
Datum: 25.04.2025
Gericht: Verwaltungsgericht Köln
Spruchkörper: 1. Kammer
Entscheidungsart: Urteil
Aktenzeichen: 1 K 6109/21
ECLI: ECLI:DE:VGK:2025:0425.1K6109.21.00

Schlagworte: Infrastrukturatlas, Ausnahmen, Ausnahmetatbestände, feststellender Verwaltungsakt

Normen: TKG § 79 Abs. 3

Leitsätze:

Bei der Entscheidung der Bundesnetzagentur über die Ausnahme von Informationen aus dem Infrastrukturatlas (§ 79 Abs. 3 TKG) handelt es sich um einen feststellenden Verwaltungsakt. Dessen Erlass kann im Wege der Verpflichtungsklage (§ 42 Abs. 1 Alt. 2 VwGO) verfolgt werden.

Maßgeblicher Zeitpunkt für die Beurteilung der Rechtmäßigkeit der Entscheidung der Bundesnetzagentur über die Ausnahme von Informationen aus dem Infrastrukturatlas (§ 79 Abs. 3 TKG) ist der Zeitpunkt der letzten mündlichen Verhandlung oder Entscheidung des Gerichts.

Für das Vorliegen der Ausnahmetatbestände des § 79 Abs. 3 Satz 1 TKG genügen konkrete Anhaltspunkte. Es müssen bestimmte, auf den Einzelfall bezogene und überprüfbare Anknüpfungstatsachen gegeben sein. Einer Überzeugung bedarf es nicht. Die bloße Möglichkeit oder reine Vermutung, ein nicht durch Tatsachen belegbarer Verdacht oder allgemeine statistische Wahrscheinlichkeiten reichen indes nicht.

Bei den in § 79 Abs. 3 Satz 1 Nr. 1 TKG genannten Schutzgütern handelt es sich um unbestimmte Rechtsbegriffe. Diese bedürfen der Auslegung und unterliegen der vollständigen gerichtlichen Kontrolle. Für die Auslegung ist auf das jeweilige unionsrechtliche Begriffsverständnis abzustellen.

Die Gefährdung der in § 79 Abs. 3 Satz 1 Nr. 1 TKG genannten Schutzgüter muss aus der Einsichtnahme nach § 79 Abs. 4 TKG folgen, mithin aus einer rechtmäßigen Einsichtnahme in den Infrastrukturatlas. Nicht erfasst sind Gefahren, die aus einer etwaigen rechtsmissbräuchlichen Verwendung der aus der Einsichtnahme gewonnenen Informationen oder einer unberechtigten Einsichtnahme in den Infrastrukturatlas folgen.

Für eine Ausnahme nach § 79 Abs. 3 Satz 1 Nr. 1 TKG genügen gesetzliche Schutz- und Vertraulichkeitspflichten ebenso wenig wie private Geheimhaltungsvereinbarungen.

Der Ausnahmetatbestand des § 79 Abs. 3 Satz 1 Nr. 2 TKG knüpft die Verletzung der Vertraulichkeit nach § 148 TKG an die Einsichtnahme nach § 79 Abs. 4 TKG an, mithin an eine rechtmäßige Einsichtnahme. Nicht erfasst sind Vertraulichkeitsverletzungen, die aus einem rechtswidrigen Umgang mit den gewonnenen Informationen oder aus einer unberechtigten Einsichtnahme in den ISA herrühren.

Für eine Ausnahme nach § 79 Abs. 3 Satz 1 Nr. 2 TKG genügt es nicht, dass es sich bei den Informationen um Betriebs- und Geschäftsgeheimnisse handelt oder diese einer privaten Geheimhaltungsvereinbarung unterliegen.

Der Ausnahmetatbestand des § 79 Abs. 3 Satz 1 Nr. 3 TKG kommt nur für Infrastrukturen in Betracht, die durch Gesetz oder aufgrund Gesetzes als Kritische Infrastrukturen bestimmt worden sind (hier verneint).

Der Ausnahmetatbestand des § 79 Abs. 3 Satz 1 Nr. 4 TKG ist auf eine Nutzung der Infrastruktur durch den Bund beschränkt. Eine analoge Anwendung auf Landes- oder kommunale Behörden kommt mangels planwidriger Regelungslücke nicht in Betracht.

Rechtskraft: nicht rechtskräftig

Tenor:

Das Verfahren wird eingestellt, soweit die Beteiligten es in der mündlichen Verhandlung übereinstimmend für in der Hauptsache erledigt erklärt haben.

Im Übrigen wird die Klage abgewiesen.

Die Kosten des Verfahrens tragen die Beteiligten je zur Hälfte.

Tatbestand

1

2

Die Beteiligten streiten um die Aufnahme von Daten in den Infrastrukturatlas (fortan: ISA). Dabei handelt es sich um ein webbasiertes Geoinformationssystem mit Daten über Einrichtungen öffentlicher Versorgungsnetze, die zu Telekommunikationszwecken genutzt werden können. Der ISA wird von der beklagten Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (fortan: BNetzA) geführt und soll die Planung des Breitbandausbaus in I. fördern. Er ist nicht öffentlich einsehbar. Berechtigte Nutzer erhalten auf Antrag einen gesicherten Zugang.

Die Klägerin ist ein kommunales Versorgungsunternehmen im Bereich Strom, Erdgas und Trinkwasser. Sie bietet auch Telefon- und Internetprodukte an und verfügt hierfür über ein eigenes Glasfasernetz. 3

Unter dem 17. Januar 2013 schlossen die Beteiligten einen Vertrag über die Teilnahme am bundesweiten Infrastrukturatlas. Darin verpflichtete sich die Klägerin zur Bereitstellung von Daten an den ISA und jährlichen Aktualisierungen. Ausgenommen wurden Daten über Infrastrukturen nach dem letzten Konzentrations- oder Verteilerpunkt (z.B. Netzanschlussleitungen von Letztverbrauchern und Erzeugern) sowie Verschlusssachen nach den Sicherheitsüberprüfungsgesetzen des Bundes und der Länder. Auch Trinkwasserleitungen sowie Einrichtungen, deren ausschließlicher Betriebszweck die Erfüllung der Versorgungsaufgabe des Strom- oder Gasverteilungsnetzes ist (z.B. Stromleitungen, Ortsnetzstationen, Umspannanlagen, Gasleitungen, Kupfernachrichtenkabel) wurden aus dem Anwendungsbereich der Datenlieferungspflicht herausgenommen. 4

Am 20. Dezember 2013 stellte die Klägerin der BNetzA erstmals Daten für den ISA zur Verfügung und aktualisierte diese in den Jahren 2014 bis 2016. Die Daten bezogen sich auf Glasfaser, Leerrohre und Zugangspunkte und wurden jeweils in den ISA übernommen. 5

Nachdem die rechtlichen Grundlagen des ISA mit dem Gesetz zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze vom 4. November 2016 (fortan: DigiNetzG) neu gefasst worden waren, schlossen die Beteiligten am 27. Oktober 2017 einen neuen Vertrag über die Teilnahme am Infrastrukturatlas der zentralen Informationsstelle des Bundes gemäß § 77a Abs. 1 Nr. 1 TKG a.F. (sog. ISA-Planung). Die Klägerin verpflichtete sich darin erneut zur Lieferung von Daten über passive Netzinfrastrukturen, einschließlich Richtfunkstrecken und Glasfaserkabeln. Ausgenommen waren Kupferkabel und andere kupferbasierte Infrastrukturen, Kabelinfrastrukturen des Teilnehmeranschlusses nach dem letzten Konzentrations- oder Verteilerpunkt, Trinkwasserleitungen, Gas- und Fernwärmerohre sowie Elektrizitätskabel. Unter Ziffer 2 des Vertrags wurde auf die Möglichkeit hingewiesen, nach § 77a Abs. 4 TKG a.F. eine Ausnahme von der Veröffentlichung im ISA-Planung zu beantragen. 6

Am 12. Juli 2018 stellte die Klägerin der BNetzA erstmals auf Grundlage des neuen Vertrages Daten über ihre Infrastruktur zur Verfügung. Mit Schreiben vom 26. März 2019 beantragte sie für Teile der Leerrohre, Glasfaserkabel, Zugangspunkte sowie für alle Multifunktionsgehäuse eine Ausnahme nach § 77a Abs. 4 Satz 1 TKG a.F. Zur Begründung führte sie aus, dass diese Infrastrukturen der Ansteuerung von Mittelspannungsschaltanlagen in den Ortsnetzstationen und Umspannwerken, der Ansteuerung und Überwachung von Trinkwasserversorgungsanlagen (Wasserwerke, Brunnenanlagen, Hochbehälter, Druckerhöhungsanlagen und Schachtbauwerke), dem Landesnetz M. im Bereich der Stadt C. zur Vernetzung der Landesbehörden (Finanzamt, Gerichte, Polizei, Gesundheitsamt, Landratsamt, Feuerwehr), sowie der Vernetzung der Gebäude von Banken untereinander dienen. Es handele sich um Infrastrukturen, die als kritische Infrastrukturen bestimmt worden seien. Eine Veröffentlichung dieser Daten widerspreche den Anforderungen der DIN ISO/IEC 7

27001:2017, nach der sie zertifiziert sei. Die genannten Infrastrukturen seien auch nachweislich besonders schutzbedürftig und für die Funktionsfähigkeit der kritischen Infrastruktur maßgeblich, weil bei einer Störung oder Zerstörung die gesamte Strom- und Wasserversorgung der Stadt C. massiv gefährdet sei bzw. ausfallen könne. Im Bereich des Landesnetzes könne es zu einer Gefährdung der Bevölkerung kommen, da die Kommunikation und Koordination der Behörden (z.B. im Katastrophenfall) ausfalle, der Datenschutz nicht mehr gewährleistet sei und sensible Daten offengelegt werden könnten. Zudem sei die Vertraulichkeit der Bankdaten gefährdet.

