



Regierung des Kantons St.Gallen, Regierungsgebäude, 9001 St.Gallen

Eidgenössisches Departement für Umwelt,
Verkehr, Energie und Kommunikation
Bundeshaus Nord
3003 Bern

Regierung des Kantons St.Gallen
Regierungsgebäude
9001 St.Gallen
T +41 58 229 89 42
info.sk@sg.ch

St.Gallen, 3. September 2026

Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit; Vernehmlassungsantwort

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 27. Mai 2026 laden Sie uns zur Vernehmlassung zur Teilrevision des eidgenössischen Fernmeldegesetzes (SR 784.10; abgekürzt FMG) im Bereich Sicherheit ein. Wir danken für diese Gelegenheit und nehmen gern wie folgt Stellung:

Wir begrüssen die vorliegende Teilrevision des Fernmeldegesetzes im Bereich Sicherheit.

Leistungsfähige und ausfallsichere Fernmeldeinfrastrukturen sind essenziell zur Sicherstellung der Kommunikation inner- und ausserhalb der Schweiz, speziell auch im Bereich der Notfallkommunikation. Die grossflächigen Ausfälle der Notfallkommunikationssysteme sowie die veränderte geopolitische Bedrohungslage zeigen, dass die Infrastruktur resilienter werden muss. Auch besteht Handlungsbedarf in den Bereichen Konsumentenschutz, Missbrauchsbekämpfung sowie Kinder- und Jugendschutz.

Die Vorlage enthält einige wichtige und sinnvolle Bestimmungen zur Stärkung der Fernmeldeinfrastruktur sowie zur Prävention und Bekämpfung von deren missbräuchlichen Verwendung. Demgegenüber fehlen jedoch an verschiedenen Stellen verpflichtende Elemente, die den Behörden Möglichkeiten eröffnen würden, bei Nichteinhaltung der Gesetzesbestimmungen entsprechende Strafen und/oder Sanktionen (bspw. Einschränkungen von fernmelderechtlichen Dienstleistungen) auszusprechen. Die vorliegenden Gesetzesanpassungen dürften nur dann eine nachhaltige Wirkung entfalten, wenn auch entsprechende Sanktionsmöglichkeiten bei Verstössen vorhanden sind und durchgesetzt werden (können).

Die Motionen Seiler-Graf (24.4392) «Es braucht griffige Massnahmen gegen die missbräuchliche Verwendung von schweizerischen Rufnummern» sowie Götte (24.4393) «Es braucht griffige Massnahmen gegen die missbräuchliche Verwendung von schweizerischen Domains!», deren Anliegen zur Stärkung des Konsumentenschutzes mit der vorlie-

genden Teilrevision umgesetzt werden sollen, wurden unter aktiver Mitwirkung der Kantonspolizei St.Gallen lanciert. Nach Durchsicht der Vernehmlassungsvorlage ist festzustellen, dass die Anliegen der beiden Motionen erst teilweise berücksichtigt wurden. Um die Anliegen dieser Motionen vollständig umzusetzen, sind nach unserer Auffassung weitere Massnahmen notwendig, die eine weitere Teilrevision des FMG notwendig machen.

Weiter soll gemäss erläuterndem Bericht (S. 14) die thematisch verwandte und gleichzeitig eingereichte Motion Candinas (24.4391) «Es braucht einen wirksamen Schutz gegen Call-ID-Spoofing von schweizerischen Rufnummern!» gestützt auf die geltenden formellrechtlichen Bestimmungen im FMG auf Verordnungsstufe umgesetzt werden. Dazu halten wir Folgendes fest:

- In Anbetracht der Tragweite des leider weit verbreiteten Phänomens «Spoofing» erscheint es angemessen, wenn grundlegende Bestimmungen zur Bekämpfung von Spoofing auf Stufe eines Gesetzes im formellen Sinn geschaffen würden. Die detaillierte Umsetzung könnte folglich auf Verordnungsstufe erfolgen.
- Die in der Motion Candinas geforderten Massnahmen zur Bekämpfung von Spoofing werden trotz der seit 1. Januar 2026 bzw. 1. Juli 2026 umgesetzten bzw. in Umsetzung befindenden Anpassungen (4. Ausgabe des Anhangs 1.7 der Verordnung des BAKOM vom 9. Dezember 1997 über Fernmeldedienste und Adressierungselemente [SR 784.101.113/1.7]) nur ungenügend umgesetzt. Dass Call-ID-Spoofing trotz der aktuellen Massnahmen weiterhin nur ungenügend eingedämmt werden kann, hat sich seit Jahresbeginn gezeigt. Dies führt zum Schluss, dass die Motion noch nicht vollständig umgesetzt ist.

