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

Per E-Mail an:
tp-secretariat@bakom.admin.ch

Bern, 17. September 2026

Stellungnahme zur Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit

Sehr geehrter Herr Bundesrat,
sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 27. Mai 2026 eröffnete Vernehmlassung zur «Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit» und danken Ihnen für die Einladung zur Stellungnahme. Der Schweizerische Verband der Telekommunikation (asut) vertritt die Interessen der Telekommunikations-, Netzwerk- und Datacenterbranche in der Schweiz. Gemeinsam mit unseren Mitgliedern treiben wir optimale Rahmenbedingungen für erstklassige Kommunikations-, Netzwerk- und Dateninfrastrukturen voran und tragen damit zu einem erfolgreichen und wettbewerbsfähigen digitalen Wirtschaftsstandort Schweiz bei. Die Telekommunikationsbranche ist direkt von der Teilrevision des FMG betroffen und gerne übermitteln wir Ihnen hiermit fristgerecht unsere Einschätzung dazu.

Einleitende Bemerkungen

Der sichere Betrieb der Telekommunikationsinfrastrukturen, sichere Fernmeldedienste sowie die Bekämpfung von Cyberbedrohungen gehören seit Jahren zu den Kernaufgaben der Fernmeldedienstanbieterinnen. Diese Sicherheitstradition geht auf das Fernmeldegeheimnis zurück, welches bereits 1874 – damals noch als Telegrafengeheimnis – in der Bundesverfassung verankert wurde. Die grosse Bedeutung der Kommunikationstechnologien für die Schweiz sowie die zunehmenden Cyberbedrohungen stellen weiterhin grosse Anforderungen an die Fernmeldedienstanbieterinnen. Wir teilen daher die Ansicht des Bundesrates, dass die Sicherheit der Kommunikationstechnologien an Bedeutung zugenommen hat.

Im Whitepaper «Mobilfunksicherheit in der Schweiz – eine Übersicht»[1] hat asut detailliert aufgezeigt, welche Massnahmen, Prozesse und organisatorischen Vorkehrungen die drei privaten Mobilfunknetzbetreiberinnen bereits ergriffen haben, um die Sicherheit der Fernmeldeinfrastrukturen und Fernmeldedienste zu gewährleisten. Zentrale Erfolgsfaktoren sind firmeninterne Sicherheitsorganisationen, Einführung und Betrieb von etablierten Managementsystemen sowie die Orientierung an international anerkannten Normen und Standards. All diese Massnahmen umfassen nicht nur den Betrieb der eigenen Infrastruktur, sondern immer auch die Lieferkette. Die heute geltenden Vorschriften in der Verordnung über Fernmeldedienste (FDV) Art. 96a-g tragen dieser Sicherheitskultur im Fernmeldewesen Rechnung.

[1] https://asut.ch/asut/media/id/3591/type/document/asut-Whitepaper+Mobilfunk-Cybersicherheit+in+der+Schweiz.pdf

asut
Schweizerischer Verband der Telekommunikation
Hirschengraben 8
3011 Bern

+41 (0)31 560 66 66
info@asut.ch
www.asut.ch

Die vorliegende Revision des FMG hingegen enthält eine Vielzahl von neuen zusätzlichen staatlichen Eingriffen, ohne dass im Detail aufgezeigt wird, welche Schutzlücken bestehen und ob bzw. wo die heute angewendeten Massnahmen und Prozesse bei den Fernmeldedienstanbieterinnen hinsichtlich Cybersicherheit ungenügend sind. Zusätzlich wird die konkrete Ausgestaltung der neuen Regelungen in vielen Punkten an den Bundesrat bzw. das BAKOM delegiert, so dass der Umfang der Regulierung und insbesondere deren Auswirkungen teilweise offenbleiben. Fehlende Schutzziele und unbestimmte Massnahmen stehen im Widerspruch zur Rechtssicherheit und zur Investitionssicherheit, welche für den Aufbau und Betrieb der Fernmeldeinfrastrukturen zwingend notwendig sind.

