

ERGEBNISPAPIER



**Telekommunikationsrecht –
wie das Recht Schritt hält**

Impressum

Herausgeber

Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung

Plattform Industrie 4.0
Bülowsstraße 78
10783 Berlin

Stand

April 2021

Diese Publikation wird ausschließlich als Download angeboten.

Gestaltung

PRpetuum GmbH, 80801 München

Bildnachweis

iStockphoto
metamorworks / S. 4
putilich / Titel

Zentraler Bestellservice für Publikationen der Bundesregierung:

E-Mail: publikationen@bundesregierung.de
Telefon: 030 182722721
Bestellfax: 030 18102722721

Diese Publikation wird vom Bundesministerium für Wirtschaft und Energie im Rahmen der Öffentlichkeitsarbeit herausgegeben. Die Publikation wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Bundestags-, Landtags- und Kommunalwahlen sowie für Wahlen zum Europäischen Parlament.



Inhalt

Einleitung	3
A: Steckbrief	4
B: Juristische Einschätzung	5
C: Handlungsoptionen und Handlungsempfehlungen	9

Einleitung

Die Arbeitsgruppe 4 „Rechtliche Rahmenbedingungen“ (AG 4) der Plattform Industrie 4.0 hat die Aufgabe, systematisch die aus ihrer Sicht wichtigsten rechtlichen Themen und Problemaufrisse von Industrie 4.0-Prozessen zu identifizieren und Handlungsoptionen aufzuzeigen. Als einen relevanten Rechtsbereich analysiert die AG 4 das Telekommunikationsrecht. In der vorliegenden Auflage der Ergebnispublikation haben sich die Anwälte sowie die Unternehmens- und Verbandsjuristen den aktuellen Entwicklungen in diesem dynamischen Rechtsbereich gewidmet.

Die Vernetzung von Produktionsanlagen und Produktionsprozessen ist ein wesentlicher Bestandteil von Industrie 4.0-Anwendungen. Daten können nur dann in Produktionsprozessen gewonnen und genutzt werden, wenn Produktionsanlagen miteinander und mit zentralen Servereinheiten verbunden sind. Insofern beschäftigt sich diese Auflage mit den Fragen, inwieweit bei der Nutzung von Industrie 4.0-Anwendungen die Vorgaben des TKG zu beachten sind, ob die Datenkommunikation im Rahmen von Industrie 4.0-

Anwendungen dem Fernmeldegeheimnis und dem speziellen Telekommunikationsdatenschutz unterfällt und welche besonderen Sicherheitsvorgaben sich aus dem TKG für Industrie 4.0-Anwendungen ergeben. Abschließend wird die Frage beleuchtet, was im Kontext öffentliche Sicherheit zu beachten ist.

Die fünf Kapitel beginnen jeweils mit einer kurzen Zusammenfassung und einem Steckbrief (Teil A), in dem das Thema sowie die sich ergebenden Fragen und Handlungsfelder abgesteckt werden. An die Steckbriefe schließt sich Teil B mit der juristischen Einschätzung der Themenkomplexe an. Dieser Teil umfasst die Zusammenstellung und Prüfung der relevanten existierenden rechtlichen Grundlagen hinsichtlich der aufgeworfenen Fragen bzw. Handlungsfelder. Abschließend werden im Teil C zu jedem Themenkomplex mögliche Handlungsoptionen für den Gesetzgeber aufgezeigt sowie konkrete Handlungsempfehlungen aus Sicht der Arbeitsgruppe „Rechtliche Rahmenbedingungen“ gegeben.



A: Steckbrief

Worum geht es:

Wesentlicher Bestandteil von Industrie 4.0-Anwendungen ist die Vernetzung von Produktionsanlagen und Produktionsprozessen. Daten können nur dann in Produktionsprozessen gewonnen und genutzt werden, wenn Produktionsanlagen miteinander und mit zentralen Servern verbunden sind. Auch die Steuerung von Produktionsprozessen in Echtzeit und das autonome Fahren von Transportfahrzeugen auf dem Produktionsgelände erfordern, dass die involvierten Maschinen und Geräte miteinander und mit zentralen Servern „sprechen“. Diese Vernetzung von Produktionsanlagen erfolgt über Telekommunikation, entweder kabelgebunden oder aber – immer vordringlicher – über Funk (WLAN oder Mobilfunk). Zuletzt ist speziell für die industrielle Anwendung der neue Mobilfunkstandard 5G entwickelt worden.