Mit Schreiben vom 19. Februar 2020 hörte die BNetzA die Klägerin zur beabsichtigten Ablehnung ihres Antrags an. 8

Am 18. März 2020 übermittelte die Klägerin der BNetzA ihre jährliche Datenaktualisierung für den ISA und verwies für Teile der Daten auf ihren Ausnahmeantrag vom 26. März 2019. Nach Auswertung der BNetzA beinhaltete die Lieferung erstmals Daten zu zwei Hauptverteilern. 9

Im Rahmen der Anhörung nahm der Prozessbevollmächtigte der Klägerin unter dem 29. Mai 2020 Stellung. Er führte aus, dass die Klägerin den Sicherheitsanforderungen der DIN ISO/IEC 27001:2017 und 27019 unterliege. Diese definierten ein Managementsystem für die Informationssicherheit („Information Security Management System“, fortan: ISMS) und würden für sämtliche Sparten der Klägerin (Strom-, Gas-, Wasser- und Wärmeversorgung sowie Telekommunikation) gelten. Auf dieser Basis habe die Klägerin eine Sicherheitsrichtlinie erarbeitet mit Maßnahmen zur physischen und umgebungsbezogenen Sicherheit sowie zur Sicherheit von Informationen bzw. Informationssystemen. Informationen zur Leittechnik (Leerrohre, Glasfaserkabel, Spleißpläne, OTDR-Messung) seien daher besonders vertraulich zu behandeln. 10

Des Weiteren sei zu berücksichtigen, dass die DIN ISO/IEC 27001 und 27019 zu den Standards gehöre, die Betreiber kritischer Infrastrukturen nach § 8a Abs. 1 BSIG zu gewährleisten hätten. Bei der Netzleittechnik handele es sich für die Energieversorgung um kritische Infrastruktur i.S.d. BSI-KritisV. Da die Infrastruktur zugleich für Versorgungszwecke anderer Sparten genutzt würde, bestehe auch eine besondere Schutzbedürftigkeit. Daneben verfüge die Klägerin über ein Glasfasernetz, mit dem ausschließlich die Steuerfunktionen für das Wasserwerk durchgeführt würden. 11

Neben der BSI-KritisV sei auch der Umsetzungsplan Kritische Infrastrukturen (fortan: UP KRITIS) zu berücksichtigen. Dieser stärke besonders präventive Aspekte. Hierzu gehörten auch Schutzmaßnahmen zur Vertraulichkeit von Informationen über kritische Infrastrukturen. 12

Schließlich würde die Zertifizierung der Klägerin nach § 11 EnWG infrage gestellt, wenn die Daten veröffentlicht würden. Die Zertifizierung beziehe sich auf sämtliche Standorte einschließlich LWL-Central Offices, TK-Stationen, TK-Verteiler und TK-Schächte. Nach § 11 Abs. 1a Satz 1 EnWG umfasse der Betrieb eines sicheren Energieversorgungsnetzes insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig seien. § 11 EnWG gelte für alle Energieversorgungsnetzbetreiber, nicht nur für Betreiber kritischer Infrastrukturen nach der BSI-KritisV. Auch Telekommunikationsnetzbetreiber unterlägen unabhängig von ihrer Einstufung als kritisch den Meldepflichten des § 109 Abs. 5 TKG a.F. 13

- Hinsichtlich der für das Landesnetz M. genutzten Glasfaserleitungen handele es sich zum einen schon gar nicht um ein öffentliches Versorgungsnetz, das der Datenlieferungspflicht unterfalle. Zum anderen müsse der Ausnahmetatbestand des § 77a Abs. 4 Satz 1 Nr. 4 TKG a.F. über seinen Wortlaut hinaus die sichere Kommunikation von Landesbehörden umfassen. Eine Beschränkung auf den Bund sei nicht gerechtfertigt. Es gehe funktional um den Schutz von Infrastrukturen, die zur Erfüllung staatlicher Aufgaben eingesetzt würden.
- Davon unabhängig sei die Klägerin hinsichtlich des Landesnetzes M. vertraglich zur Geheimhaltung verpflichtet. Dies ergebe sich aus Ziffer 00 ihres Vertrages mit der A. GmbH über die Bereitstellung von Glasfaserinfrastrukturen für das Landesnetz M.. Eine Einsichtnahme über den ISA würde daher die Vertraulichkeit nach § 77m TKG a.F. verletzen, sodass der Ausnahmetatbestand des § 77a Abs. 4 Satz 1 Nr. 2 TKG a.F. erfüllt sei. 15
- Mit Bescheid vom 29. Juni 2021 – zugestellt am 30. Juni 2021 – lehnte die BNetzA den Antrag auf Ausnahme der am 12. Juli 2018 und 26. März 2019 gelieferten Daten ab. Zur Begründung führte sie aus, dass kein Ausnahmetatbestand vorliege: 16
- Zu § 77a Abs. 4 Satz 1 Nr. 1 TKG a.F. habe die Klägerin nichts vorgetragen. 17
- § 77a Abs. 4 Satz 1 Nr. 2 TKG a.F. sei nicht erfüllt. Es gebe keine konkreten Anhaltspunkte für die Annahme, dass eine Einsichtnahme die Vertraulichkeit nach § 77m TKG a.F. verletzen würde. Die öffentlich-rechtliche Verpflichtung zur Lieferung von Daten an den ISA könne nicht durch den Abschluss privater Geheimhaltungsvereinbarungen entfallen. Zudem sei eine unberechtigte Nutzung der Daten infolge der nur vergrößerten Darstellung der Daten im ISA deutlich erschwert. Eine missbräuchliche Nutzung der Daten sei durch § 77m TKG a.F. untersagt. Ein Verstoß begründe zudem ggf. Schadensersatzansprüche. 18
- § 77a Abs. 4 Satz 1 Nr. 3 TKG a.F. liege ebenfalls nicht vor. Die Klägerin habe nicht dargelegt, dass ihre Infrastrukturen die maßgeblichen Schwellenwerte im Anhang der BSI-KritisV überschritten. Davon unabhängig habe sie weder eine besondere Schutzbedürftigkeit noch eine Maßgeblichkeit für die Funktionsfähigkeit der kritischen Infrastruktur nachgewiesen. Ihre Ausführungen zu § 8a BSI-Gesetz seien zu pauschal. Soweit aus anderen Gesetzen Sicherheitspflichten folgten (hier § 11 EnWG), gingen diese den Datenlieferungspflichten aus § 77a TKG a.F. nicht vor. Der Gesetzgeber habe auf eine entsprechende Einschränkung verzichtet, sodass die jeweiligen Pflichten und die damit verbundenen Ziele (Versorgungssicherheit auf der einen und Breitbandausbau auf der anderen Seite) gleichrangig nebeneinander stünden. Durch die Beschränkung der Einsichtnahme werde den widerstreitenden Interessen genüge getan. 19
- Hinsichtlich des Landesnetzes Saarlands betreffe der Einwand, die Daten unterfielen nicht der Datenlieferungspflicht, die erste Stufe des Verfahrens. Streitgegenständlich sei hingegen die zweite Stufe der Ausnahme von einer Veröffentlichung. Im Übrigen bestünden keine Anhaltspunkte dafür, dass es sich um ein geschlossenes Behördennetz handele. Mit Blick auf die Kennzeichnung in der Datenlieferung sei vielmehr davon auszugehen, dass das Landesnetz mit Teilen von Infrastrukturen (z.B. Glasfaserkabeln) betrieben werde, die auch der öffentlichen Telekommunikationssparte der Klägerin dienen. Davon unabhängig sei § 77a Abs. 4 Satz 1 Nr. 4 TKG a.F. nicht erfüllt. Der Wortlaut sei eindeutig auf den Bund beschränkt. Mit Blick auf den Zweck des ISA seien die Ausnahmetatbestände eng auszulegen. 20
- Die Vollziehung des Bescheids setzte die BNetzA mit E-Mail vom 29. Juni 2021 bis zu dessen Unanfechtbarkeit aus, sodass bis heute keine Darstellung der streitgegenständlichen 21

Daten im ISA erfolgt.

Mit Schreiben vom 1. Juli 2021 hörte die BNetzA die Klägerin zur beabsichtigten Ablehnung des Ausnahmeantrags hinsichtlich der zwei Hauptverteiler an. Unter dem 8. September 2021 nahm die Klägerin dahingehend Stellung, dass es sich um sog. Central Offices und damit um vertrauliche, besonders schutzbedürftige Informationen handele, die für die Funktionsfähigkeit des Netzes als kritische Infrastruktur maßgeblich seien. 22

Am 22. Juli 2021 legte die Klägerin Widerspruch gegen den Bescheid vom 29. Juni 2021 ein. Zur Begründung führte sie – in Ergänzung ihrer vorherigen Stellungnahmen – aus: Der Vertrag mit der A. GmbH beinhalte die Überlassung dedizierter Glasfaserkabelstrecken zur freien und unbeschränkten Nutzung für das Landesnetz M., das die A. GmbH als Auftragnehmerin des Landes M. realisiere. Die hierfür bereitgestellten Glasfaserkabel dienten ausschließlich der Informationsübertragung für das Landesnetz. Physisch-technisch handele es sich um ein geschlossenes Behördennetz. Die entsprechenden Glasfaserkabel seien in Microrohre (Speedpipes) eingebracht, die ihrerseits per Schutzummantelung zu Microduct-Systemen verbunden seien. In einen Erdgraben seien in der Regel mehrere Microduct-Systeme eingebracht (vgl. Foto in Beiakte Heft 1, Bl. 311). Die für das Landesnetz M. bereitgestellten Glasfaserkabel seien trotz der gemeinsamen Verlegung und Wegeführung physisch eindeutig von anderen Glasfaserkabeln zu unterscheiden. Teilweise erfolge auch eine eigene Wegeführung, etwa zum Anschluss einzelner Behörden. 23

Die Glasfaserkabel bzw. Microduct-Systeme würden in den zwei Hauptverteilern eingeführt, die zugleich als Koppelungs- bzw. Übergabestellen für das Landesnetz M. dienten. Die entsprechenden Zugangsregelungen zu den zwei Koppelungspunkten seien im Vertrag mit der A. GmbH enthalten. Funktional seien diese Hauptverteiler daher ebenfalls Teil des Landesnetzes M.. Insoweit bestehe ein inhaltlicher Zusammenhang zwischen den zwei Verwaltungsverfahren. 24

In rechtlicher Hinsicht ergänzte die Klägerin, dass private Geheimhaltungsvereinbarungen nicht aus dem Regelungsumfang des § 77m TKG a.F. ausgegrenzt werden dürften. Die Gesetzesbegründung verweise auf den Schutz von Betriebs- und Geschäftsgeheimnissen und die zugrunde liegende Richtlinie 2014/61/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Maßnahmen zur Reduzierung der Kosten des Ausbaus von Hochgeschwindigkeitsnetzen für die elektronische Kommunikation (fortan: Kostensenkungsrichtlinie). 25