Fernmeldeinfrastrukturen sind komplexe technische Systeme, die von den Netzbetreiberinnen individuell geplant und betrieben werden. Die notwendige Hardware und Software werden dazu von unterschiedlichen Lieferantinnen beschafft und betrieben. Diese Infrastrukturen sind nicht «ab der Stange» und Cybersicherheit ist kein «Feature», das man dazukaufen und einschalten kann. Cybersicherheit wird vielmehr durch die Fernmeldedienstanbieterin im Betrieb «produziert». Durch die Anwendung internationaler Normen, durch spezialisierte Cyber-Fachkräfte, durch effektive Management-Systeme und durch entsprechende interne Organisationen.

Aus Sicht der Telekommunikationsbranche liegt die Verantwortung für die Cybersicherheit der Fernmeldeinfrastrukturen und der Fernmeldedienste in erster Linie bei den Unternehmen. Die rechtlichen Vorgaben und damit die vorliegende Teilrevision FMG sollen sich daher auf die notwendigen Rahmenbedingungen beschränken und Eingriffe des Staates sollen nur subsidiär erfolgen. Die Regulierung soll in jedem Fall verhältnismässig, risikobasiert, technologie- und unternehmensneutral, subsidiär sowie rechtssicher ausgestaltet sein.

Angesichts der grossen Tragweite der Teilrevision auf den Betrieb der Fernmeldeinfrastrukturen und die Investitionen in die Netze sollen die Auswirkungen der vorgeschlagenen Regulierung und Eingriffe in einer Regulierungsfolgeabschätzung untersucht und deren Folgen aufgezeigt werden.

Detaillierte Einschätzung zu den Änderungen im FMG

1. Zweck (Art. 1 Abs. 1 sowie 2 Bst. b und f)

Die Teilrevision FMG umfasst mehrheitlich Sicherheitsaspekte der Fernmeldeinfrastrukturen und der Fernmeldedienste. Dies soll auch im Zweckartikel deutlich gemacht werden. Zusätzlich wird jedoch in Art. 1 Abs. 2 Bst. f festgehalten, dass mit dem FMG neu auch die Resilienz der Fernmeldeinfrastrukturen gewährleistet werden soll. Resilienz geht jedoch weit über das vorliegende Revisionspaket hinaus. So stellten sich beispielsweise während der Corona-Pandemie ganz andere Fragen zur Resilienz als während eines Stromausfalls oder einer Cyberbedrohung.

Änderungsantrag zu Art. 1 Abs. 2 Bst. f
f. die Sicherheit ~~und Resilienz~~ von Fernmeldeinfrastrukturen gewährleisten.

2. Rechte und Pflichten von Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen oder Kabelkanalisationen (Art. 3a)

Mit Art. 3a werden Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen sowie Eigentümerinnen von Kabelkanalisationen gewissen Pflichten und Rechten des FMG unterstellt. Heute gelten diese Rechte und Pflichten nur für Anbieterinnen von Fernmeldediensten. Mit der Anpassung von Art. 3a werden vergleichbare Rahmenbedingungen für alle Akteure geschaffen. Dies ist grundsätzlich zu begrüssen. Unklar ist jedoch, wieso bei den Kabelkanalisationen nur die Eigentümerin verpflichtet wird.

3. Sperrung des Zugangs zu Telefonie und Internet (Art. 6a)

In Art. 6a wird geregelt, in welchen Fällen (z.B. fiktive oder falsche Identität, falsche Dokumente) der Zugang zu Telefonie und Internet gesperrt werden muss. Neu soll diese Pflicht nicht nur für Prepaid-Angebote, sondern auch für Abonnementsverhältnisse gelten. Offen bleibt jedoch, ob damit eine

Pflicht für die Fernmeldedienstanbieterinnen besteht, die Kundendaten zu überprüfen oder ob die zuständigen Behörden die Fernmeldedienstanbieterinnen darauf hinweisen werden (analog Art. 6b).