Das Telekommunikationsrecht hat sich seit der Marktliberalisierung Ende der 90er-Jahre stetig weiterentwickelt und umfasst neben seinem Kern, den Regelungen zum Zugang zu TK-Infrastruktur von marktbeherrschenden Unternehmen, auch Regelungen, die symmetrisch

TK-Anbieter unabhängig von deren Marktmacht treffen. Dies sind Regelungen zum Kunden- und Datenschutz, zur Netz-, Dienst- und öffentlichen Sicherheit, aber auch Regelungen zur Netzneutralität und zur Vergabe von Rufnummern und anderen Kennungen.

Mit der neuen Richtlinie über den europäischen Kodex für die elektronische Kommunikation¹ („TK-Kodex“) hat der europäische Richtlinienggeber den Richtlinienrahmen, der bisher die Basis für das deutsche TKG bildete, grundlegend reformiert.² Der deutsche Gesetzgeber setzt die Änderungen, die durch den TK-Kodex erfolgt sind, aktuell mit dem Telekommunikationsmodernisierungsgesetz in nationales Recht um und novelliert das TKG grundlegend.

Im novellierten TKG werden erstmals spezielle Regelungen für die Maschinenkommunikation (M2M) aufgenommen, die auch für Industrie 4.0-Anwendungen Bedeutung haben. Neben dem TKG wird der Telekommunikationsdatenschutz im neu geschaffenen Telekommunikations-Telemedien-Datenschutz-Gesetz („TTDSG“) geregelt. Zudem ergeben sich aus weiteren Richtlinien und Verordnungen der EU zusätzlich Vorgaben für TK-Anbieter. Die wesentlichen Richtlinien und Verordnungen sind die ePrivacy-Richtlinie³, die Roaming-Verordnung⁴ und die TK-Binnenmarkt-VO⁵.

1 Richtlinie (EU) 2018/1972 v. 11.12.2018 über den europäischen Kodex für die elektronische Kommunikation.

2 Aufgehoben wurden die Zugangsrichtlinie (Richtlinie 2002/19/EG), die Genehmigungsrichtlinie (Richtlinie 2002/20/EG), die Rahmenrichtlinie (Richtlinie 2002/21/EG) und die Universaldienstrichtlinie (Richtlinie 2002/22/EG).

3 Richtlinie 2002/58/EG v. 12.06.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

4 Verordnung (EU) 531/2012 v. 13.06.2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union.

5 Verordnung (EU) 2015/2120 v. 25.11.2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union.

Fragen und Handlungsfelder:

- Inwieweit sind für das Design, den Betrieb oder die Nutzung von Industrie 4.0-Anwendungen die Vorgaben des TKG zu beachten?
- Unterfällt die Datenkommunikation im Rahmen von Industrie 4.0-Anwendungen dem Fernmeldegeheimnis und dem speziellen Telekommunikationsdatenschutz?
- Welche besonderen Sicherheitsvorgaben ergeben sich aus dem TKG für Industrie 4.0-Anwendungen?
- Sind für Industrie 4.0-Anwendungen Funkfrequenzen für Campus-Netze möglich?
- Was gilt es im Kontext öffentliche Sicherheit zu beachten?

B: Juristische Einschätzung**1. Anwendungsbereich des TKG für Industrie 4.0-Anwender**

Die Anwendbarkeit des TKG ergibt sich nach § 1 Abs. 2 TKG-RefE für Anbieter von Telekommunikationsdiensten i. S. d. § 3 Abs. 1 TKG-RefE. Zentrales Element des Anwendungsbereichs des TKG-RefE sind dabei „Telekommunikationsdienste“. Diese werden in § 3 Nr. 61 TKG-RefE definiert und erfahren im Vergleich zur bisherigen Definition in § 3 Nr. 24 TKG eine definitorische Erweiterung.

a. Telekommunikationsdienste

Das neue TKG fasst unter „Telekommunikationsdiensten“ nunmehr solche Dienste zusammen, die in der Regel gegen Entgelt über Telekommunikationsnetze erbracht werden, mit Ausnahme von Diensten, die Inhalte über Telekommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben. Damit umfasst die erweiterte Definition der Telekommunikationsdienste a) Internetzugangsdienste, b) interpersonelle Telekommunikationsdienste und c) Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation genutzt werden. Das TKG findet damit wie bisher auf klassische Dienste der Signalübertragung Anwendung (wie bspw. SMS und Sprachtelefonie) und nunmehr auch auf interpersonelle Telekommunikationsdienste, die selbst keine Signalübertragung darstellen (wie bspw. E-Mail, Messenger, VoIP).