Weiter fordern wir, dass im FMG ein zusätzlicher Artikel geschaffen wird, der den Datenaustausch zwischen Switch, BACS, Fedpol und den kantonalen Polizeibehörden sowie den Providern regelt und zum Ziel hat, erkannte bösartige oder vermögensschädigende URL in einer Datenbank («Real Time») verbreiten zu können. Heute besteht im Bereich URL zwar ein wöchentliches Bulletin, dieses ist in der heutigen Form jedoch zu träge. Phishing URL können bereits nach rund zwei Stunden wieder «alt» oder verbraucht oder von der Täterschaft wieder abgeschaltet sein. Gefordert ist daher ein schnellerer Austausch nach Erkennen von solchen URL mit sämtlichen Providern. Dabei ist die Mitwirkung letztgenannter massgebend. Ein Schutz der Bevölkerung kann nicht umgesetzt werden, wenn sich die Provider nicht am Blocking der URL oder weiterer Adressierungselemente beteiligen.

Schliesslich begrüssen wir die Pflicht der Anbieter zu Beratung der Eltern und zur Bereitstellung von Kontroll-Apps. Diese reicht unseres Erachtens aber nicht aus, da die Verantwortung so rein bei den Eltern verbleibt. Für einen wirksamen Schutz bräuchte es zwingend technische Mechanismen bzw. Schutzfunktionen direkt bei der Nutzung der Angebote. Zudem sollte sich die Revision nicht nur auf den Kinder- und Jugendschutz bei pornografischem Material beschränken, sondern muss auch Gefahren wie Cybermobbing, Gewaltinhalte, Cybergrooming, Fake News, Schutz der eigenen Daten und Privatsphäre sowie allfällige zukünftige Gefahren verbindlich sowie zukunftssicher abdecken.

Bei der weiteren Ausgestaltung der Vorlage ist zudem sicherzustellen, dass den Anforderungen an Rechtsschutz, Datenschutz und Sicherheit angemessen Rechnung getragen wird.

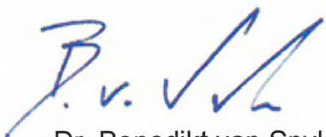
Unsere Anmerkungen und Änderungsanträge zu den einzelnen Bestimmungen haben wir in einer separaten Beilage als Anhang zu diesem Schreiben festgehalten.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Im Namen der Regierung



Dr. Laura Bucher
Präsidentin



Dr. Benedikt van Spyk
Staatssekretär

Beilage:

Anhang mit Änderungsanträgen zu den einzelnen Bestimmungen und Stellungnahme zum Fragebogen zur Vernehmlassungsvorlage

Zustellung nur per E-Mail (pdf- und Word-Version) an:

tp-secretariat@bakom.admin.ch



Anhang zur Vernehmlassungsantwort «Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit»