Dies ist insbesondere in Bezug auf Art. 6a Abs. 2 von grosser Bedeutung. Auf eine Sperrung soll verzichtet werden, wenn ein Zugang zu Telefonie oder Internet Gegenstand eines Überwachungsauftrages des Dienstes Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) ist. Verantwortlich dafür ist die zuständige Behörde, die sicherstellen muss, dass in solchen Fällen auf eine Sperrung verzichtet wird. Dies lässt den Schluss zu, dass Sperrungen von einer «zuständigen Behörde» ausgehen. Offen ist jedoch, welche Behörden dies genau sind.

In der Praxis zeigt sich zudem, dass sich nach einer erfolgten Sperre die betroffenen Kundinnen oder Kunden oder der Dienst ÜPF regelmässig an die Fernmeldedienstanbieterin wenden mit der Anfrage nach den Gründen für die Sperrung. Dies weiss in der Regel jedoch nur die anordnende Behörde und nicht die Fernmeldedienstanbieterin.

Antrag zu Art. 6a
Die Verantwortlichkeiten der zuständigen Behörden und die Abläufe betreffen Aufforderung zur Sperrung sowie Abklärungen, um auf eine Sperre zu verzichten, müssen klar und eindeutig geregelt werden.

4. Sperrung von Telefonnummern und Domain-Namen (Art. 6b)

Neu sollen auch Telefonnummern und Domain-Namen zweiter Ebene blockiert werden können, wenn ein begründeter Verdacht auf mutmasslichen Betrug nach Art. 146 Strafgesetzbuch besteht. Durch eine rasche Blockierung für fünf Tage (die durch Staatsanwaltschaften oder Gerichte verlängert werden kann) sollen Kundinnen und Kunden vor Betrug geschützt werden.

Betrug und weitere Vergehen oder Verbrechen unter Verwendung von Telefon- und Internetdiensten sind für Fernmeldedienstanbieterinnen und deren Kundinnen und Kunden ein zunehmendes Problem. Die Branche hat daher beispielsweise im Bereich der Spoofing-Anrufe aus dem Ausland freiwillig Abwehrmassnahmen entwickelt, welche dieses Jahr vom BAKOM im Rahmen einer Technischen und Administrativen Vorschrift (TAV) verpflichtend eingeführt wurden.

Die Branche stellt sich daher nicht grundsätzlich gegen eine Ausweitung der Blockierungspflicht bei Domain-Namen. Die Sperrung von Telefonnummern und die Blockierung von Domain-Namen muss jedoch von der zuständigen Behörde, d.h. dem Fedpol, zwingend angeordnet werden, nachdem das Fedpol den begründeten Verdacht abgeklärt hat. Ein Hinweis allein reicht nicht aus, und es ist auch nicht die Aufgabe einer Fernmeldedienstanbieterin oder einer Registerbetreiberin abzuklären, ob ein Verdacht vorliegt und ob dieser ausreichend begründet ist.

Im Parlament ist gegenwärtig die Motion «Es braucht griffige Massnahmen gegen die missbräuchliche Verwendung von schweizerischen Domains!» (24.4393) von Nationalrat Michael Götte in Beratung, wobei beide Räte bereits den Bestimmungen zur Blockierung von Domain-Namen zugestimmt haben. Die Motion sieht vor, dass die Blockierung nicht nur bei Betrug zur Anwendung kommt, sondern beispielsweise bei allen Vergehen und Verbrechenstatbeständen sowie Versuchen dazu. Sollte die Motion überwiesen werden, dann würden die Blockierungstatbestände deutlich ausgeweitet werden (z.B. Persönlichkeitsrechte, Verletzung der Privatsphäre, Urheberrechte etc.).

Neben einer zwingenden Anordnung durch die Behörde sollen auch die Verfahren und die Information der Betroffenen vertieft geklärt werden. Damit soll verhindert werden, dass falsche Domains blockiert werden und dass sich betroffene Personen oder Unternehmen rasch gegen eine – allenfalls ungerechtfertigte – Blockierung wehren können. Dies gilt insbesondere hinsichtlich allfälliger zusätzlicher Tatbestände (z.B. aufgrund Motion Götte).

