und Geltung **7**

des § 28 Abs. 1 Nr. 4, der eine Verarbeitung entgegen § 12 Abs. 1 sanktioniert, bestehen deshalb Bedenken, da dieser Tatbestand im Ergebnis gesetzlich **nicht ausreichend bestimmt** ist.

II. Einzelkommentierung

1. Störungserkennung und -beseitigung

8 **Berechtigte** zur Datenverarbeitung sind die **Anbieter** gem. § 3 Abs. 2 S. 1. Diese dürfen nach der Grundregel des § 12 Abs. 1 S. 1 Verkehrsdaten der Endnutzer sowie die Steuerdaten, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf dem den am Kommunikationsvorgang beteiligten Server gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind, verarbeiten, um **Störungen** oder **Fehler** an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen.

9 **a) Telekommunikationsanlage und Erweiterung auf Netz und Dienste.** Voraussetzung für diese Erlaubnis zur Datenverarbeitung ist nach dem Wortlaut von § 12 Abs. 1 S. 1 zunächst, dass ein **Fehler** oder eine **Störung** einer **Telekommunikationsanlage** vorliegt oder möglich sein könnte. Telekommunikationsanlagen sind nach § 3 Nr. 60 TKG technische Einrichtungen, Systeme oder Server, die als Nachrichten identifizierbare elektromagnetische oder optische Signale oder Daten im Rahmen der Erbringung eines Telekommunikationsdienstes senden, übertragen vermitteln, empfangen, steuern oder kontrollieren können. Umfasst werden somit sowohl die Vermittlungsanlage als auch das Netz als Ganzes, da die Datenübertragung durch diese Systeme als Ganzes stattfindet.

10 **Umstritten** ist, ob auch **Fakturierungssysteme bzw. Billingsysteme** als Telekommunikationsanlage gelten und der Anbieter damit auch Verkehrsdaten zum Erkennen von Störungen an diesen Systemen nach § 12 verarbeiten darf. Insofern wurde zu § 100 TKG aF vertreten, dass diese Fakturierungssysteme nicht miterfasst werden, da sie von der Legaldefinition der Telekommunikationsanlage dem Wortlaut nach nicht erfasst sind (zu § 100 TKG aF siehe u.a. Geppert/Schütz/*Braun* TKG § 100 Rn. 6). Hierfür wurde auch Erwgr. 29 angeführt, der insofern auch nur von Fehlern bei der Übertragung von Nachrichten und deren Ermittlung spricht.

11 Diese **enge Sichtweise** ist durch das Urteil des **EuGH** zur Sicherheit bei Webseiten nach § 15 TMG **überholt.** Diese Rechtsprechung (*EuGH* Urt. v. 19.10.2016 – C-582/14, NJW 2016, 3579) ist auf die Anwendung von § 12 zu übertragen. Sie führt dazu, dass über den zu engen Wortlaut des § 12 angemessene Maßnahmen zur Störungsbeseitigung und Funktionsgewährleistung umfassend für die Telekommunikationsdienste und das Telekommunikationsnetz einschließlich der Fakturierungssysteme datenschutzrechtlich zulässig und nach Art. 4 ePrivacy-RL, §§ 165, 63 Abs. 2 TKG erforderlich sind.

12 Der **EuGH** hat zu § 15 TMG aF geurteilt, dass dessen Wortlaut keine ausreichenden Möglichkeiten zur Verarbeitung von personenbezogenen Daten zu Zwecken der Sicherheit zulasse und damit in seiner **engen Auslegung gegen EU-Recht** verstoße. Vielmehr sei eine **Erlaubnis durch Abwägung der berechtigten Interessen** nach Art. 7 lit. f DSRL zu beachten, wie im Anschuss auch der BGH auf Basis des EuGH-Urteils bestätigt hat. Die **Verarbeitung personenbezogener Daten** sei nach Art. 7 lit. f der RL 95/46/EG **rechtmäßig,** wenn sie zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung

Verantwortlichen oder von dem/den Dritten wahrgenommen wird, denen die Daten übermittelt werden, erforderlich ist, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Die deutsche Regelung schränke bei enger Auslegung die Tragweite dieses Grundsatzes ein, indem sie es ausschließe, dass der Zweck, die generelle Funktionsfähigkeit des Online-Mediums zu gewährleisten, Gegenstand einer Abwägung mit dem Interesse oder den Grundrechten und Grundfreiheiten der Nutzer sein kann.