Stellungnahme zur Vernehmlassungsvorlage

Artikel	Antrag	Begründung / Bemerkung
Art. 3 Bst. d	Zustimmung	Miteinbezug der Software ist wichtig, da heute nahezu alle Fernmeldeanlagen mit Software funktionieren.
Art. 4 Abs 4	Die KANN-Formulierung zur Veröffentlichung der Liste ist zu streichen und als Verpflichtung aufzuführen.	Eine solche Liste ist für die Übersicht und öffentliche Einsichtnahme für Strafverfolgungsbehörden unverzichtbar, entsprechend ist die KANN-Formulierung nicht zielführend. Das BAKOM ist zur Veröffentlichung zu verpflichten.
Art. 4 neuer Absatz 6	Neuer Absatz 6: Die zuständige Behörde kann der ausländischen Anbieterin von Fernmeldediensten mit Schweizer Adressierungselementen bei Nichteinhaltung der gesetzlichen Bestimmungen deren Registration und Leistungserbringung widerrufen.	Mit der vorliegenden Bestimmung. Ohne diese Bestimmung erscheint weiterhin problematisch, dass Nummernblöcke, welche an ausländische Anbieter verkauft wurden, bei Nichteinhaltung der gesetzlichen Pflichten nicht mehr zurückgerufen werden können. Damit sollen dem BAKOM Möglichkeiten geschaffen werden, die Registration und Leistungserbringung bei wiederholtem Fehlverhalten zu widerrufen.
Art. 6a neuer Absatz	Die Sperrung hat durch die Schweizer Anbieterin von Fernmeldediensten oder bei ausbleibender Rückmeldung der ausländischen Anbieterin direkt durch das BAKOM zu erfolgen.	Die Sperrung muss auch durch die CH-Anbieterin (bei Untervergabe) oder bei direktem Verkauf der Adressierungselemente ins Ausland durch das BAKOM möglich sein. Ansonsten bestünden keine gesetzlichen Möglichkeiten bei der Vergabe an Anbieterinnen von Fernmeldediensten ins Ausland wirksame Sperrungen vorzunehmen. Bereits heute treten verschiedene ausländische Provider auf, welche die Daten der Kunden nicht bekannt geben, wobei keine wirksame Möglichkeit zur Sperrung besteht.
Art. 6a neuer Absatz	Die Anbieterin informiert die betroffene Person unverzüglich über die Sperrung und deren Grund. Sie stellt ein rasches Verfahren zur Berichtigung der Identifikationsdaten und zur Aufhebung einer ungerechtfertigten Sperrung sicher.	Bei einer falschen Zuordnung oder fehlerhaften Identifikation kann eine Sperrung die Kommunikation vollständig unterbrechen. Zwar stehen Kundinnen und Kunden grundsätzlich die Schlichtung nach Art. 12c FMG und der Zivilweg offen. Diese allgemeinen Wege ersetzen jedoch kein rasches, unmittelbar bei der Anbieterin verfügbares Korrekturverfahren.
Art. 6b Abs. 1	Ersetzen des Wortlautes "fedpol" durch "Polizeibehörden von Bund und Kantonen"	Fedpol hat keine entsprechenden Prozesse und personelle Ressourcen, welche die von Kantonen gemeldeten Betrugsfälle entgegennehmen und innert kurzer Zeit nach Meldungseingang an die Provider weiterleiten würde. Zudem verfügt fedpol in den allermeisten Fällen nicht selber über die notwendigen Erkenntnisse, um einen Hinweis auf Sperrung abzugeben. Diese stammen fast ausschliesslich von den Kantonen und dass diese aus der ganzen Schweiz zuerst an fedpol weitergeleitet werden müssen, um diese wiederum weiterzuleiten, ist ineffizient. Zudem geht wertvolle Zeit verloren.