§ 77a Abs. 2 Satz 1 Nr. 4 TKG a.F. könne nicht dahingehend ausgelegt werden, dass „ausschließlich“ die Behördenkommunikation von Bundesbehörden erfasst sei. Weder enthalte der Wortlaut eine solche strikte Begrenzung, noch entspreche dies dem Sinn und Zweck der Vorschrift. Zumindest die Kommunikation zwischen Bundes- und Landesbehörden müsse umfasst sein. Hierfür sprächen Art. 91c Abs. 1 GG und das auf dieser Grundlage ergangene Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder. Danach sei im Bereich der Informationstechnik eine Bund-Länder-Zusammenarbeit vorgesehen, etwa durch ein Verbindungsnetz zwischen Bund und Ländern. 26

Mit Widerspruchsbescheid vom 2. November 2021 – zugestellt am 4. November 2021 – wies die BNetzA den Widerspruch der Klägerin zurück. Zur Begründung führte sie ergänzend aus, dass die Datenlieferungspflicht der Klägerin auch die Daten der für das Landesnetz M. genutzten Glasfaserkabel umfassten. Diese seien Teil eines öffentlichen Versorgungsnetzes, weil die Klägerin über ihr Netz öffentlich Telekommunikationsdienstleistungen bereitstelle. Dass einzelne Einrichtungen dieses Netzes nicht öffentlich zugänglich seien, sei 27

unbeachtlich. Nach der Gesetzesbegründung sei das öffentliche Versorgungsnetz als Ganzes zu betrachten. Davon unabhängig verdeutliche ein Umkehrschluss zu § 77a Abs. 2 Satz 1 Nr. 4 TKG a.F., dass auf der ersten Stufe Daten auch zu Behördennetzen zu liefern seien.

Ein Ausnahmetatbestand sei nicht gegeben. Die Voraussetzungen des § 77a Abs. 2 Satz 1 Nr. 2 TKG a.F. lägen nicht vor. Es bestünden keine Anhaltspunkte dafür, dass die Einsichtnahme in die das Landesnetz betreffenden Glasfaserkabel die Vertraulichkeit gemäß § 77m TKG a.F. verletzen würde. Dabei sei zu berücksichtigen, dass die Infrastrukturen im ISA weder dem Landesnetz M. noch der A. GmbH zugeordnet wären. Sie wären von den übrigen, bereits freigegebenen Infrastrukturen der Klägerin nicht zu unterscheiden. Bei einer konkreten Anfrage könne die Klägerin auf die Kennzeichnung als „für eigene Planung reserviert – nicht verfügbar“ verweisen. Daher könne durch eine Einsichtnahme kaum auf das Landesnetz M. zurückgeschlossen werden. Davon unabhängig beziehe sich § 77m TKG a.F. nicht auf Betriebs- und Geschäftsgeheimnisse aus dem Verhältnis zwischen Eigentümer und Betreiber einer Infrastruktur. Die Vorschrift regule allein die Pflichten desjenigen, der im Wege der §§ 77a ff. TKG a.F. Informationen erhalte. Der Kreis der Einsichtnahmeberechtigten sei dabei von vornherein auf bestimmte, am Breitbandausbau konkret interessierte Personen beschränkt. Da es sich bei den meisten Infrastrukturdaten um Betriebs- und Geschäftsgeheimnisse handele, reiche allein das nicht für die Erfüllung des Ausnahmetatbestands. Erforderlich sei ein besonders hohes Schutzbedürfnis der Information oder konkrete Anhaltspunkte, dass eine Durchbrechung des üblichen Schutzniveaus wahrscheinlicher sei als üblich. Beides sei hier nicht der Fall. Eine private Geheimhaltungsvereinbarung reiche nicht aus. 28

Zu § 77a Abs. 4 Satz 1 Nr. 4 TKG a.F. führte die Beklagte ergänzend aus, dass es um den Schutz der öffentlichen Sicherheit in der Ausprägung des Schutzes staatlicher Einrichtungen gehe. Der Wortlaut sei eindeutig auf den Bund beschränkt. Dass der Gesetzgeber weder die Kommunikation zwischen Bund und Ländern noch der Landesbehörden untereinander genannt habe, zeige, dass er nur die Kommunikation auf der Ebene des Bundes als in besonderem Maße schützenswert eingestuft habe. 29

Mit Bescheid vom 10. November 2021 – zugestellt am 12. November 2021 – lehnte die BNetzA auch den Antrag auf Ausnahme für die am 18. März 2020 gelieferten Daten zu den zwei Hauptverteilern ab. Sie führte aus, dass diese Infrastrukturen, selbst wenn sie zum Landesnetz M. gehörten, keinen Ausnahmetatbestand erfüllten. Zur Begründung verwies sie auf die zuvor ergangenen Bescheide. 30

Am 9. Dezember 2021 legte die Klägerin Widerspruch gegen den Bescheid vom 10. November 2021 ein, den die BNetzA mit Widerspruchsbescheid vom 24. Januar 2022 – zugestellt am 26. Januar 2022 – zurückwies. Zur Begründung wurde jeweils auf das vorangegangene Widerspruchsverfahren Bezug genommen. 31

Die Klägerin hat am 1. Dezember 2021 (Az. 1 K 6109/21) und am 17. Februar 2022 (Az. 1 K 1167/22) Klage gegen die Ablehnungs- und Widerspruchsbescheide erhoben. Das Gericht hat die Verfahren mit Beschluss vom 27. Februar 2023 verbunden. 32

Zur Begründung ihrer Klage trägt die Klägerin in Ergänzung ihres bisherigen Vorbringens im Wesentlichen vor: 33

Für die Beurteilung der Ausnahmetatbestände sei auf das seit dem 1. Dezember 2021 geltende TKG abzustellen. § 79 Abs. 3 Satz 1 TKG verdeutliche, dass es sich bei der Ausnahme um eine gebundene Entscheidung handele. Da nach dem Gesetzeswortlaut 34

konkrete Anhaltspunkte reichten, dürften die Anforderungen an die Darlegungslast nicht überspannt werden.

Die Ausnahmetatbestände des § 79 Abs. 3 Satz 1 Nr. 1 und 3 TKG lägen vor. Sie habe hierzu bereits auf die Einhaltung des ISMS nach § 8a Abs. 1 BSIG, den UP KRITIS und die Anforderungen des § 11 EnWG verwiesen. Davon ausgehend seien insbesondere die Details zur Ansteuerung und Überwachung von Mittelspannungsschaltanlagen in den Ortsnetzstationen und Umspannwerken, von Trinkwasserversorgungsanlagen und der Vernetzung der Gebäude von Banken untereinander besonders schutzbedürftig und als kritische Infrastrukturen mit besonderer Schutzbedürftigkeit von einer Einsichtnahme auszunehmen. Sabotageangriffe auf diese Infrastrukturen, etwa die Trinkwasserversorgung, müssten durch einen möglichst hohen Vertraulichkeitsschutz verhindert werden. 35

Die Ausnahmetatbestände des § 79 Abs. 3 Satz 1 Nr. 2 und 4 TKG n.F. lägen ebenfalls vor. Sie habe bereits dargelegt, dass es um Infrastrukturen gehe, die zur Verwirklichung einer sicheren Behördenkommunikation genutzt würden und sie diesbezüglich einer Vertraulichkeitsverpflichtung unterliege. 36

Beim Landesnetz M. handele es sich um ein Netz, das den höchsten Sicherheitsanforderungen entspreche, ausschließlich Behördenzwecken zur Verfügung stehe und nach außen hin abgeschottet sei. Herzstück des Datennetzes sei ein ringförmiger Glasfaserring, der alle M.ländischen Städte verbinde und mit einer Bandbreite von 10 Gigabit/s eine redundante und sichere Datenübertragung ermögliche. Von dem Glasfaserring gingen in jeder Stadt eigene Cityringe aus, an die die Landesbehörden, Polizeidienststellen und Rathäuser angebunden seien. Auftraggeber sei das beim Landesfinanzministerium angesiedelte R. bzw. das O.. Die A. GmbH habe das Netz auf Basis eigener Glasfaserinfrastrukturen sowie in Zusammenarbeit mit lokalen Stadtwerkepartnern gebaut. Im Bereich der Stadt C. bediene sie sich hierfür der passiven Netzinfrastrukturen und Glasfaserkabel der Klägerin. 37

Davon ausgehend handele es sich beim Landesnetz M. schon nicht um ein öffentliches Versorgungsnetz, weshalb es von vornherein nicht vom Anwendungsbereich des § 79 TKG erfasst sei. Jedenfalls sei der Ausnahmetatbestand des § 79 Abs. 3 Satz 1 Nr. 4 TKG n.F. erfüllt. Bei der Auslegung der Vorschrift müsse berücksichtigt werden, dass die Bundesländer nach Art. 83 GG für einen wesentlichen Teil der Ausführungen der Bundesgesetze zuständig seien. Auch die Bund-Länder-Behördenkommunikation sei in den Schutzbereich einzubeziehen. Die Anforderungen an eine sichere Behördenkommunikation würden angesichts vielfältiger Krisen und Bedrohungen anwachsen. So hätten bereits Hackerangriffe auf die J. GmbH, dem Telekommunikationstochterunternehmen der Z. AG, und den Stromkonzern Y. stattgefunden. Auch das Bundesinnenministerium warne, dass die Gefahr von Cyberangriffen seit der russischen Invasion in die Ukraine stark zugenommen habe. Ebenso weise das Bundesamt für Verfassungsschutz darauf hin, dass mögliche Saboteure versuchten, im Internet Informationen über Digital-, Strom- und Gasnetze abzugreifen. Auch die Datenbank der Beklagten könne Ziel von Hackerangriffen werden, weshalb die Transparenzpflichten der Unternehmen kritisch zu betrachten seien. Die S. I. GmbH überdenke bereits ihre Datenlieferungspflichten für den ISA. Im Fall der Klägerin dürften die streitgegenständlichen Infrastrukturdaten wegen der Notwendigkeit einer sicheren Behördenkommunikation nicht in den ISA aufgenommen werden. 38

In der mündlichen Verhandlung vom 25. April 2025 hat die Beklagte die Bescheide vom 29. Juni 2021 in Gestalt des Widerspruchsbescheids vom 2. November 2021 und vom 10. November 2021 in Gestalt des Widerspruchsbescheids vom 24. Januar 2022 insoweit 39

aufgehoben, als Infrastrukturen betroffen sind, die der Ansteuerung und Überwachung von Trinkwasserversorgungsanlagen dienen. Die Beteiligten haben das Verfahren daraufhin insoweit für in der Hauptsache erledigt erklärt.