Ein Webseitenbetreiber darf deshalb in **richtlinienkonformer Auslegung** nach Art. 7 lit. f DSRL (bzw. nun Art. 6 lit. f DS-GVO) auch ohne Einwilligung des Nutzers sogar über das Ende eines Nutzungsvorgangs hinaus personenbezogene Daten (Nutzungsdaten) dann erheben und verwenden, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten. Diese Erforderlichkeit besteht auch zur Verwirklichung des berechtigten Interesses des Anbieters, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gem. Art. 1 Abs. 1 DSRL geschützt sind, überwiegen (s. auch zu § 15 TMG aF Spindler/Schmitz/*Schmitz* TMG § 15 Rn. 4–7). **13**

Nach BGH (Urt. v. 16.5.2017 – VI ZR 135/17 Rn. 41 ff.) sind hierbei konkrete **Feststellungen** zu den **Tatsachen** erforderlich, aus denen sich das jeweilige Interesse ergibt. Hierbei spielt das Maß des Personenbezugs der Daten und demzufolge auch das Maß der Schutzbedürftigkeit der Daten eine entscheidende Rolle für die Frage, welches „berechtigtes Interesse" des Anbieters anerkannt wird und wie die Abwägung mit dem Schutzbedürfnis des Betroffenen ausfällt. Es kommt deshalb von vornherein zu einer entsprechenden Wechselwirkung (Spindler/Schmitz/*Schmitz* TMG § 15 Rn. 51–53). **14**

Diese **Grundsätze** sind auf **§ 12 zu übertragen,** auch soweit es die **Störungsbearbeitung sowie die Missbrauchsbekämpfung betrifft.** Eine Verarbeitung zur Störungsbearbeitung und Missbrauchsbekämpfung ist damit zulässig, soweit ihre Erhebung und ihre Verwendung erforderlich ist, um die generelle Funktionsfähigkeit der Dienste einschließlich deren Abrechenbarkeit zu gewährleisten. Diese Erforderlichkeit besteht auch zur Verwirklichung des berechtigten Interesses des Anbieters, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. **15**

Hierbei ist gem. der Rechtsprechung des **BGH** (Urt. v. 16.5.2017 – VI ZR 135/17 Rn. 41) zu berücksichtigen, dass vorliegend **Telefonnummern** und ggf. **IP-Adressen** durch den Anbieter verarbeitet werden und damit im Regelfall von einem **größeren Personenbezug** und einem höheren Schutzbedürfnis auszugehen ist, als wenn ein Webseitenbetreiber ihm im Regelfall unbekannte IP-Adressen verarbeitet. Allerdings ist auch zu bedenken, dass der Anbieter von vornherein diese Daten zur Leistungserbringung verarbeiten muss und damit auch der Kreis der Personen, die Kenntnis von diesen Daten erhalten, nicht vergrößert wird. **16**

Zudem ist die weitere auf dem **EuGH-Urteil basierende nationale Rechtsprechung** zur **Datenverarbeitung** (*VG Hamburg* Beschl. v. 24.4.2017 – 13 E 5912/16, BeckRS 2017, 111797; s. ähnlich auch *OLG Karlsruhe* Urt. v. 9.5.2012 – 6 U 38/11) zu beachten. Hiernach ist diese zulässig und erforderlich, wenn bei vernünftiger Betrachtung das Angewiesensein auf das infrage stehende Mittel zu bejahen und ein Verzicht auf die Daten nicht sinnvoll oder unzumutbar ist. Dabei ist, wenn ein Vertragsverhältnis besteht, die Erforderlichkeit vor dem Hin- **17**