Abschliessend schlagen wir eine begriffliche Klärung vor. In Art. 6b geht es um eine Blockierung oder Deaktivierung von Domain-Namen und nicht um eine Internetsperre, wie sie beispielsweise im Gesetz über Geldspiele vorgesehen ist. Es soll daher konsequent der Begriff «Blockierung» bzw. «blockieren» verwendet werden.

Antrag zu Art. 6b
Angesichts der offenen politischen Debatte im Parlament zur Motion Götte beantragen wir vorerst nur formale und prozedurale Anpassungen in Art. 6b. Insbesondere soll in Bezug auf die Domain-Namen (im Titel und in Abs. 2) konsequent der Begriff Blockierung verwendet werden. Zudem sollen – allenfalls in Rücksprache mit der zuständigen Registry – Schnittstellen, Abläufe und die Information der betroffenen Personen und Unternehmen praxistauglich geregelt werden.

5. Grundsätze (Art. 20)

Die Telekommunikationsbranche und insbesondere die Anbieterinnen öffentlicher Telefoniedienste engagieren sich bereits heute gemeinsam mit den kantonalen Notrufzentralen (PSAP) sowie dem zuständigen Bundesamt BAKOM für eine funktionierende Notkommunikation sowie für deren laufende Verbesserung. In der Kommunikationskette von den Benutzerinnen und Benutzern bis zu den Mitarbeitenden in den Notrufzentralen sind die Fernmeldedienstanbieterinnen jedoch nur für einen Teil der Kommunikation zuständig und verantwortlich. Die End-to-End-Kommunikation hängt daher von allen Beteiligten ab und aus technischen Gründen gilt im Mobilfunk das Best-Effort-Prinzip. Eine hundertprozentige Gewähr, dass eine Notkommunikation immer möglich ist, gibt es daher nicht. Art. 20 Abs. 1 soll entsprechend angepasst werden.

Dies gilt auch in Art. 20 Abs. 2 hinsichtlich der Redundanz. Bereits heute werden PSAP durch einen Zweitanbieter erschlossen, womit die «minimale Rückfallebene» bereits sichergestellt ist. Art. 20 Abs. 2 soll entsprechend angepasst werden, um Missverständnisse hinsichtlich einer weitergehenden Redundanz zu vermeiden.

Änderungsantrag zu Art. 20 Abs. 1 und 2
[1] Die Anbieterinnen des öffentlichen Telefondienstes müssen ~~sicherstellen, dass~~ die Kommunikation zwischen den Benutzerinnen und Benutzern und den von den Notdiensten sowie den Hilfs- und Beratungsdiensten betriebenen Zentralen (Notkommunikation) ~~jederzeit möglich ist~~ ermöglichen.
[2] Sie müssen dazu insbesondere die Leitweglenkung, die Standortidentifikation und ~~die Redundanz (~~eine minimale Rückfallebene~~)~~ sicherstellen.

6. Systemaufgaben (Art. 20a)

Gemäss erläuterndem Bericht geht es in Art. 20a nicht um die Notkommunikation der Bevölkerung zu den Notrufzentralen, sondern um ein spezielles IP-Netz (ESInet), das der Kommunikation zwischen den Notrufzentralen und PSAP dient und erweiterte Funktionen wie Bild-, Video- und Textkommunikation erlaubt. Hinsichtlich Ausfallsicherheit führt der Bundesrat im erläuternden Bericht aus, dass mit dem ESInet kein autonomes Netz geplant ist. Damit ist es auch nicht notwendig, ein Netz zu betreiben, welches ausschliesslich dieser Funktion dient. Insbesondere, da ein zusätzliches Netz die Komplexität und Fehleranfälligkeit erhöht.