Die Klägerin beantragt nunmehr noch, 40

die Beklagte unter Aufhebung der Bescheide vom 29. Juni 2021 in Gestalt des Widerspruchsbescheids vom 2. November 2021 und vom 10. November 2021 in Gestalt des Widerspruchsbescheids vom 24. Januar 2022 – soweit diese nicht aufgehoben worden sind –, zu verpflichten, festzustellen, dass die von ihr am 12. Juli 2018, 26. März 2019 und 18. März 2020 gelieferten und als „kritisch“ gekennzeichneten Daten nicht in den Infrastrukturatlas aufgenommen werden. 41

Die Beklagte beantragt, 42

die Klage abzuweisen. 43

Sie wiederholt im Wesentlichen ihre Ausführungen in den angefochten Bescheiden und Widerspruchsbescheiden und trägt ergänzend vor: Es sei unerheblich, auf welchen Beurteilungszeitpunkt abgestellt würde, da sich § 77a Abs. 4 TKG a.F. und § 79 Abs. 3 TKG n.F. rechtlich nicht unterscheiden. 44

§ 77a Abs. 4 Satz 1 Nr. 1 TKG a.F. sei nicht gegeben. Da es sich bei Netzinfrastrukturdaten grundsätzlich um sensible Daten handele, hätte die Klägerin darlegen müssen, dass die Sensibilität der streitgegenständlichen Daten aufgrund eines Sonderstellungsmerkmals über die grundsätzliche Sensibilität von Netzinfrastrukturen hinausgehe. Hierzu habe sie nichts Konkretes vorgetragen. Auch zu einer möglichen Gefahr habe sie nichts dargelegt. 45

§ 77a Abs. 4 Satz 1 Nr. 2 TKG a.F. sei ebenfalls nicht erfüllt. Der Kreis der Einsichtnahmeberechtigten sei nach § 77a Abs. 3 TKG a.F. stark eingeschränkt und unterliege den Vertraulichkeitsverpflichtungen aus § 77m TKG a.F. Der Ausnahmetatbestand setze daher ein besonders hohes Schutzbedürfnis oder konkrete Anhaltspunkte dafür voraus, dass eine Durchbrechung des üblichen Schutzniveaus wahrscheinlicher sei als üblich. Dabei sei zu berücksichtigen, dass die Daten im ISA nur vergrößert dargestellt würden und einsichtnahmeberechtigte Nutzer keinen Zugang zu Rohdaten erhielten. Im Fall der Klägerin würde das Landesnetz M. nicht als solches bezeichnet. Auch die Sensibilität der Daten als solche und der Umstand, dass es sich um Betriebs- und Geschäftsgeheimnisse handele, genüge nicht für den Ausnahmetatbestand. Dies treffen generell auf Netzinfrastrukturdaten zu, weshalb die Anhaltspunkte für eine Verletzung der Vertraulichkeit durch die Einsichtnahme über die grundsätzliche Sensibilität der Daten hinausgehen müsse. Private Geheimhaltungsvereinbarungen genügten hierfür nicht. 46

§ 77a Abs. 4 Satz 1 Nr. 3 TKG a.F. greife schon deshalb nicht, weil die Klägerin nicht dargelegt habe, dass es sich tatsächlich um kritische Infrastrukturen handele. Wann eine Infrastruktur als kritisch einzustufen sei, ergebe sich aus dem jeweiligen Gesetz und den darauf gestützten Rechtsverordnungen, insbesondere aus § 2 Abs. 10 BSIG i.V.m. der BSI-KritisV sowie aus § 12g Abs. 1 EnWG. Die Klägerin habe nicht dargelegt, die Schwellenwerte der BSI-KritisV zu überschreiten. Eine Zertifizierung nach der DIN ISO/IEC 27001 bzw. 27019 stelle keinen solchen Nachweis dar. Im Übrigen seien die in der DIN enthaltenen Sicherheitsvorkehrungen allgemeiner Art und branchenüblich. Mangels Kritikalität der Infrastruktur gehe auch der Verweis auf den UP KRITIS ins Leere. 47

48

Unabhängig hiervon habe die Klägerin die weitere Voraussetzung des Ausnahmetatbestands nicht erfüllt. Nach der Zielsetzung des Gesetzgebers seien auch im Falle kritischer Infrastrukturen lediglich besonders schützenswerte Komponenten aus dem ISA auszunehmen. Es müsse ein besonderer Schutzbedarf vorliegen, der über das übliche Maß vergleichbarer Einrichtungen hinausgehe. Dies habe die Klägerin nicht dargelegt. Allein die Zertifizierung nach der DIN ISO/IEC 27001 bzw. 27019 und das darauf aufbauende Schutzkonzept der Klägerin begründeten keine Anhaltspunkte für das Vorliegen einer besonderen, individuellen Schutzbedürftigkeit. Auch die Schilderungen der Klägerin hinsichtlich der Versorgungsrelevanz bzgl. der Sparten Strom, Erdgas, Trinkwasser und Wärme und ihr pauschaler Verweis auf mögliche Sabotageangriffe genügten nicht.

Die Darstellung der Daten im ISA stehe weder in Konflikt mit dem ISMS noch mit anderen gesetzlichen Schutzpflichten wie denen aus § 11 EnWG. Die gesetzlichen Regelungen stünden gleichberechtigt nebeneinander. Den Sicherheitspflichten werde insbesondere durch die Beschränkung des Kreises der Einsichtnahmeberechtigten, die Einsichtnahmevoraussetzungen und eine sorgfältige Prüfung jeden Antrags Rechnung getragen. Im Falle einer positiven Bescheidung würden nur bestimmte Gebiete des ISA für einen begrenzten Zeitraum freigeschaltet. Darüber hinaus würden die an den ISA gelieferten Daten nach hohen Sicherheitsstandards behandelt und in einer gesicherten Umgebung im Rechenzentrum der Beklagten gespeichert. Dabei würden die Vorgaben des Bundesamts für Sicherheit in der Informationstechnik zur Datensicherheit eingehalten und regelmäßig überprüft, etwa durch Penetrationstests. 49

§ 77a Abs. 4 Satz 1 Nr. 4 TKG a.F. liege ebenfalls nicht vor. Die Datenlieferungspflicht der Klägerin sei hier nicht streitgegenständlich, sodass ihr Vorbringen zur Frage der Öffentlichkeit des Versorgungsnetzes nicht relevant sei. Der Ausnahmetatbestand erfasse lediglich bundesinterne Behördenkommunikation. Eine erweiternde Auslegung komme nicht in Betracht. Ziel der Kostensenkungsrichtlinie sei die Schaffung größtmöglicher Transparenz über für den Breitbandausbau potenziell mitnutzbarer Infrastrukturen. Art. 4 Abs. 1 Satz 3 Kostensenkungsrichtlinie sehe dabei vor, dass die Mitgliedstaaten eine Beschränkung des Zugangs nur ausnahmsweise erlauben dürften, wenn dies für die Sicherheit und Integrität der Netze, die nationale Sicherheit, die öffentliche Gesundheit oder Sicherheit, die Vertraulichkeit oder den Schutz von Betriebs- und Geschäftsgeheimnissen erforderlich sei. Die Ausnahmetatbestände seien daher eng auszulegen. 50

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird Bezug genommen auf den Inhalt der Gerichtsakten in diesem Verfahren und im Verfahren 1 K 1167/22 sowie der beigezogenen Verwaltungsvorgänge der Beklagten. 51

Entscheidungsgründe 52

Soweit die Beteiligten das Verfahren übereinstimmend für in der Hauptsache erledigt erklärt haben, war es entsprechend § 92 Abs. 3 Satz 1 VwGO einzustellen. 53

Im Übrigen ist die Klage zulässig (dazu I.), aber unbegründet (dazu II.). 54

I. Die Klage ist zulässig. 55

Die Klage ist als Verpflichtungsklage (§ 42 Abs. 1 Alt. 2 VwGO) statthaft. Sie ist auf den Erlass eines feststellenden Verwaltungsakts i.S.d. § 35 Satz 1 VwVfG gerichtet. 56

57

Nach der gesetzlichen Definition in § 35 Satz 1 VwVfG ist Verwaltungsakt jede Verfügung, Entscheidung oder andere hoheitliche Maßnahme, die eine Behörde zur Regelung eines Einzelfalles auf dem Gebiet des öffentlichen Rechtes trifft und die auf unmittelbare Rechtswirkung nach außen gerichtet ist.

Regelungscharakter hat eine Maßnahme, wenn sie nach ihrem Erklärungsgehalt darauf gerichtet ist, eine Rechtsfolge zu setzen. Das ist nicht nur dann der Fall, wenn Rechte des Betroffenen begründet, geändert oder aufgehoben werden, sondern – als Besonderheit des feststellenden Verwaltungsakts – auch dann, wenn sie mit bindender Wirkung festgestellt oder verneint werden. 58

Vgl. BVerwG, Urteil vom 5. November 2009 – 4 C 3.09 –, juris Rn. 15. 59

Davon ausgehend richtet sich das Begehren der Klägerin, dass die noch streitgegenständlichen Informationen nicht in den ISA aufgenommen werden, auf den Erlass eines feststellenden Verwaltungsakts. Gemäß § 79 Abs. 3 Satz 1 TKG nimmt die BNetzA bei Vorliegen eines Ausnahmetatbestands die gelieferten Informationen nicht in den ISA auf. Nach der Vorgängervorschrift des § 77a Abs. 4 Satz 1 TKG a.F. war von einer Aufnahme abzusehen. Das „Nicht-Aufnehmen“ der Informationen in den ISA löst für sich genommen keine Rechtsfolgen für den Datenlieferanten aus. Es handelt sich um einen rein tatsächlichen Vorgang (Realakt). Die BNetzA erkennt damit aber das Interesse des Datenlieferanten an der Schutzbedürftigkeit der gelieferten Informationen an. Der Regelungscharakter der Maßnahme liegt darin, das Ergebnis des behördlichen Subsumtionsvorgangs zu den Ausnahmetatbeständen verbindlich festzuschreiben und den Eintritt der gesetzlichen Rechtsfolge des „Nicht-Aufnehmens“ verbindlich festzustellen. 60