Interpersonelle Telekommunikationsdienste sind nach § 3 Nr. 24 TKG-RefE gewöhnlich gegen Entgelt erbrachte Dienste, die einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze zwischen

einer endlichen Anzahl von Personen ermöglichen, wobei der Empfänger von der Person bestimmt wird, die die Telekommunikation veranlasst.

Anwender von Industrie 4.0-Lösungen stellen in der Regel keine Internetzugangsdienste bereit und bieten mit ihren Anwendungen der Maschinenvernetzung auch keine Möglichkeit der interpersonellen Kommunikation. Allerdings können Industrie 4.0-Anwendungen Dienste sein, die ganz oder überwiegend in der Übertragung von Signalen bestehen. Dies kann beispielsweise der Betrieb eines Campus-Netzes auf dem Produktionsgelände sein. Betreiber ist hierbei nicht notwendigerweise derjenige, der die TK-Anlage steuert, sondern derjenige, der gegenüber den Nutzern für die Signalübertragung verantwortlich ist.⁶

b. Telekommunikationsnetz

Auch Betreiber von Telekommunikationsnetzen unterliegen den Vorgaben des TKG. Ein Telekommunikationsnetz ist gemäß § 3 Nr. 65 TKG-RefE die Gesamtheit von Übertragungssystemen. Dabei ist es unerheblich, ob sie auf einer permanenten Infrastruktur oder zentralen Verwaltungskapazität basieren und gegebenenfalls Vermittlungs- und Leitweeinrichtungen sowie anderweitige Ressourcen einsetzen. Darin sind auch die nicht aktiven Netzbestandteile mit eingeschlossen, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen. Ebenso betroffen sind Satellitennetze, leitungs- und paketvermittelte Netze, einschließlich des Internets und mobiler Netze, Stromleitungssysteme (soweit sie zur Signalübertragung genutzt werden), Netze für Hör- und Fernsehfunksowie Kabelfernsehnetze (unabhängig von der Art der übertragenen Information). Derjenige Industrieanwender, der seine Produktionsanlage vernetzt und dabei zur Vernetzung eigene Übertragungsinfrastruktur

6 EuGH, Urt. v. 30.04.2014 – C-475/12.

tur betreibt oder als Verantwortlicher für sich betreiben lässt, ist ein Betreiber eines Telekommunikationsnetzes, mit der Folge, dass die Vorgaben des TKG und diejenigen des TTDSG auf ihn Anwendung finden.⁷

c. Öffentliche Telekommunikationsnetze oder öffentlich zugängliche Telekommunikationsdienste

Ein Großteil der Pflichten des TKG und auch des TTDSG betrifft nur öffentliche Telekommunikationsnetze oder öffentlich zugängliche Telekommunikationsdienste. Öffentlich zugänglich sind Telekommunikationsdienste, wenn diese einem unbestimmten Personenkreis zur Verfügung stehen.⁸ Die Öffentlichkeit ist in der Regel dann nicht gegeben, wenn die Netze oder Dienste vom Industrie 4.0-Anwender selbst genutzt werden.⁹ Ein vernetztes Produktionsgelände nutzt in der Regel der Anwender nur selbst für sich. Eröffnet er den Zugang zu seinen vernetzten Anlagen aber auch Zulieferern und können diese die vernetzten Anwendungen bspw. im Rahmen eines integrierten Produktionsprozesses nutzen, muss über die Öffentlichkeit des Netzes und der Dienste nachgedacht werden. Maßgeblich wird sein, ob nur seine Zulieferer Zugang zu seinem Telekommunikationsnetz erhalten, was keinen unbestimmten Personenkreis darstellt, oder ob der Zugang darüber hinaus auch weiteren Unternehmen oder Personengruppen offensteht.