		Um eine wirksame Gesetzesänderung vorzunehmen, ist fedpol wie auch den kantonalen Polizeikorps die Möglichkeit zu eröffnen, entsprechende Verdachtsmeldungen zeitverzugslos und selber abzusetzen. Im Übrigen gilt dasselbe auch für Absatz 2. Wenn Absatz 1 nicht geändert würde, hätte dies dieselben ineffizienten Auswirkungen, weshalb der Änderungsantrag zu Abs. 1 auch Auswirkungen auf Abs. 2 hat.
Art. 6b Abs. 1	Das Begriffspaar «begründeter Verdacht» ist durch «[begründete] Anhaltspunkte» oder «Indizien» zu ersetzen.	Der «begründete Verdacht» bzw. der «Verdacht» ist ein Begriff des Strafprozessrechts und kann kaum dem Normzweck eines präventiven Akts entsprechen (sog. Crime Disruption, S. 29 erläuternder Bericht). Ziel der Bestimmung ist, durch einen präventiven Akt die Sperrung vorzunehmen und damit die kriminelle Handlung zu stören. Nach vorliegender Auffassung würde bei der gegenständlichen Formulierung des «begründeten Verdachts» die Schwelle ungleich höher angesetzt, was nicht Sinn und Zweck eines präventiven Akts sein kann.
Art. 6b Abs. 1	Die Eingrenzung auf ausschliesslich Art. 146 StGB – Betrug ist zu eng und mind. einer Erweiterung auf ausgewählte Straftatbestände (wie z.B. Art. 156 - Erpressung [Sextorsion]) oder allgemein auf Vergehen und/oder Verbrechen	Die Einschränkung auf ausschliesslich Betrugsstatbestände (Art. 146 StGB) erscheint zu eng und dürfte damit nicht zur erwarteten Besserung führen. Die dieser Gesetzesänderung zugrundeliegende Motion Götte (24.4393) verlangt die Ausdehnung auf Vergehens- und Verbrechenstatbestände (inkl. deren Versuche) und mit der vorliegenden Einschränkung auf Betrug würde dem Anliegen der Motion nicht ansatzweise Rechnung getragen. Diese Forderung würde auch in angepasster Form weder dem Legalitätsprinzip noch dem Verhältnismässigkeitsprinzip widersprechen.
Art. 6b Abs. 1	Die Frist von fünf Tagen ist auf mind. 30 Tage zu verlängern	Die Sperrfrist von maximal fünf Tagen ist zu kurz, um weitere Massnahmen prüfen zu können oder wie im Bericht zur Vernehmlassung zu entnehmen ist, die Kriminalitätsstörung (Crime Disruption) über einen bestimmten Zeitraum aufrechterhalten zu können. Deshalb ist die Frist per Gesetz (mind. 30 Tage) zu verlängern, um eine wirksame und nachhaltige Entwicklung zu ermöglichen. Unklar ist mit vorliegender Bestimmung, was nach Ablauf der Frist passiert. Gemäss Vernehmlassungsunterlagen stellt die Sperrung gem. Abs. 1 einen präventiven Akt dar, um weitere kriminelle Handlungen zu unterbinden bzw. zu stören (sog. Crime Disruption). Diesem Grundgedanken widerspricht jedoch die Verlängerungsmöglichkeit durch die Strafverfolgungsbehörden (StA / Gerichte) gem. Abs. 4, weil damit der Sperrzweck vom präventiv-polizeilichen Handeln (in der Kompetenz der Polizeibehörden) einen direkten Übergang in den repressiven Akt, d.h. der gerichtspolizeilichen Handlung, wechselt. In der präventiven Handlung liegt jedoch keine Zuständigkeit der Staatsanwaltschaft. Eine solche Frist von 30 Tagen erscheint zumindest angemessen für die Fälle einer möglichen



		Anordnung der Fortführung nach Abs. 4 durch die Staatsanwaltschaft oder durch das Gericht, damit für die Eröffnung eines Strafverfahrens sowie Anordnung von Zwangsmassnahmen durch die Staatsanwaltschaft angemessen Zeit besteht (gem. vorgeschlagenem Prozess: Feststellung kant. Polizei – Rapportierung an fedpol – Rapportierung an kant. Staatsanwaltschaft – Eröffnung Strafverfahren – Fortführung der Sperrung).
Art. 6b Abs 3	Ersetzen des Wortlautes "fedpol" durch "Polizeibehörden von Bund und Kantonen"	In Analogie zum Änderungsantrag für Abs. 1 desselben Artikels ist die Formulierung entsprechend anzupassen, damit zielführende, zeitverzugslose und wirksame Sperrungen überhaupt ermöglicht werden können.
Art. 6b Abs 4	Die Rechtsfolge nach Abschluss des Verfahrens ist zu definieren, sofern an der Sperrung festgehalten werden muss/soll.	Die Rechtsfolge ist hier unklar, was nach Abschluss des Verfahrens mit der gesperrten Rufnummer oder der Domain geschehen soll. Es erscheint begrüssenswert, wenn der Gesetzgeber sich dazu äussert, was mit der gesperrten Telefonnummer oder mit dem gesperrten Domain-Namen beim Abschluss des Strafverfahrens geschehen soll, wenn eine Aufhebung der Sperre ausser Betracht fällt (eine «Einziehung» solcher fernmeldetechnischer Adressierungselemente als Gegenstände i.S.v. Art. 69 StGB dürfte im Ergebnis wenig zielführend sein).
Art. 6b Abs. 4	Schaffung einer neuen ausdrücklichen Grundlage im FMG oder der StPO für die direkte Sperrung von Telefonnummern oder eines Domain-Namens durch die Staatsanwaltschaft	Weiter wäre begrüssenswert, wenn im FMG (oder in der StPO) eine ausdrückliche rechtliche Grundlage geschaffen würde, dass auch ohne vorherige (präventiv-polizeiliche) Sperre im Rahmen eines Strafverfahrens die Sperrung einer Telefonnummer oder eines Domain-Namens von der Staatsanwaltschaft angeordnet werden kann («Die Staatsanwaltschaft oder das zuständige Gericht kann im Rahmen eines Strafverfahrens in sachgemässer Anwendung von Art. 263 ff. StPO anordnen, dass eine Telefonnummer oder ein Domain-Name gesperrt wird.» Es wäre auch zu normieren, wie (und durch wen) die gesperrten Adressierungselemente am Ende eines Strafverfahrens «eingezogen» werden können [definitiver Entzug der Verfügungsbeziehung der bisherigen Inhaberschaft über die Telefonnummer/Internet-Domain für die Zukunft].
Art. 6b neuer Absatz 6	Die betroffene Inhaberin oder der betroffene Inhaber ist so rasch wie möglich über die Sperrung und die zuständige Behörde zu informieren. Sie oder er kann eine anfechtbare Verfügung und eine unverzügliche Überprüfung bzw. Korrektur verlangen. Die Information kann aufgeschoben werden, soweit und solange dies zum Schutz der Prävention oder eines Strafverfahrens erforderlich ist.	Der blosse «Hinweis» einer Behörde und die anschliessende Sperrung durch eine Anbieterin oder Registerbetreiberin lassen den verfügbaren Rechtsweg nicht klar erkennen. Wegen der Rechtsweggarantie nach Art. 29a BV und der Möglichkeit, bei Realakten eine Verfügung nach Art. 25a VwVG zu verlangen, ist der Rechtsschutz ausdrücklich, rasch und für alle Sperrstellen einheitlich zu regeln. Dies ist besonders wichtig, wenn auch kantonale Polizeibehörden Sperrhinweise direkt erteilen können sollen.