Vgl. auch VG Köln, Urteil vom 26. März 2015 – 1 K 2637/14 –, juris Rn. 48, und nachgehend OVG NRW, Beschluss vom 7. Januar 2016 – 13 A 999/15 –, juris Rn. 5, die ebenfalls davon ausgehen, dass die Entscheidung auf der zweiten Verfahrensstufe durch Feststellungsbescheid ergeht. 61

Die Zulässigkeit der Klage begegnet im Übrigen keinen Bedenken. 62

II. Die Klage ist unbegründet. 63

Die Beklagte hat die Ausnahme der – nach der Teilaufhebung noch streitgegenständlichen – Informationen aus dem ISA zu Recht abgelehnt. Die Bescheide vom 29. Juni 2021 in Gestalt des Widerspruchsbescheids vom 2. November 2021 und vom 10. November 2021 in Gestalt des Widerspruchsbescheids vom 24. Januar 2022 sind insoweit rechtmäßig und verletzen die Klägerin nicht in ihren Rechten (§ 113 Abs. 5 Satz 1 VwGO). 64

1. Maßgeblicher Zeitpunkt für die Beurteilung der Sach- und Rechtslage ist der Zeitpunkt der mündlichen Verhandlung. Davon ausgehend beurteilt sich der von der Klägerin verfolgte Ausnahmeanspruch nach § 79 Abs. 3 TKG in der Fassung vom 23. Juni 2021. 65

Die Frage des maßgeblichen Zeitpunkts der gerichtlichen Prüfung einer Verwaltungsentscheidung ist nicht dem Prozessrecht, sondern dem materiellen Recht zu entnehmen, da das materielle (Bundes- oder Landes-)Recht nicht nur die tatbestandlichen Voraussetzungen für die Rechtmäßigkeit eines Verwaltungsakts bestimmt, sondern auch die Antwort auf die Frage gibt, zu welchem Zeitpunkt diese Voraussetzungen erfüllt sein müssen. 66

StRSpr., vgl. nur BVerwG, Beschluss vom 25. Oktober 2018 – 6 B 125.18 –, juris Rn. 4. 67

Bei einer Verpflichtungsklage richtet sich die Beurteilung der Sach- und Rechtslage grundsätzlich nach dem Zeitpunkt der letzten mündlichen Verhandlung oder Entscheidung, wenn und soweit sich aus dem materiellen Recht kein abweichender Beurteilungszeitpunkt ergibt.	68
StRSpr., vgl. nur BVerwG, Urteile vom 20. April 2023 – 1 C 4.22 –, juris Rn. 9, und vom 5. November 2020 – 3 C 12.19 –, juris Rn. 11.	69
Für den von der Klägerin geltend gemachten Ausnahmeanspruch ergibt sich aus dem materiellen Recht kein abweichender Beurteilungszeitpunkt. Zwar knüpfen sowohl § 79 Abs. 3 Satz 1 TKG als auch § 77a Abs. 4 Satz 1 TKG a.F. dem Wortlaut nach an die auf der ersten Stufe des Verwaltungsverfahrens gelieferten Informationen an. Sinn und Zweck der Vorschrift sprechen aber dagegen, für die Beurteilung der Schutzbedürftigkeit der Daten auf den Zeitpunkt der Datenlieferung abzustellen. Vielmehr sind nachträgliche Sach- und Rechtsänderungen sowohl für einen wirksamen Schutz der Daten relevant, als auch für das gegenläufige Interesse, nicht schutzbedürftige Informationen im Interesse einer wirtschaftlicheren Nutzung vorhandener Infrastrukturen und eines zügigen Breitbandausbaus im ISA zusammenzuführen.	70
Vgl. zum Zweck der Datenlieferungspflicht OVG NRW, Beschluss vom 7. Januar 2016 – 13 A 999/15 –, juris Rn. 6 f. m.w.N.	71
Auch das zum 1. Dezember 2021 in Kraft getretene Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts vom 23. Juni 2021 (Telekommunikationsmodernisierungsgesetz, fortan: TKModG) erfordert keinen anderen Beurteilungszeitpunkt. Mit der Neufassung der Rechtsvorschriften zum ISA war keine materielle Rechtsänderung verbunden.	72
Vgl. BT-Drs. 19/26108, S. 305 zu § 78 Abs. 3 TKG-E. So auch bereits zur ersten Stufe des Verwaltungsverfahrens OVG NRW, Beschluss vom 6. Oktober 2022 – 13 B 513/21 –, juris Rn. 24.	73
Auch die behördliche Zuständigkeit hat sich nicht geändert. Die Beklagte hat die Aufgaben der zentralen Informationsstelle des Bundes gemäß § 78 Abs. 2 Satz 2 TKG vom Bundesministerium für Verkehr und digitale Infrastruktur übertragen bekommen. Dies ergibt sich aus dem – dem Gericht im Verfahren 1 K 1406/21 vorgelegten – Organisationserlass des Bundesministeriums für Wirtschaft und Klimaschutz vom 21. Oktober 2022 (Az. N01).	74
2. Die Klägerin hat keinen Anspruch auf Ausnahme der noch streitgegenständlichen Daten aus dem ISA. Die Voraussetzungen des § 79 Abs. 3 TKG liegen nicht vor.	75
Gemäß § 79 Abs. 3 Satz 1 TKG nimmt die zentrale Informationsstelle des Bundes nach Abs. 2 erhaltene Informationen nicht in die Übersicht nach Abs. 1 Nr. 1 auf, soweit konkrete Anhaltspunkte dafür vorliegen, dass (1.) eine Einsichtnahme nach Abs. 4 die Sicherheit und Integrität der Einrichtung oder der sonstigen physischen Infrastruktur oder die öffentliche Sicherheit oder die öffentliche Gesundheit gefährdet, (2.) eine Einsichtnahme nach Absatz 4 die Vertraulichkeit gemäß § 148 TKG verletzt, (3.) Teile einer Infrastruktur betroffen sind, die durch Gesetz oder aufgrund eines Gesetzes als Kritische Infrastrukturen bestimmt worden und nachweislich besonders schutzbedürftig und für die Funktionsfähigkeit der Kritischen Infrastruktur maßgeblich sind, oder (4.) Teile öffentlicher Versorgungsnetze oder sonstiger	76

physischer Infrastrukturen betroffen sind, die durch den Bund zur Verwirklichung einer sicheren Behördenkommunikation genutzt werden. Gemäß § 79 Abs. 3 Satz 2 TKG sind in diesen Fällen für die jeweiligen Gebiete, in denen sich die Einrichtungen oder sonstigen physischen Infrastrukturen befinden, Informationen i.S.v. § 136 Abs. 3 Nr. 3 und § 153 Abs. 3 Nr. 3 TKG aufzunehmen (d.h. die Kontaktdaten eines oder mehrerer Ansprechpartner beim Eigentümer oder Betreiber des öffentlichen Versorgungsnetzes oder der sonstigen physischen Infrastruktur).

Für das Vorliegen der Ausnahmetatbestände genügen konkrete Anhaltspunkte. Es müssen bestimmte, auf den Einzelfall bezogene und überprüfbare Anknüpfungstatsachen gegeben sein. Einer Überzeugung bedarf es nicht. Die bloße Möglichkeit oder reine Vermutung, ein nicht durch Tatsachen belegbarer Verdacht oder allgemeine statistische Wahrscheinlichkeiten reichen indes nicht. 77

Vgl. auch *Leitzke*, in: Säcker/Körber, Kommentar TKG – TTDSG, 4. Aufl. 2023, § 79 Rn. 21; *Scherer/Butler*, in: Fetzer/Scherer/Graulich, TKG, 3. Aufl. 2021, § 77a Rn. 38; *Stelter*, in: Scheurle/Mayen, Telekommunikationsgesetz, 3. Aufl. 2018, § 77a Rn. 35. 78

Davon ausgehend liegen die Ausnahmetatbestände des § 79 Abs. 3 Satz 1 TKG hier nicht vor. Es bestehen keine konkreten Anhaltspunkte dafür, dass eine Einsichtnahme die in Nr. 1 genannten Schutzgüter gefährdet (dazu a.) oder die Vertraulichkeit gemäß § 148 TKG verletzt (dazu b.). Es sind auch keine Teile einer Infrastruktur betroffen, die als Kritische Infrastrukturen bestimmt worden sind (dazu c.) oder durch den Bund zur Verwirklichung einer sicheren Behördenkommunikation genutzt werden (dazu d.). 79

a. Der Ausnahmetatbestand des § 79 Abs. 3 Satz 1 Nr. 1 TKG ist nicht erfüllt. 80

Bei den in § 79 Abs. 3 Satz 1 Nr. 1 TKG genannten Schutzgütern handelt es sich um unbestimmte Rechtsbegriffe. Diese bedürfen der Auslegung und unterliegen der vollständigen gerichtlichen Kontrolle. 81

Anders *Roth/Löhr*, in: Geppert/Schütz, Beck'scher TKG-Kommentar, 5. Aufl. 2023, § 79 Rn. 51, die von einem Beurteilungsspielraum bei der Prüfung der Ausnahmetatbestände ausgehen. 82

Für die Auslegung ist auf das jeweilige unionsrechtliche Begriffsverständnis abzustellen. Hierfür spricht, dass der Gesetzgeber den Ausnahmekatalog an Art. 4 Abs. 1 Satz 3 Kostensenkungsrichtlinie angepasst hat. 83

Vgl. BT-Drs. 18/8332, S. 41 zu § 77a Abs. 4 TKG-E. So auch *Leitzke*, in: Säcker/Körber, Kommentar TKG – TTDSG, 4. Aufl. 2023, § 79 Rn. 24; *Scherer/Butler*, in: Fetzer/Scherer/Graulich, TKG, 3. Aufl. 2021, § 77a Rn. 41. 84

Nach Art. 4 Abs. 1 Satz 3 Kostensenkungsrichtlinie dürfen die Mitgliedstaaten eine Beschränkung des Zugangs zu den Mindestinformationen nur dann erlauben, wenn dies für die Sicherheit und Integrität der Netze, die nationale Sicherheit, die öffentliche Gesundheit oder Sicherheit, die Vertraulichkeit oder den Schutz von Betriebs- und Geschäftsgeheimnissen erforderlich ist. 85