Art. 20a Abs. 1 Bst. b verlangt den redundanten Betrieb des ganzen Netzes. Wenn jedoch dieselben Adressierungselemente gleichzeitig in zwei (redundanten) Netzen aktiv sind, kann diese zu Störungen und Fehlern führen. Daher sieht der zugrundeliegende ETSI-Standard vor, dass die Redundanz jeweils nur innerhalb eines ESInet sichergestellt wird. Dies soll in Bst. b entsprechend angepasst werden.

End-to-End-Test gehören nach Art. 20a Abs. 1 Bst. e ebenfalls zu den Systemaufgaben. Da mit dem Begriff Plattform in der Regel ein konkretes Software-Produkt verstanden wird, soll in Bst. e von Test- und Integrationsumgebung gesprochen werden. Zudem erfordert ein End-to-End-Test auch eine entsprechende Testumgebung bei den Notrufzentralen. Der konkrete Testumfang muss daher in der TAV gemäss Art. 20a Abs. 3 durch das BAKOM definiert werden.

Änderungsantrag Art. 20a Abs. 1 Bst. b und c
[1] Die Notkommunikation muss mit den folgenden übergeordneten Aufgaben (Systemaufgaben) durch eine oder mehrere Anbieterinnen sichergestellt werden:
~~a. Betrieb eines ausschliesslich der Notkommunikation dienenden, jederzeit verfügbaren Netzes;~~
~~b. redundanter~~ Betrieb des gesamten, in sich redundanten Netzes ~~nach Buchstabe a~~ oder von Teilen davon durch eine Zweitanbieterin;
[…]
e. Betrieb einer Test- und Integrationsumgebung ~~plattform~~, die End-zu-End-Tests ermöglicht;

7. Verpflichtung zum Angebot von Systemaufgaben (Art. 20b)

Die Verpflichtung zum Angebot der Systemaufgaben erscheint konzeptionell noch nicht ausreichend ausgearbeitet. Entweder sind die Systemaufgaben, unabhängig davon, ob bereits eine oder mehrere Systemaufgaben freiwillig erbracht werden, zwingend und jederzeit zu erfüllen. Dann müsste die Verpflichtung immer gelten und könnte vergleichbar zur Grundversorgungsverpflichtung ausgestaltet werden. Sollten hingegen die Systemaufgaben möglichst auf freiwilliger Basis erbracht werden und eine Verpflichtung nur subsidiär greifen, dann müsste dies deutlicher formuliert und festgehalten werden. Sollte ein Ausschreibung- oder Einladungsverfahren zur Anwendung kommen, dann sind die entsprechenden Verfahrensdauern bei der Planung zu berücksichtigen. Der Verzicht auf eine Ausschreibung oder Einladung wegen Dringlichkeit ist dann nicht notwendig.

Antrag zu Art. 20b
Art. 20b soll dahingehend präzisiert werden, ob die Systemaufgaben in erster Linie auf freiwilliger Basis durch die Fernmeldedienstanbieterinnen erbracht werden sollen (Verpflichtung greift nur subsidiär) oder ob eine zwingende Verpflichtung analog der Grundversorgungspflicht beabsichtigt ist.

Änderungsantrag Art. 20b Abs. 3 Bst. a
[1] Das BAKOM kann eine Anbieterin ohne Ausschreibungs- oder Einladungsverfahren bestimmen, wenn eine der folgenden Voraussetzungen erfüllt ist:
~~a. Es kann wegen zeitlicher Dringlichkeit kein Ausschreibungs- oder Einladungsverfahren durchgeführt werden;~~

8. Kostentragung (Art. 20c)

Sollte gemäss Art. 20b eine oder mehrere Anbieterinnen zur Erfüllung der Systemaufgaben verpflichtet werden, dann müssten die Kosten auf sachgerechte, transparente und nicht-diskriminierende Weise auf alle Fernmeldedienstanbieterinnen verteilt werden, deren Kundinnen und Kunden die Notkommunikation auch Nutzen können. Bei der Kostenentschädigung der verpflichteten Anbieterin sind nicht nur die Betriebskosten zu berücksichtigen, sondern insbesondere auch die Vorhalte- und Investitionskosten. Beispielsweise, wenn eine Zweitanbieterin nur die Redundanz sicherstellt und entsprechende Investitionen tätigt, deren Systeme jedoch gar nicht zum Einsatz kommen.