Art. 13b Abs. 1	Absatz 1 ist auf die Bereitstellung von Abdeckungskarten für die Notsuche zu erweitern	Mit der Einschränkung auf Personendaten entfällt möglicherweise die gesetzliche Grundlage für die zur Verfügungstellung von sogenannten Abdeckungskarten. Hier muss das BAKOM aufzeigen, auf welcher gesetzlichen Grundlage die Abdeckungskarten bei Notsuchen in Zukunft zur Verfügung gestellt werden.
Art. 20	Zustimmung	Die Ausweitung der Flexibilität bezüglich zukunftsstaurlicher Kommunikationsmittel macht absolut Sinn. So kann beispielsweise die Videotelefonie aufschlussreiche Hinweise für eine Lagerfassung liefern. Eine Anbindung an zwei Anbieter ist dabei zwingen, um die Redundanz zu gewährleisten.
Art. 29 Abs1	Einfügen einer Frist von 30 Tagen / eines Monats zur Erteilung der Auskünfte	Eine Frist für die Erteilung von Auskünften ist zwingend notwendig, ansonsten keine Wirksamkeit für die Auskunftserteilung besteht bzw. die Auskunft irgendwann erteilt werden kann.
Art. 30a Abs. 3 und Art. 48d Abs. 4	Der Bundesrat konkretisiert insbesondere die Voraussetzungen der Erforderlichkeit und Verhältnismässigkeit, die Datenminimierung und Zweckbindung, die Zugriffsberechtigungen, die Protokollierung, die Aufbewahrungs- und Löschfristen sowie periodische Kontrollen. Die Aufsichtsbefugnisse des EDÖB bleiben vorbehalten.	Art. 6, 7, 22 und 23 DSG sowie die Aufsicht des EDÖB nach Art. 4 und 49 ff. DSG gelten bereits. Die Erläuterungen zu beiden Bestimmungen bezeichnen die Bearbeitung besonders schützenswerter Personendaten als erforderlichen Ausnahmefall. Wegen des Profilings und der möglichen verdeckten Bearbeitung biometrischer Daten sind die zentralen Schutzvorgaben dennoch ausdrücklich zu operationalisieren; eine zusätzliche Aufsichtsbehörde neben dem EDÖB ist nicht erforderlich.
Art. 48a Abs. 4 Bst. d	Die Meldepflichten und Meldewege für Störungen und Cyberangriffe sind auf Verordnungsstufe mit Art. 96 FDV sowie den Art. 74d und 74e ISG und der Cybersicherheitsverordnung zu harmonisieren. Mehrfachmeldungen sind durch eine Weiterleitung zwischen den zuständigen Bundesstellen zu vermeiden.	Eine zusätzliche starre Frist im FMG ist nicht angezeigt. Störungen, die mindestens 10'000 Kundinnen und Kunden betreffen können, sind nach Art. 96 Abs. 1 FDV bereits unverzüglich der Nationalen Alarmzentrale zu melden; diese informiert das BAKOM. Meldepflichtige Cyberangriffe auf kritische Infrastrukturen sind nach den Art. 74d und 74e ISG innert 24 Stunden nach ihrer Entdeckung dem BACS zu melden; fehlende Angaben können nach der Cybersicherheitsverordnung innert 14 Tagen ergänzt werden. Entscheidend ist daher die Koordination der bestehenden Pflichten, nicht eine zusätzliche parallele 24- oder 72-Stunden-Frist an das BAKOM.
Art. 59 Abs. 2	Einfügen einer konkreten wiederkehrenden Frist zur Rückmeldung (z.B. halbjährlich / jährlich, zu Beginn eines Quartals, innert eines Monats)	Der verwendete Begriff der «Regelmässigkeit» ist unspezifisch bzw. nicht konkret genug. Unserer Kenntnis zur Folge fehlen dem BAKOM aber auch dem Dienst ÜPF teilweise die Rückmeldungen der Provider, wem Nummernblöcke vergeben wurden (so müssen Nummernblöcke stand Heute nur einmal jährlich zurückgemeldet werden). Die Bundesbehörden müssten bei den Providern nachhaken, weshalb die Liste diesbezüglich nicht immer aktuell sei, auch wenn diese jährlich aktualisiert werden sollte.