Das Schutzgut der Sicherheit und Integrität der Einrichtung oder der sonstigen physischen Infrastruktur knüpft sowohl an den physischen Bestand als auch an die Funktionsfähigkeit der Infrastruktur an. 86

Das Schutzgut der öffentlichen Sicherheit umfasst nach dem unionsrechtlichen Begriffsverständnis sowohl die innere als auch die äußere Sicherheit eines Mitgliedstaats. Die öffentliche Sicherheit kann daher sowohl durch die Beeinträchtigung des Funktionierens der Einrichtungen des Staates und seiner wichtigen öffentlichen Dienste sowie die Gefährdung des Überlebens der Bevölkerung als auch durch die Gefahr einer erheblichen Störung der auswärtigen Beziehungen oder des friedlichen Zusammenlebens der Völker oder eine Beeinträchtigung der militärischen Interessen berührt werden.	87
Vgl. EuGH, Urteil vom 4. April 2017 – C-544/15 –, juris Rn. 39.	88
Das Schutzgut der öffentlichen Gesundheit umfasst u.a. den Schutz der Bevölkerung vor Krankheiten mit epidemischem Potenzial und sonstigen übertragbaren Krankheiten. Dabei ist zu berücksichtigen, dass die Gesundheit und das Leben von Menschen einen sehr hohen Rang einnehmen und es Sache der Mitgliedstaaten ist, zu bestimmen, auf welchem Niveau sie den Schutz der Gesundheit der Bevölkerung gewährleisten wollen und wie dieses Niveau erreicht werden soll.	89
Vgl. EuGH, Urteile vom 5. Dezember 2023, C-128/22 –, juris Rn. 52, 78, und vom 8. Juni 2017 – C-296/15 –, juris Rn. 82.	90
Im Rahmen des Ausnahmetatbestands des § 79 Abs. 3 Satz 1 Nr. 1 TKG verbleibt dem Schutzgut der öffentlichen Gesundheit voraussichtlich nur ein geringer Anwendungsbereich, da der Gesetzgeber Trinkwasserversorgungsnetze schon aus der Begriffsbestimmung öffentlicher Versorgungsnetze in § 3 Nr. 43 Buchst. a Unterbuchst. ee TKG und damit aus der Datenlieferungspflicht des § 79 Abs. 2 TKG herausgenommen hat.	91
Vgl. <i>Leitzke</i> , in: Säcker/Körber, Kommentar TKG – TTDSG, 4. Aufl. 2023, § 79 Rn. 24; <i>Roth/Löhr</i> , in: Geppert/Schütz, Beck'scher TKG-Kommentar, 5. Aufl. 2023, § 79 Rn. 68; <i>Scherer/Butler</i> , in: Fetzer/Scherer/Graulich, TKG, 3. Aufl. 2021, § 77a Rn. 44.	92
Die Gefährdung der vorgenannten Schutzgüter muss nach dem eindeutigen Wortlaut von § 79 Abs. 3 Satz 1 Nr. 1 TKG aus der Einsichtnahme nach Abs. 4 folgen.	93
Nach § 79 Abs. 4 Satz 1 TKG gewährt die zentrale Informationsstelle des Bundes den am Ausbau von öffentlichen Versorgungsnetzen Beteiligten nach Maßgabe der Einsichtnahmebedingungen nach Abs. 5 Einsicht in die Übersicht nach Abs. 1, soweit mit dem Ausbauvorhaben Einrichtungen geschaffen werden sollen, die zu Telekommunikationszwecken genutzt werden können. Nach Satz 2 gehören zu den am Ausbau von öffentlichen Versorgungsnetzen Beteiligten insbesondere Gebietskörperschaften, Eigentümer und Betreiber öffentlicher Versorgungsnetze sowie deren Auftragnehmer.	94
Nach § 79 Abs. 5 Satz 1 und 2 TKG regelt die zentrale Informationsstelle des Bundes die Einzelheiten der Einsichtnahme in Einsichtnahmebedingungen, die insbesondere der Sensitivität der erfassten Daten und dem zu erwartenden Verwaltungsaufwand Rechnung zu tragen haben. Zudem haben die Einsichtnahmeberechtigten nach § 79 Abs. 5 Satz 2 TKG die Vertraulichkeit nach § 148 TKG zu wahren. Demnach dürfen Informationen, die im Rahmen der Einsichtnahme, gewonnen werden, nur für die Zwecke verwendet werden, für die sie bereitgestellt werden. Die Informationen dürfen nicht an Dritte weitergegeben werden; Betriebs- und Geschäftsgeheimnisse sind zu wahren.	95
Durch die ausdrückliche Bezugnahme auf die Einsichtnahme nach § 79 Abs. 4 TKG erfasst der Ausnahmetatbestand des § 79 Abs. 3 Satz 1 Nr. 1 TKG ausschließlich Gefährdungen aus	96

einer rechtmäßigen Einsichtnahme in den ISA. Nicht erfasst sind Gefahren, die aus einer etwaigen rechtsmissbräuchlichen Verwendung der aus der Einsichtnahme gewonnenen Informationen oder einer unberechtigten Einsichtnahme in den ISA folgen.

Die Kammer verkennt nicht, dass der Vorschrift bei dieser Auslegung voraussichtlich nur ein geringer praktischer Anwendungsbereich verbleibt. Dies stimmt allerdings mit dem Ziel des Gesetzgebers überein, die Ausnahmetatbestände möglichst eng zu fassen. Besonders deutlich wurde dies im Gesetzgebungsverfahren zum DigiNetzG. Hier sah der ursprüngliche Gesetzesentwurf der Bundesregierung zunächst vor, in Nr. 3 sämtliche Kritische Infrastrukturen von einer Veröffentlichung im ISA auszunehmen, 97

vgl. § 77a Abs. 4 Satz 1 Nr. 3 TKG-E in BT-Drs. 71/16, S. 9. 98

Erst der Ausschuss für Verkehr und digitale Infrastruktur setzte durch, dass die Ausnahme auf solche Teile Kritischer Infrastrukturen beschränkt wurde, die besonders schutzbedürftig und für die Funktionsfähigkeit der Infrastruktur maßgeblich sind. Begründet wurde dies damit, dass den nach der Kostensenkungsrichtlinie umzusetzenden Maßnahmen ein substantieller Anwendungsbereich erhalten bleiben sollte. Es seien keine Infrastrukturen in Gänze aus dem ISA auszunehmen, sondern lediglich besonders schützenswerte Netzkomponenten. Nur so könnten der ISA als wesentliches Informations- und Transparenzmittel erhalten bleiben und die beabsichtigten Kostensenkungsziele tatsächlich erreicht werden. 99

Vgl. BT-Drs. 18/9023, S. 4 und 14 f. Vgl. auch *Roth/Löhr*, in: Geppert/Schütz, Beck'scher TKG-Kommentar, 5. Aufl. 2023, § 79 Rn. 78; *Scherer/Butler*, in: Fetzer/Scherer/Graulich, TKG, 3. Aufl. 2021, § 77a Rn. 48. 100

Zugleich hat der Gesetzgeber die Gefahren, die mit einer Veröffentlichung sensibler Infrastrukturinformationen im ISA einhergehen, durch die rechtlichen Anforderungen an eine Einsichtnahme – beschränkter Kreis von Einsichtnahmeberechtigten, Anknüpfung an konkrete Ausbauvorhaben, Einsichtnahmebedingungen, die der Sensitivität der Daten Rechnung tragen, Wahrung der Vertraulichkeit nach § 148 TKG – auf ein zumutbares Maß reduziert. Die verbleibenden Missbrauchsgefahren sind nach der gesetzgeberischen Wertung zugunsten des mit dem ISA verfolgten Zwecks hinzunehmen. 101

Dies zugrunde gelegt sind vorliegend keine konkreten Anhaltspunkte dafür gegeben, dass eine Einsichtnahme in den ISA die Sicherheit und Integrität der streitgegenständlichen Infrastrukturen oder die öffentliche Sicherheit gefährdet. 102

Der Einwand der Klägerin, sie sei nach § 11 Abs. 1 EnWG zum Betrieb eines sicheren Energieversorgungsnetzes verpflichtet, was nach § 11 Abs. 1a EnWG insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme umfasse, greift nicht durch. Die Betreiberpflichten der Klägerin aus § 11 EnWG stehen gleichrangig neben ihrer Datenlieferungspflicht aus § 79 Abs. 2 TKG. Bei der Lösung dieser Normenkollision ist zu berücksichtigen, dass der Gesetzgeber die besondere Sensibilität von Netzinfrastrukturdaten bei der konkreten Ausgestaltung des § 79 TKG, insbesondere den rechtlichen Anforderungen an eine Einsichtnahme in den ISA, berücksichtigt hat. Das Bestehen gesetzlicher Schutz- oder Vertraulichkeitspflichten genügt daher für sich genommen nicht, um eine Ausnahme der Informationen aus dem ISA zu rechtfertigen. Das gleiche gilt für Zertifizierungen, die der Klägerin – wie hier nach DIN ISO/IEC 27001:2017 und 27019 – ausgestellt wurden. Auch private Geheimhaltungsvereinbarungen – wie hier zwischen der Klägerin und der A. GmbH – können keine Ausnahme begründen. 103

Das Vorbringen der Klägerin, die Informationen zum Landesnetz M. seien mit Blick auf die öffentliche Sicherheit besonders schutzbedürftig, begründet ebenfalls keine Ausnahme. Die Beklagte hat zu Recht darauf hingewiesen, dass im ISA lediglich Informationen zum Telekommunikationsnetz der Klägerin dargestellt werden, ohne dass sich hieraus Rückschlüsse auf die konkrete Nutzung ergeben. Soweit die Klägerin abstrakt Missbrauchsrisiken im Umgang mit den aus einer Einsichtnahme gewonnenen Informationen befürchtet, unterfallen diese – wie dargestellt – nicht dem Anwendungsbereich des Ausnahmetatbestands. Im Übrigen merkt die Kammer an, dass bereits aus den offenkundigen Standorten der an das Landesnetz M. angeschlossenen Behörden Rückschlüsse auf die geografische Lage der Telekommunikationsinfrastruktur möglich sind. Dass sich die damit einhergehende Gefährdung durch eine Einsichtnahme in den ISA erhöhen würde, ist nicht erkennbar. Soweit die Klägerin einwendet, dass die Informationen im ISA infolge der Aktualisierungspflichten auf dem jeweils neuesten Stand seien, geht ihr Vorbringen nicht über die Geltendmachung abstrakter Missbrauchsrisiken hinaus.