Änderungsantrag zu Art. 20c
[3] Werden gemäss Artikel 20b Absatz 1 mehrere Anbieterinnen mit derselben Systemaufgabe beauftragt, regelt der Bundesrat die Entschädigung so, dass die Anbieterinnen angemessen und diskriminierungsfrei entschädigt werden.

9. End-zu-End-Tests (Art. 20d)

Art. 20d soll gemäss den Ausführungen und Anträgen zu Art. 20a angepasst werden

Antrag zu Art. 20d
Anpassung gemäss Anträgen zu Art. 20a.

10. Schutz der Integrität der Notkommunikation (Art. 20e)

Für die Benutzerinnen und Benutzer ist es wichtig, dass sie jederzeit Zugang zu den Notdiensten haben. Eine Trennung vom Netz zum Schutz der Integrität der Notkommunikation kann daher

einschneidende Folgen für die betroffenen Benutzerinnen und Benutzer haben. Zudem soll berücksichtigt werden, dass eine Störung auch von einem Endgerät ausgehen kann. Der Entscheid, welche Massnahmen getroffen werden müssen und ob Benutzerinnen und Benutzer vom Netz getrennt werden sollen, muss von den von den Notdiensten sowie den Hilfs- und Beratungsdiensten betriebenen Zentralen getroffen werden. Verantwortlich für die Umsetzung einer Massnahme ist dann nur diejenige Fernmeldedienstanbieterin, aus deren Netz eine Störung stammt.

Änderungsantrag zu Art. 20e
[1] Die zur Notkommunikation verpflichteten Anbieterinnen von Fernmeldediensten und die Herstellerinnen von Fernmeldeanlagen ergreifen im Rahmen ihres jeweiligen Einflussbereiches Massnahmen zum Schutz der Integrität der Notkommunikation.
[2] Sie stützen sich dabei ~~insbesondere~~ auf die Hinweise der von den Notdiensten sowie den Hilfs- und Beratungsdiensten betriebenen Zentralen und koordinieren ihre Massnahmen über die ~~der~~ Koordinationsstelle nach Artikel 20a Buchstabe d. Die Anbieterinnen ergreifen die Massnahmen umgehend ~~und so lange wie nötig~~.

11. Lokalisierung von Störungen (Art. 34a)

Grundsätzlich anerkennt die Branche die Absicht des Bundesrates, Störungen des Fernmeldeverkehrs oder Rundfunks zu verhindern. Um den Ursprung einer Störung zu identifizieren, sollen Anbieterinnen, Eigentümerinnen oder Betreiberinnen von Fernmeldeanlagen dem BAKOM auf Verlangen alle relevanten Informationen im massgeblichen Zeitraum zur Verfügung stellen. Dazu gehören insbesondere Abstrahlungseigenschaften und -einstellungen von Antennen. Gemäss erläuterndem Bericht betrifft dies auch moderne Mobilfunkantennen mit Beamforming-Fähigkeiten. Die einzelnen Beams werden jedoch von den intelligenten Antennen automatisiert gesteuert und wechseln im Millisekunden-Takt. Je nach Systemlieferantin und Frequenzband werden diese Daten gar nicht gespeichert und selbst wenn sie vorhanden wären, würden dadurch enorme Datenmengen generiert werden. Daher ist diese Pflicht für Mobilfunkantennen mit Beamforming-Fähigkeit gegenwärtig nicht erfüllbar. Für die Abklärung, ob eine Mobilfunkantenne Ursache einer Störung ist, kann das BAKOM jedoch auf die vorhandenen Daten in der BAKOM-Antennendatenbank zurückgreifen und die entsprechenden Antennendiagramme und Sendeparameter verwenden.