Handlungsempfehlung

Angesichts der komplexen Pflichten, die sich für TK-Anbieter aus dem TKG und aus EU-Verordnungen ergeben, kann es sinnvoll sein, die Anwendbarkeit dieser Gesetze und Regelungen zu begrenzen. Insoweit gilt es, Industrie 4.0-Szenarien bereits in der Konzeptphase auf etwaige telekommunikationsrechtliche Auswirkungen der Inbetriebnahme oder Vernetzung von Industrie 4.0-Anwendungen zu beleuchten und gegebenenfalls Gestaltungsalternativen zu erwägen. Zielführend können bspw. folgende Weichenstellungen sein:

- „Konnektivität“ (Netze und Dienste) für Industrie 4.0-Anwendungen von externen Anbietern einkaufen (anstatt selbst als Betreiber zu agieren);

- Industrie 4.0-Anwendungen ausschließlich einem möglichst eng definierten Personenkreis verfügbar machen (ein Angebot an die Öffentlichkeit ausschließen).

2. Fernmeldegeheimnis und Telekommunikationsdatenschutz für Industrie 4.0-Anwendungen

Das telekommunikationsrechtliche Fernmeldegeheimnis, welches bisher in § 88 Abs. 2 TKG geregelt wurde, galt nach seinem Wortlaut für jeden Diensteanbieter – ein Angebot an die Öffentlichkeit war nicht erforderlich. Der zwischenzeitlich veröffentlichte Referentenentwurf des TTDSG beschränkt in § 3 Abs. 2 das Fernmeldegeheimnis nunmehr auf Anbieter öffentlicher Telekommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze.¹⁰

Die ePrivacy-RL, die die europäische Grundlage des Telekommunikationsdatenschutzes bildet, umfasst vom Schutzbereich des Fernmeldegeheimnisses in Art. 5 Abs. 1 ebenfalls nur ein öffentliches Kommunikationsnetz oder einen öffentlich zugänglichen Kommunikationsdienst. Damit unterliegen nach dem im TTDSG-RefE geänderten Fernmeldegeheimnis und den europäischen Vorgaben Anbieter von geschlossenen Benutzergruppen und innerbetrieblichen Unternehmensnetzen, die nicht öffentlich sind, nicht dem Fernmeldegeheimnis des TTDSG-RefE der ePrivacy-RL.¹¹ Auch die Regelungen des sektorspezifischen Datenschutzes über die Verarbeitung von Verkehrsdaten in §§ 9 und 10 TTDSG-RefE gelten nach § 1 Abs. 1 Nr. 2 TTDSG-RefE nur für Anbieter öffentlicher Telekommunikationsdienste und Betreiber öffentlicher Telekommunikationsnetze.

Handlungsempfehlungen

Es ist zu begrüßen, dass lediglich die Kommunikation über öffentliche Telekommunikationsnetze dem Fernmeldegeheimnis und dem Telekommunikationsdatenschutz unterliegt. Über die Telekommunikationsnetze von vernetzten Produktionsstätten wird keine Kommunikation übertragen, die des besonderen Schutzes durch das Fernmeldegeheimnis und des speziellen Telekommunikationsdatenschutzes bedarf. Da eine Verletzung des Telekommunikationsgeheimnisses nach § 206 Abs. 1 StGB strafbewährt ist, müssen Industrie 4.0-Anwender besondere Vorsicht walten lassen,

7 Der EuGH grenzt anhand der Verantwortlichkeit für die Signalübertragung ab: EuGH Urt. v. 05.06.2019 – C-142/18 – Skype vs. IBP und EuGH Urt. v. 13.06.2019 – C-193/18 – Google LLC vs. Bundesrepublik Deutschland.

8 So die Definition des § 3 Nr. 44 TKG-RefE. Das OLG Hamm, Urt. v. 28.05.2020 – 4 U 82/19, sieht einen Vermieter, der seinen Mietern Telekommunikationsanschlüsse anbietet, nicht als Anbieter öffentlich zugänglicher Telekommunikationsdienste an, weil das Angebot nur gegenüber seinen Mietern und damit einem begrenzten Adressatenkreis gegenüber erfolgt.

9 Sassenberg/Kiparski in: Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things, 2. Aufl., 2020, Kap. 2 Rn. 9.

10 Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien sowie zur Änderung des Telemediengesetzes v. 12.01.2021 (TTDSG).

11 Kiparski/Sassenberg, CR 2018, 325.

wem sie Zugang zu ihrem TK-Netz gewähren, um nicht ungewollt ein öffentliches Telekommunikationsnetz zu betreiben.