104

Davon unabhängig verfährt der Einwand nicht, dass es sich um ein geschlossenes Behördennetz handele, zu dem nach § 79 Abs. 2 TKG gar keine Informationen hätten geliefert werden müssen. Die Datenlieferungspflicht des § 79 Abs. 2 Satz 1 TKG knüpft an die Stellung der Klägerin als Eigentümerin eines öffentlichen Versorgungsnetzes für die Bereitstellung von Telekommunikationsdiensten (§ 3 Nr. 43 Buchst. a Unterbuchst. aa TKG) an. Betrachtet wird jeweils das Versorgungsnetz als Ganzes,

105

so ausdrücklich BT-Drs. 18/8332, S. 35 zum Begriff „öffentliche Versorgungsnetze“.

106

Aus den gleichen Gründen begründet auch das Vorbringen der Klägerin zu den Infrastrukturen, die der Vernetzung von Banken untereinander dienen, keine Ausnahme. Konkrete Anhaltspunkte dafür, dass eine Einsichtnahme die Sicherheit und Integrität dieser Einrichtung oder die öffentliche Sicherheit gefährden könnte, bestehen nicht.

107

Die weiteren Einwände der Klägerin greifen ebenfalls nicht durch. Ihr Vorbringen beschränkt sich im Wesentlichen auf die Geltendmachung allgemeiner Sicherheitsrisiken für öffentliche Infrastrukturen sowie der Gefahr von Cyberangriffen sowohl gegen die Klägerin als auch gegen die BNetzA. Ihr Vortrag richtet sich damit letztlich gegen die Veröffentlichung von Infrastrukturinformationen an sich. Zum gegenwärtigen Zeitpunkt bestehen indes keine Anhaltspunkte für die Annahme, dass der Gesetzgeber nicht mehr an § 79 TKG festhalten wolle.

108

b. Der Ausnahmetatbestand des § 79 Abs. 3 Satz 1 Nr. 2 TKG ist nicht erfüllt.

109

Schutzgut der Vorschrift ist die Vertraulichkeit nach § 148 TKG. Laut Gesetzesbegründung liegen Anhaltspunkte für eine Verletzung der Vertraulichkeit nicht schon in der Sensibilität der Netzinfrastrukturdaten an sich. Diesem Umstand werde bereits durch die Verpflichtung der Einsichtnahmeberechtigten zur Wahrung der Vertraulichkeit Rechnung getragen. Anhaltspunkte für die Verletzung der Vertraulichkeit müssten daher über die grundsätzliche Sensibilität der Daten als Netzinfrastrukturdaten hinausgehen.

110

Vgl. BT-Drs. 18/8332, S. 41 zu § 77a Abs. 4 Satz 1 Nr. 2 TKG-E.

111

Der Wortlaut des Ausnahmetatbestands knüpft zudem – wie in § 79 Abs. 3 Satz 1 Nr. 1 TKG – eindeutig an die Einsichtnahme nach § 79 Abs. 4 TKG an, d.h. an eine rechtmäßige Einsichtnahme. Nicht erfasst sind demnach Vertraulichkeitsverletzungen, die aus einem rechtswidrigen Umgang mit den gewonnenen Informationen oder aus einer unberechtigten

112

Einsichtnahme in den ISA herrühren.

Dies zugrunde gelegt bestehen vorliegend keine konkreten Anhaltspunkte dafür, dass eine Einsichtnahme in den ISA die Vertraulichkeit verletzt. 113

Dass es sich bei den streitgegenständlichen Informationen um Betriebs- und Geschäftsgeheimnisse der Klägerin handelt, genügt hierfür nicht. Dem in Art. 4 Abs. 1 Satz 3 Kostensenkungsrichtlinie genannten Schutz von Betriebs- und Geschäftsgeheimnissen hat der Gesetzgeber durch die Pflichten zur Wahrung der Vertraulichkeit nach § 79 Abs. 5 Satz 3 i.V.m. § 148 Abs. 1 Satz 3 TKG Rechnung getragen. Soweit hiergegen in der Kommentarliteratur eingewandt wird, dass ein Betriebs- und Geschäftsgeheimnis seine Eigenschaft als solches bereits dann verliere, wenn es einem einsichtnehmenden Wettbewerber bekannt werde, 114

so zu § 77a Abs. 4 Satz 1 Nr. 2 TKG a.F. *Stelter*, in: Scheurle/Mayen, Telekommunikationsgesetz, 3. Aufl. 2018, § 77a Rn. 38, 115

schließt sich die Kammer dieser Auffassung nicht an. Als Betriebs- und Geschäftsgeheimnisse werden alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge verstanden, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat. 116

Vgl. BVerfG, Beschluss vom 14. März 2006 – 1 BvR 2087/03 –, juris Rn. 87. 117

Die so geschützte Information wird durch die Aufnahme in den ISA indes nicht öffentlich bekannt, sondern bleibt weiterhin nur einem durch § 79 Abs. 4 TKG begrenzten Personenkreis zugänglich. Dieser ist überdies gemäß § 79 Abs. 5 Satz 3 i.V.m. § 148 TKG zur Wahrung des bekannt gewordenen Betriebs- und Geschäftsgeheimnisses verpflichtet. Welche „Schwäche“ der Regelung des § 148 TKG innewohnen soll, 118

so *Stelter* zu § 77m TKG a.F., in: Scheurle/Mayen, Telekommunikationsgesetz, 3. Aufl. 2018, § 77a Rn. 38, 119

ist für die Kammer nicht erkennbar. Das Vorbringen der Klägerin hierzu beschränkt sich erneut auf die Geltendmachung abstrakter Missbrauchsrisiken. 120

Auch die von der Klägerin in Bezug genommene vertragliche Geheimhaltungsvereinbarung mit der A. GmbH begründet keine Ausnahme. Vertragliche Vereinbarungen lassen gesetzliche Pflichten – wie hier die Veröffentlichungspflichten aus § 79 TKG – unberührt. 121

So auch *Roth/Löhr*, in Geppert/Schütz, Beck'scher TKG-Kommentar, 5. Aufl. 2023, § 79 Rn. 73, die darauf verweisen, dass der zivilrechtliche Vertrag ggf. angepasst werden müsse. 122

c. Der Ausnahmetatbestand des § 79 Abs. 3 Satz 1 Nr. 3 TKG ist nicht erfüllt. 123

Der Ausnahmetatbestand kommt nur für Infrastrukturen in Betracht, die durch Gesetz oder aufgrund Gesetzes als Kritische Infrastrukturen bestimmt worden sind. Die Definition der Kritischen Infrastrukturen knüpft an die jeweilige Gesetzeslage an, beispielsweise an § 2 Abs. 10 BSIG oder § 12g Abs. 1 EnWG. 124

Vgl. BT-Drs. 18/8332, S. 41 zu § 77a Abs. 4 Satz 1 Nr. 3 TKG-E. 125

126

Diese Voraussetzung ist hier nicht erfüllt. Die Klägerin hat in der mündlichen Verhandlung klargestellt, dass es sich bei ihren öffentlichen Versorgungsnetzen nicht um Kritische Infrastrukturen in diesem Sinne handelt. Die für eine entsprechende Einstufung nach § 2 Abs. 10 BSIg relevanten Schwellenwerte der BSI-KritisV würden nicht überschritten.	
d.Der Ausnahmetatbestand des § 79 Abs. 3 Satz 1 Nr. 4 TKG ist nicht erfüllt.	127
Der Anwendungsbereich der Vorschrift ist seinem Wortlaut nach auf eine Nutzung der streitgegenständlichen Infrastrukturen „durch den Bund“ zur Verwirklichung einer sicheren Behördenkommunikation beschränkt. Hiermit nicht vereinbar ist die Auffassung der Klägerin, es reiche aus, dass über das Landesnetz M. auch mit Bundesbehörden kommuniziert werde.	128
Eine analoge Anwendung der Vorschrift auf Landes- und kommunale Behörden – wie hier das Landesnetz M. – kommt nicht in Betracht. Die Kammer lässt dabei offen, ob eine sichere Behördenkommunikation auf Landes- und kommunaler Ebene mit der Interessenlage des § 79 Abs. 3 Satz 1 Nr. 4 TKG vergleichbar ist. Jedenfalls fehlt es an einer planwidrigen Regelungslücke.	129
Durch eine Analogie wird die durch eine Norm angeordnete Rechtsfolge auf einen Sachverhalt übertragen, der nicht dem Tatbestand der Norm unterfällt. Eine Analogie darf nur vorgenommen werden, um eine echte Regelungslücke auszufüllen. Darunter ist eine Unvollständigkeit des Tatbestandes einer Norm wegen eines versehentlichen, dem Normzweck zuwiderlaufenden Regelungsversäumnisses des Normgebers zu verstehen. Eine solche Lücke darf von den Gerichten im Wege der Analogie geschlossen werden, wenn sich aufgrund der gesamten Umstände feststellen lässt, dass der Normgeber die von ihm angeordnete Rechtsfolge auch auf den nicht erfassten Sachverhalt erstreckt hätte, wenn er ihn bedacht hätte.	130
Vgl. BVerwG, Beschluss vom 11. September 2008 – 2 B 43/08 –, juris Rn. 7 m.w.N.	131
Für die Frage, welche Regelungskonzeption dem Gesetz zugrunde liegt, kommt neben dem Wortlaut der Vorschrift auch der Systematik und den Gesetzesmaterialien eine nicht unerhebliche Bedeutung zu. In Betracht zu ziehen sind die Begründung eines Gesetzentwurfs, der unverändert verabschiedet worden ist, die darauf bezogenen Stellungnahmen von Bundesrat (Art. 76 Abs. 2 Satz 2 GG) und Bundesregierung (Art. 76 Abs. 3 Satz 2 GG) und die Stellungnahmen, Beschlussempfehlungen und Berichte der Ausschüsse. In diesen Materialien finden sich regelmäßig die im Verfahren als wesentlich erachteten Vorstellungen der am Gesetzgebungsverfahren beteiligten Organe und Personen. Eine Interpretation, die als richterliche Rechtsfortbildung den Wortlaut des Gesetzes hintanstellt und sich über den klar erkennbaren Willen des Gesetzgebers hinwegsetzt, greift unzulässig in die Kompetenzen des demokratisch legitimierten Gesetzgebers ein. Insoweit darf richterliche Rechtsfortbildung nicht dazu führen, dass die Gerichte ihre eigene materielle Gerechtigkeitsvorstellung an die Stelle derjenigen des Gesetzgebers setzen.	132
Vgl. BVerfG, Beschluss vom 28. November 2023 – 2 BvL 8/13 –, juris Rn. 130 f. m.w.N.	133
Nach diesen Maßstäben kommt eine analoge Anwendung von § 79 Abs. 3 Satz 1 Nr. 4 TKG hier nicht in Betracht.	134
Bereits im ersten Gesetzesentwurf der Bundesregierung zum DigiNetzG war der Ausnahmetatbestand des § 77a Abs. 4 Satz 1 Nr. 4 TKG-E dahingehend formuliert, Teile öffentlicher Versorgungsnetze auszunehmen, die durch den Bund zur Verwirklichung einer	135