Antrag zur Art. 34a
Moderne Mobilfunkantennen mit Beamforming-Funktionalität sollen von Art. 34a Abs. 1 ausgenommen werden.

12. Kinder- und Jugendschutz (Art. 46a)

2008 wurde die asut Brancheninitiative zum Jugendmedienschutz eingeführt, welche zahlreiche freiwillige Massnahmen zum Jugendschutz sowie zur Förderung der Medienkompetenz enthielt und laufend weiterentwickelt wurde. asut ist zudem Gründungsmitglied der Branchenorganisation zur Umsetzung der Jugendschutzmassnahmen nach dem Gesetz über den Jugendschutz in den Bereichen Film und Videospiele. Einige der Massnahmen aus der Brancheninitiative wurden zwischenzeitlich ins FMG sowie in die FDV überführt. Der Bundesrat möchte nun in Art. 46a zusätzlich die Pflicht einführen, dass Internetzugangsanbieterinnen Mittel bieten, um Kinder und Jugendliche wirksam vor pornografischen Inhalten zu schützen.

Die Verantwortung für den Schutz der Kinder und Jugendlichen liegt letztlich bei den Eltern oder Erziehungsberechtigten, die den Kindern und Jugendlichen die Endgeräte zur Nutzung des Internets zur Verfügung stellen und auch die Jugendschutzeinstellungen konfigurieren. Zudem können Schutzmassnahmen durch die Nutzung von VPN-Software etc. umgangen werden. Der wirksame Schutz vor pornografischen Inhalten kann also nicht garantiert werden und liegt letztlich auch nicht in der Verantwortung der Anbieterin des Internetzugangs.

Änderungsantrag zu Art. 46a
[1] Die Anbieterinnen von Internetzugängen müssen ihre Kundinnen und Kunden über die Möglichkeiten im Bereich des Kinder- und Jugendschutzes beraten und ihnen Mittel bieten, mit denen sie ihre Kinder und Jugendlichen ~~wirksam~~ vor pornografischen Inhalten ~~geschützt werden~~ schützen können.

13. Resilienz der Fernmeldeinfrastrukturen und Schutz vor Cyberbedrohungen (Art. 48a)

Mit Art. 48a verpflichtet der Bundesrat die Anbieterinnen von Fernmeldediensten, Manipulationen von Fernmeldeinfrastrukturen zu bekämpfen und vor Cyberbedrohungen zu schützen. Dazu gehört auch die Resilienz bei Cyberbedrohungen. Weitere Pflichten hinsichtlich Resilienz sind nicht aufgeführt und diese würden auch weit über das Themenfeld Cybersicherheit hinausgehen (z.B. Pandemie, Stromausfall). Daher soll der Titel von Art. 48a entsprechend präzisiert werden.

Änderungsantrag zu Art. 48a
Art. 48a ~~Resilienz der Fernmeldeinfrastrukturen und~~ Schutz der Fernmeldeinfrastrukturen vor Cyberbedrohungen

Die im asut Whitepaper «Mobilfunk-Cybersicherheit in der Schweiz – eine Übersicht» aufgezeigten Massnahmen zur Stärkung der Cybersicherheit und Bekämpfung von Cyberbedrohungen sind weitgehend vereinbar mit den Vorgaben in Art. 48a Abs. 1. Aus Sicht der Branche ist es zwingend, dass sich die geforderten technischen, operativen und administrativen Massnahmen an den internationalen Normen, Standards und Best-Practices orientieren sowie dem Stand der Technik entsprechen. Ziel ist kein absoluter Schutz, sondern die Massnahmen sollen verhältnismässig und den jeweiligen Risiken entsprechend sein. Bei der weiteren Konkretisierung von Art. 48a in einer Verordnung soll ein branchenweites kohärentes Mindestsicherheits-Niveau im Sinne von Minimalstandards erreicht werden.