3. Sicherheitsvorgaben für Industrie 4.0-Anwender

§ 164 TKG-RefE regelt spezielle technische Schutzmaßnahmen, die je nach Art der erbrachten Telekommunikationsdienste einzuhalten sind. Grundsätzlich müssen auch Diensteanbieter, die keine öffentlichen Telekommunikationsdienste erbringen, erforderliche technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten treffen.

Bietet der Industrie 4.0-Anwender hingegen öffentlich zugängliche Dienste oder Netze an, dann betreffen diesen eine Vielzahl an Sicherheitspflichten aus § 164 ff. TKG-RefE. Dies umfasst u. a. die Pflicht zur Benennung eines Sicherheitsbeauftragten und die Pflicht, ein Sicherheitskonzept zu erstellen. Ebenfalls ist der Anwender verpflichtet, angemessene technische Vorkehrungen und sonstige Maßnahmen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch soweit sie durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, zu treffen und die Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten zu beherrschen. Zudem muss er erforderliche technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten treffen. Die Bundesnetzagentur („BNetzA“) hat als zuständige Aufsichtsbehörde einen Sicherheitskatalog erstellt,¹² der Anbietern als Grundlage für das Sicherheitskonzept nach § 165 Abs. 2 TKG-RefE und für die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach § 164 Abs. 1 und 2 TKG-RefE dient. Aktuell überarbeitet die BNetzA den Sicherheitskatalog, um neuen Anforderungen an die Netzsicherheit Rechnung zu tragen.¹³ Dies sind insbesondere Anforderungen durch die Anbindung eines Telekommunikationssystems an das Internet oder die Erbringung von Telekommunikationsdiensten im Internet. Beides wird auf Industrie 4.0-Anwender eher nicht zutreffen, da diese ihre

Unternehmensnetze vom Internet abschirmen werden. Ebenfalls werden zusätzliche Sicherheitsanforderungen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial aufgestellt. Dies gilt für öffentliche Telekommunikationsnetze und -dienste mit mehr als 100.000 Teilnehmern und damit nicht für Industrie 4.0-Anwender.

Vorgaben für die Daten- und Informationssicherheit ergeben sich aus § 168 TKG-RefE. Die Meldepflicht des § 168 Abs. 1 TKG-RefE bei der Verletzung des Schutzes personenbezogener Daten geht der der DS-GVO vor. Die Meldung hat gegenüber der BNetzA und dem BfDI zu erfolgen. Aus § 168 TKG-RefE ergeben sich neben der Pflicht, ein Verzeichnis über Verletzungen zu führen, auch Informationspflichten bei Störungen. Sicherheitsvorfälle mit erheblichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste müssen nach § 167 Abs. 1 TKG-RefE unverzüglich der BNetzA und dem BSI gemeldet werden. Wie schon bei den Sicherheitsvorgaben des § 164 Abs. 2 TKG-RefE treffen die Vorgaben für die Daten- und Informationssicherheit und diejenigen für Sicherheitsvorfälle nur diejenigen Industrie 4.0-Anwender, die öffentlich zugängliche Telekommunikationsdienste erbringen oder öffentliche Telekommunikationsnetze betreiben.

Handlungsempfehlungen

Industrie 4.0-Anwender, die keine öffentlichen Dienste anbieten und kein öffentliches Telekommunikationsnetz betreiben, werden von den Sicherheitsvorgaben und Vorgaben für die Daten- und Informationssicherheit des TKG nicht erfasst. Dies gilt es im Kontext dem Grunde nach beizubehalten, da das TKG und die grundlegenden EU-Richtlinien speziell auf öffentliche Telekommunikationsdienste und -netze ausgelegt sind. Gleichwohl gilt es für Industrie 4.0-Anwender, die allgemeinen Vorgaben der IT-Sicherheit einzuhalten bzw. die Vorgaben des IT-Sicherheitsgesetzes, sofern der Industrie 4.0-Anwender als Betreiber Kritischer Infrastrukturen oder als Unternehmen im besonderen öffentlichen Interesse in den Anwendungsbereich des aktuell in der Novellierung befindlichen IT-Sicherheitsgesetzes fällt.¹⁴

12 BNetzA, Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten, Version 1.1, Stand 07.01.2016.

13 BNetzA, Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten, Version 2.0, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf?blob=publicationFile&v=10 (letzter Abruf: 30.01.2021).