sicheren Behördenkommunikation genutzt werden. Welche Erwägungen dieser Formulierung, insbesondere der Beschränkung auf den „Bund“, zugrunde lagen, ist nicht erkennbar. In der Begründung finden sich hierzu, abgesehen von einer Wiederholung des Regelungstextes, keine Ausführungen.	
Vgl. BT-Drs. 18/8332, S. 12 und 40 f.	136
Die auf den „Bund“ beschränkte Formulierung des Ausnahmetatbestands wurde im weiteren Gesetzgebungsverfahren nicht in Frage gestellt. Der Bundesrat gab lediglich zu bedenken, dass die Beschränkung der Ausnahmetatbestände Nr. 3 und 4 auf „Teile“ einer Infrastruktur oder eines Versorgungsnetzes nicht hinreichend bestimmt sein könnte.	137
Vgl. BR-Drs. (Beschluss), 71/16, S. 8.	138
Daran anschließend nahm der Ausschuss für Verkehr und digitale Infrastruktur tatbestandliche Einschränkungen an der Ausnahme Kritischer Infrastrukturen in Nr. 3 vor. Zur Begründung führte er aus, dass dem ISA als wesentliches Informations- und Transparenzmittel zur Erreichung der beabsichtigten Kostensenkungsziele ein substantieller Anwendungsbereich erhalten bleiben sollte.	139
Vgl. BT-Drs. 18/9023, S. 4 und 14 f.	140
Der Bundesrat sah seiner Prüfbitte bezüglich des Anwendungsbereichs der Ausnahmeregelungen damit Rechnung getragen.	141
Vgl. BR, 948. Sitzung, Erläuterung zum Tagesordnungspunkt 15, S. 15(a).	142
Im Gesetzgebungsverfahren zum TKModG wurde die auf den „Bund“ beschränkte Formulierung des Ausnahmetatbestands ebenfalls nicht in Frage gestellt. Die Vorschrift wurde inhaltlich unverändert in § 78 Abs. 3 Satz 1 Nr. 4 TKG-E übernommen, ergänzt lediglich um die sonstigen physischen Infrastrukturen.	143
Vgl. BT-Drs. 19/26108, S. 77 und 305.	144
Auch der Bundesrat und der Ausschuss für Wirtschaft und Energie sahen an dieser Stelle keinen Änderungsbedarf.	145
Vgl. BR-Drs. 29/21 (Beschluss), und BT-Drs. 19/28865, S. 133.	146
Angesichts dieser Vorgeschichte kann die Kammer keine planwidrige Regelungslücke feststellen. Aus den Gesetzesmaterialien lässt sich nicht der Schluss ziehen, der Gesetzgeber habe den Ausnahmetatbestand des § 79 Abs. 3 Satz 1 Nr. 4 TKG lediglich versehentlich auf den „Bund“ beschränkt. Der Begriff ist rechtlich eindeutig und wurde trotz der wiederholten Befassung der Gesetzgebungsorgane mit dem Ausnahmetatbestand nicht in Frage gestellt. Dass der Gesetzgeber die Ausnahme auch auf die Länder und Kommunen – oder allgemein „den Staat“ – erstreckt hätte, lässt sich nicht erkennen. Dagegen spricht zudem, dass die Gesetzgebungsorgane die Ausnahmetatbestände mit Blick auf die mit dem ISA verfolgten Kostensenkungsziele eher eng als weit fassen wollten.	147
Vgl. auch <i>Roth/Löhr</i> , in Geppert/Schütz, Beck'scher TKG-Kommentar, 5. Aufl. 2023, § 79 Rn. 86 ff., die eine Regelungslücke mit Verweis auf die Gesetzgebungsgeschichte ebenfalls ablehnen. Ohne Auseinandersetzung mit der Frage des Anwendungsbereichs der Vorschrift <i>Leitzke</i> , in Säcker/Körber, TKG TTDSG, 4. Aufl. 2023, § 79 Rn. 28, und <i>Scherer/Butler</i> , in:	148

Fetzer/Scherer/Graulich, TKG, 3. Aufl. 2021, § 77a Rn. 49, die der BNetzA jeweils zustimmen, dass der Bund die Nutzung der Infrastruktureile zur sicheren Behördenkommunikation bestätigen müsse. Wohl auch für ein auf den Bund beschränktes Verständnis *Stelzer*, in: Scheurle/Mayen, Telekommunikationsgesetz, 3. Aufl. 2018, § 77a Rn. 40, der als Anwendungsbeispiel den Deutschen Bundestag anführt.

Die Kostenentscheidung beruht, soweit über die Klage streitig entschieden wurde, auf § 154 Abs. 1 VwGO. Im Übrigen – d.h. soweit die Beteiligten das Verfahren hinsichtlich der Infrastrukturen, die der Ansteuerung und Überwachung von Trinkwasserversorgungsanlagen dienen, übereinstimmend in der Hauptsache für erledigt erklärt haben – entspricht es billigem Ermessen i.S.d. § 161 Abs. 2 Satz 1 VwGO, der Beklagten die Kosten des Verfahrens aufzuerlegen. Diese hat die Klägerin durch die teilweise Aufhebung der angefochtenen Bescheide und Widerspruchsbescheide klaglos gestellt. 149

Die Berufung war nicht zuzulassen, da die Sache keine grundsätzliche Bedeutung i.S.d. § 124a Abs. 1 Satz 1, § § 124 Abs. 2 Nr. 3 TKG hat. Die Frage der Auslegung der einzelnen Ausnahmetatbestände des § 79 Abs. 3 TKG lässt sich ohne Weiteres mit dem Gesetzeswortlaut und den üblichen Auslegungsregeln beantworten. 150

Rechtsmittelbelehrung 151

Innerhalb eines Monats nach Zustellung dieses Urteils kann bei dem Verwaltungsgericht Köln schriftlich beantragt werden, dass das Oberverwaltungsgericht für das Land Nordrhein-Westfalen in Münster die Berufung zulässt. Der Antrag muss das angefochtene Urteil bezeichnen. 152

Innerhalb von zwei Monaten nach Zustellung des Urteils sind die Gründe darzulegen, aus denen die Berufung zuzulassen ist. Die Begründung ist, soweit sie nicht bereits mit dem Antrag vorgelegt worden ist, bei dem Oberverwaltungsgericht für das Land Nordrhein-Westfalen in Münster schriftlich einzureichen. 153

Der Antrag ist zu stellen und zu begründen durch einen Rechtsanwalt oder einen Rechtslehrer an einer staatlichen oder staatlich anerkannten Hochschule eines Mitgliedstaates der Europäischen Union, eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum oder der Schweiz, der die Befähigung zum Richteramt besitzt, oder eine diesen gleichgestellte Person als Bevollmächtigten. Behörden und juristische Personen des öffentlichen Rechts einschließlich der von ihnen zur Erfüllung öffentlicher Aufgaben gebildeten Zusammenschlüsse können sich auch durch eigene Beschäftigte mit Befähigung zum Richteramt oder durch Beschäftigte mit Befähigung zum Richteramt anderer Behörden oder juristischer Personen des öffentlichen Rechts einschließlich der von ihnen zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse vertreten lassen. Auf die besonderen Regelungen in § 67 Abs. 4 Sätze 7 und 8 VwGO wird hingewiesen. 154

Beschluss 155

Der Wert des Streitgegenstandes wird bis zur Bekanntgabe des Verbindungsbeschlusses vom 27. Februar 2023 für die ursprünglichen Verfahren wie folgt festgesetzt: 156

für das Verfahren 1 K 6109/21 auf 157

5.000,- Euro, 158

für das Verfahren 1 K 1167/22 auf	159
500,- Euro;	160
danach auf	161
5.000,- Euro.	162

Gründe	163
---------------	-----

Die Festsetzung des Streitwerts beruht, auch in Bezug auf den Einzelbetrag des ursprünglichen Verfahrens 1 K 6109/21, auf § 52 Abs. 2 GKG. Der festgesetzte Wert entspricht insoweit jeweils dem Auffangstreitwert. Für den Einzelbetrag des ursprünglichen Verfahrens 1 K 1167/22 wird der Streitwert gemäß § 52 Abs. 1 GKG auf die niedrigste Wertstufe festgesetzt. Der Streitgegenstand dieses Verfahrens war auf die Informationen zu zwei Hauptverteilern beschränkt, die die Klägerin im Verwaltungsverfahren nachgeliefert hatte.	164
---	-----

Rechtsmittelbelehrung	165
------------------------------	-----

Gegen diesen Beschluss kann innerhalb von sechs Monaten, nachdem die Entscheidung in der Hauptsache Rechtskraft erlangt oder das Verfahren sich anderweitig erledigt hat, bei dem Verwaltungsgericht Köln schriftlich oder zur Niederschrift des Urkundsbeamten der Geschäftsstelle Beschwerde eingelegt werden, über die das Oberverwaltungsgericht für das Land Nordrhein-Westfalen in Münster entscheidet, falls das Verwaltungsgericht ihr nicht abhilft. Ist der Streitwert später als einen Monat vor Ablauf der genannten Frist festgesetzt worden, kann die Beschwerde innerhalb eines Monats nach Zustellung oder formloser Mitteilung des Festsetzungsbeschlusses eingelegt werden. Die Beschwerde ist nur zulässig, wenn der Wert des Beschwerdegegenstandes zweihundert Euro übersteigt. Die Beschwerde findet auch statt, wenn sie das Gericht, das die Entscheidung erlassen hat, wegen der grundsätzlichen Bedeutung der zur Entscheidung stehenden Frage zulässt.	166
---	-----