tergrund des Rechtsfertigungstatbestands (damals noch § 28 Abs. 1 Nr. 1 BDSG aF) eng auszulegen, weil sich der Vertragspartner grundsätzlich darauf verlassen können soll, dass seine Daten nur für den Zweck verwendet werden, zu dem er sie gegeben hat. Wann die Nutzung personenbezogener Daten für die Verfolgung eines berechtigten Interesses erforderlich im genannten Sinne ist, hängt auch davon ab, in welchem Maße die Interessen des Betroffenen Schutz verdienen; je mehr Schutz sie verdienen, desto eher kann dem Nutzenden eine alternative, wenn auch weniger effiziente Art der Verfolgung seines berechtigten Interesses ohne Nutzung der personenbezogenen Daten zugemutet werden. Da die gesamte Datenverwendung aufgrund des Gesetzesvorbehalts (damals noch § 4 Abs. 1 BDSG aF) grundsätzlich verboten ist, muss im Regelfall die verantwortliche Stelle die Zulässigkeit der Datenverarbeitung beweisen (s. insgesamt entsprechend zu § 15 TMG aF Spindler/Schmitz/*Schmitz* TMG § 15 Rn. 60–62).

18 Bei einer **Abwägung** überwiegen deshalb im Regelfall nicht die Interessen der Nutzer an einem Unterlassen dieser Verarbeitung zur Aufrechterhaltung der Funktionsfähigkeit der Dienste, Netze und der Abrechnung. Zwar ist der Personenbezug und die Schutzbedürftigkeit der Verkehrsdaten als sehr hoch einzustufen, den Nutzern ist aber bewusst, dass der Anbieter diese Daten zur Leistungserbringung verwendet, und erwartet entsprechende Sicherheitsmaßnahmen. Die Sicherung der Funktionsfähigkeit von Netz und Diensten einschließlich der **Überprüfung der Fakturiersysteme** auf eine Störung sowie die Missbrauchsbekämpfung sind nur unter angemessener Verarbeitung der Verkehrsdaten sinnvoll und möglich. Bei dieser Abwägung ist zu berücksichtigen, dass der Anbieter eine **vertragliche** und **gesetzliche Verpflichtung** hat, diese Funktionsfähigkeit der Dienste und Netze (§ 165 TKG) und deren Abrechnung (§§ 165, 63 Abs. 2 TKG) zu gewährleisten sowie Missbrauch und Angriffe zu verhindern (§ 165 TKG, Art. 32 DS-GVO). Bei der Beurteilung, ob dieser Verarbeitung ein Interesse des Betroffenen entgegensteht, ist dies ebenfalls mit einzustellen.

19 **b) Fehler oder Störung.** Das Erheben der Verkehrsdaten nach § 12 Abs. 1 muss dem Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen dienen. Hierbei ist insbesondere strittig, wie der **Begriff einer Störung** zu verstehen ist und auf welche Funktionen sich dieser beziehen muss.

20 Nach Ansicht des **BGH** (Urt. v. 16.5.2017 – VI ZR 135/17 Rn. 41) ist der Begriff der Störung sehr weitgehend zu verstehen als jede nicht gewollte Veränderung der vom Anbieter für sein Telekommunikationsangebot genutzten technischen Einrichtungen. Eine solche Störung liegt nach Auffassung des BGH daher auch dann bereits vor, wenn zum Beispiel Internetdienstleister bestimmte IP-Adressbereiche eines anderen Anbieters sperren, weil von Ihnen Schadprogramme ausgesendet werden. Auch in diesem Falle läge eine Veränderung der Telekommunikationsanlage vor, da diese nicht mehr wie vorgesehen nutzbar sei. Insbesondere setzt die Befugnis zur Datenverarbeitung nach Ansicht des BGH nicht voraus, dass im Einzelfallfall bereits Anhaltspunkte für eine Störung oder einen Fehler an der Telekommunikationsanlage vorlegen. Es genüge vielmehr, dass die in Rede stehende Datenverarbeitung erforderlich, geeignet und im engeren Sinne verhältnismäßig sei, um abstrakten Gefahren für die Funktionstüchtigkeit des Telekommunikationsbetriebes entgegenzuwirken.

21 Diese weite Auslegung des **BGH** zu § 100 TKG aF ist auf **Kritik** gestoßen (s. im Einzelnen Geppert/Schütz/*Braun* TKG § 100 Rn. 11).