14 Mit Beschluss vom 16.12.2020 hat die Bundesregierung einen Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme angenommen und damit das Legislativverfahren gestartet. Nach entsprechender Notifizierung bei der EU-Kommission ist eine finale parlamentarische Beratung im April 2021 vorgesehen sowie eine finale Befassung des Bundesrates für den 07.05.2021.

4. Funkfrequenzen für Campus-Netze

Mit der Vergabe der sog. 5G-Frequenzen hat die BNetzA erstmals die Einzelzuteilung von Frequenzen zur lokalen Nutzung für Mobilfunk im Frequenzbereich 3,7 bis 3,8 GHz ermöglicht.¹⁵ Diese Frequenzen können u. a. für Industrie 4.0 eingesetzt werden. Sie werden nicht im Rahmen einer Auktion, sondern gemäß § 55 Abs. 3 TKG (§ 90 Abs. 3 TKG-RefE) als Einzelzuteilung ohne Vergabeverfahren vergeben. Antragsberechtigt für eine lokale Frequenz ist jeweils der Eigentümer des Grundstücks oder jemand, der ein sonstiges Nutzungsrecht an demselben (z. B. Miete, Pacht) hat. Mit den lokalen Frequenzen sind Industrieunternehmen erstmals in der Lage, selbst bei der BNetzA Frequenzen für ihr Produktionsareal zu beantragen und damit selbst ein Campus-Netz aufzubauen. Mit Stand Januar 2021 hat die BNetzA bereits 102 Zuteilungen von Frequenzen für lokale 5G-Netze erteilt.¹⁶ Wichtig ist, dass mit den lokalen Frequenzen keine öffentlichen Telekommunikationsdienstleistungen erbracht werden dürfen.¹⁷

Handlungsempfehlungen

Lokale Frequenzen sind ein wichtiger Schritt für Campus-Netze und damit für Industrie 4.0-Anwender. Die Einschränkung in der Nutzung von lokalen Frequenzen auf nicht-öffentliche Telekommunikationsdienstleistungen schützt Industrie 4.0-Anwender zudem vor der Anwendbarkeit zahlreicher Vorgaben des TKG und des TTDSG. Dennoch sollte die Nachfrage nach lokalen Frequenzen eng überwacht werden, da es sich bei Funkfrequenzen um knappe Güter handelt, die bei zu geringer Nutzung ggf. anderweitig allokiert werden könnten.

Neben der Eigenrealisierung eines Campus-Netzes gibt es verschiedene Abstufungen des Outsourcings des Campus-Netzes auf einen auf den Netzbetrieb spezialisierten Anbieter. Industrie 4.0-Anwender können die Konnektivität insgesamt von einem Mobilfunknetzbetreiber einkaufen, der dann für den Industrie 4.0-Anwender ein Campus-Netz

errichtet, hierfür seine Funkfrequenzen nutzt, ggf. auch Verbindungen aus dem Campus-Netz heraus in das Telefonnetz und das Internet anbietet und den Netzbetrieb realisiert. In diesem Fall obliegen die rechtlichen Pflichten aus dem TKG und dem TTDSG dem Mobilfunknetzbetreiber, jedenfalls so lange, wie der Industrie 4.0-Anbieter sein Campus-Netz nicht Dritten zur Verfügung stellt.

Industrie 4.0-Anwender können auch für sich lokale Frequenzen beantragen, eigenständig Netztechnik von einem Hersteller erwerben, aber den Netzbetrieb auf einen Betreiber outsourcen. Betreibt der Netzbetreiber das Campus-Netz in eigener Hoheit, ist dieser ein Netzbetreiber und unterliegt den rechtlichen Verpflichtungen aus dem TKG und dem TTDSG.¹⁸

Was müssen Industrie 4.0-Anwender hinsichtlich der Vorgaben der öffentlichen Sicherheit beachten?