Stellungnahme zum Fragebogen zur Vernehmlassungsvorlage

Frage	Antwort	Begründung / Bemerkungen
1	Ein Mitbenutzungsrecht wird begrüsst, sofern der physische Zutritt zu den gemeinsam genutzten Infrastrukturen verbindlich und sektorenübergreifend geregelt wird.	KI, Cloud Computing und ähnliche, in Zukunft stark wachsende Technologien, sind äusserst datenintensiv und erfordern schnelle und zuverlässige Verbindungen und eine möglichst lückenlose Abdeckung. Dazu muss das Netz grossflächig ausgebaut werden. Durch ein gegenseitiges Mitbenutzungsrecht bestehender Infrastrukturen können Synergien genutzt und entsprechend Ressourcen optimal eingesetzt werden. Gerade bei öffentlichen Bauprojekten dürften grosse Synergiepotentiale durch eine gemeinsame Infrastrukturnutzung vorhanden sein. Ein Mitbenutzungsrecht dürfte auch schnellere oder wegfallende Genehmigungsverfahren zur Folge haben. Voraussetzung sind klare Regeln zum physischen Zutrittsschutz, namentlich zu Berechtigungs- und Schlüsselmanagement, Zutrittsprotokollierung, Begleitung, Notfallzugang, Schutz- und Trennkzepten sowie Haftung. Die Mitbenutzung darf die Sicherheit und Integrität der mitbenutzten Fernmelde-, Strom- oder Wasserinfrastruktur nicht beeinträchtigen.
2	Ein gegenseitiges Mitbenutzungsrecht wird begrüsst, sofern der physische Zutritt zu den gemeinsam genutzten Infrastrukturen verbindlich und sektorenübergreifend geregelt wird.	Versorgungsbetriebe sollten ebenfalls das Recht erhalten, die passive Infrastruktur der Fernmeldeanbieterinnen zu benutzen. Insbesondere, wenn sie ihrerseits Kommunikationsnetze (aus)bauen bzw. nutzen wollen. Beispielsweise wenn ein Versorgungsbetrieb Kommunikationsleitungen für den Betrieb intelligenter Stromnetze, sogenannter Smart Grids, verlegen muss. Ein gegenseitiges Mitbenutzungsrecht dürfte auch von Vorteil sein, weil beispielsweise lokale Elektrizitätswerke oftmals selbst als Telekommunikationsanbieterinnen auftreten und bspw. ein regionales Glasfasernetz bauen oder betreiben. Diese Anforderungen müssen spiegelbildlich auch gelten, wenn Versorgungsbetriebe passive Infrastrukturen von Fernmeldeanbieterinnen mitbenutzen. Der Zugang ist mit geeigneten Auflagen zu versehen oder zu verweigern, wenn andernfalls die physische Sicherheit oder Integrität einer kritischen Infrastruktur beeinträchtigt würde.