Die Vorgaben zur öffentlichen Sicherheit befinden sich im 10. Teil des TKG-RefE. Diese knüpfen einerseits hinsichtlich der Umsetzung von Überwachungsmaßnahmen an Telekommunikationsanlagen an, mit denen öffentlich zugängliche Telekommunikationsdienste erbracht werden (§ 169 TKG-RefE), und andererseits hinsichtlich von Auskunftsersuchen von Sicherheitsbehörden an nummerngebundene interpersonelle Telekommunikationsdienste nach § 3 Nr. 37 TKG-RefE oder Dienste der Signalübertragung, bei denen Rufnummern vergeben werden (§ 171 TKG-RefE). Dies heißt insbesondere, dass derjenige Industrie 4.0-Anwender, der mit seinen Telekommunikationsanlagen öffentlich zugängliche Telekommunikationsdienste erbringt, Maßnahmen und Einrichtungen zur Überwachung der Telekommunikation vorzuhalten und organisatorische Vorkehrungen für deren unverzügliche Umsetzung zu treffen hat. Derjenige, der Rufnummern vergibt, um darüber interpersonelle Telekommunikation anzubieten, oder Dienste der Signalübertragung, muss die Daten der Anschlussinhaber erheben und Sicherheitsbehörden beauskunften.

15 BNetzA, BK1-17/001, VfG. Nr. 62/2018, AmBl. 10/2018 v. 30.05.2018, bestätigt durch BVerwG, Urt. v. 24.06.2020 – 6 C 3.19.

16 BNetzA, Übersicht der Zuteilungsinhaber für Frequenzzuteilungen für lokale Frequenznutzungen im Frequenzbereich 3.700–3.800 MHz, Stand 15.01.2021, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OffentlicheNetze/LokaleNetze/Zuteilungsinhaber.pdf;jsessionid=05E7DF13AFFA3E22DD41C4336E7F00CA?__blob=publicationFile&v=5 (letzter Abruf: 30.01.2021).

17 BNetzA, Grundlegende Rahmenbedingungen des zukünftigen Antragsverfahrens für den Bereich 3.700 MHz – 3.800 MHz für Anwendungen des drahtlosen Netzzugangs, VfG. Nr. 43/2019, AmBl. 6/2019 v. 27.03.2019.

18 Siehe zum Netzbetrieb: BGH, Urt. v. 16.03.2012 – V ZR 98/11.

C: Handlungsoptionen und Handlungsempfehlungen

Die Fokussierung der spezialgesetzlichen Vorgaben des TKG auf öffentliche Telekommunikationsnetze und -dienste sollte beibehalten werden. Reine Campus-Netze, die allein den vernetzten Produktionsanlagen des Unternehmens dienen, sind nicht öffentlich und unterfallen daher nicht den umfangreichen spezialgesetzlichen Regelungen des TKG und des TTDSG. Sicherheits- und Datenschutzanforderungen an Campus-Netze sollten sich aus den allgemeinen gesetzlichen Regelungen zur IT-Sicherheit¹⁹ und dem Datenschutz der DS-GVO ergeben.

Auch sollten die Arbeiten an der ePrivacy-Verordnung vorangetrieben und zeitnah zum Abschluss gebracht werden.

Die Kollisionsregel des Art. 95 DS-GVO erhöht die Komplexität der rechtlichen Regelungen im Telekommunikationsdatenschutz erheblich. Diese Komplexität sollte durch die ePrivacy-Verordnung reduziert werden.

Für Industrie 4.0-Anwender und für Unternehmen, die selbst Campus-Netze betreiben, gilt es darauf zu achten, den Zugang zu ihrem Campus-Netz so zu gestalten, dass sie kein öffentliches Netz betreiben und keine öffentlich zugänglichen Telekommunikationsdienste anbieten. So kann die Anwendbarkeit vieler spezialgesetzlicher Regelungen des TKG und des TTDSG ausgeschlossen werden. Soll Dritten Zugang zum Campus-Netz gewährt werden, sollte über ein Betreibermodell des Campus-Netzes durch einen Dritten nachgedacht werden, der die spezialgesetzlichen Vorgaben des TKG und des TTDSG einfacher einhalten kann als ein Industrieunternehmen.

19 Sofern es sich bei den betroffenen Unternehmen um Kritische-Infrastruktur-Betreiber und Unternehmen im besonderen öffentlichen Interesse handelt, ist an der Stelle v. a. auf das in Novellierung befindliche IT-Sicherheitsgesetz zu verweisen.

AUTOREN

Dr. Angela Busche (Oppenhoff) | Dr. Alexander Duisberg (Bird&Bird) | Dr. Gerd Kiparski (1&1 Drillisch AG) | Thomas Schauf (Telekom AG)