Änderungsantrag zu Art. 48a Abs. 1
[1] Die Anbieterinnen von Fernmeldediensten müssen dem Risiko angemessene technische, operative und administrative Massnahmen ergreifen […]

Die Fernmeldedienstanbieterinnen arbeiten im Bereich der Cybersicherheit seit Jahren eng mit den zuständigen Bundesbehörden wie dem BACS, dem BAKOM oder dem BWL zusammen. Vorgaben und Pflichten hinsichtlich des Schutzes vor Cyberbedrohungen sind zudem in verschiedenen Gesetzen festgehalten (z.B. FMG, ISG, DSG). Die in Art. 48a Abs. 2 festgehaltene Aufgabe des BAKOM, Risikofaktoren zu ermitteln, zu überwachen und zu bewerten soll daher in Koordination mit anderen Bundesstellen erfolgen, um Doppelspurigkeiten und Missverständnisse zu vermeiden. Bei der Festlegung der Risikofaktoren soll zudem auf internationale Normen, Standards und Best-Practices abgestellt werden. Damit wird verhindert, dass eine Schweizer Risikobewertung nicht mit den globalen technischen Standards vereinbar ist (Swiss-Finish).

Antrag zu Art. 48a Abs. 2
Bei der Ausgestaltung der Risikofaktoren soll auf internationale Normen, Standards und Best-Practices abgestellt werden. Zudem soll die Koordination zwischen den Bundesbehörden sichergestellt werden, um Doppelspurigkeiten zu verhindern.

Die Branche begrüsst die Möglichkeit zur Zusammenarbeit innerhalb der Branche sowie mit weiteren privaten und öffentlichen Stellen nach Art. 48a Abs. 3. Zu prüfen wäre dabei auch der Einbezug der Lieferantinnen, da diese auf breite internationale Erfahrungen zurückgreifen können. Konsequenterweise stellt sich aber die Frage, ob nicht auch die Risikobewertung gemäss Art. 48a Abs. 2 im Rahmen dieser freiwilligen Kooperationen möglich wäre. So wurden im Rahmen der Nationalen Cyberstrategie (NCS) verschiedene sektorspezifische «Cyber-Security-Center» ins Leben gerufen (z.B. Finance, Health, Rail). Es sollte daher die Möglichkeit offengelassen werden, dass sich auch die Fernmeldebranche im Rahmen eines CSC selbst organisiert. Dieser subsidiäre Ansatz würde auch der Tatsache Rechnung tragen, dass das notwendige Cyber-Know-how im Fernmeldebereich weitgehend bei den Anbieterinnen von Fernmeldediensten liegt.

Antrag zu Art. 48a Abs. 2 und 3
Es soll geprüft werden, ob und inwieweit die Risikobeurteilung hinsichtlich der Cybersicherheit von der Fernmeldebranche selbst umgesetzt werden soll und wie dabei gleichzeitig die Aufsicht durch den Bund sichergestellt werden kann.

Welche Massnahmen die Fernmeldedienstanbieterinnen konkret gemäss Bundesrat umsetzen müssen, ist in Art. 48a Abs. 4 nicht konkret geregelt. Vielmehr erhält der Bundesrat weitreichende Befugnisse, diese Verpflichtungen nachträglich zu erlassen oder zu ändern. Diese umfassende Delegationsnorm beurteilt die Branche als sehr kritisch, weil Infrastrukturen in der Regel hohe Investitionen erfordern und auf einen längeren Zeithorizont geplant werden. Nachträgliche Änderungen der

Spielregeln schwächen die Rechtssicherheit und hemmen notwendige Investitionen. In einem früheren Rechtsgutachten im Auftrag der asut hatte Prof. Häner[2] in einer vergleichbaren Fragestellung festgestellt, dass eine solche Delegation nicht verfassungskonform ist. Daher sollen die Eckpunkte der Delegationsnorm im Gesetz verankert werden.

Änderungsantrag zu Art. 48a Abs. 4
[4] Der Bundesrat präzisiert die Massnahmen nach Absatz 1, wobei er sich an international anerkannten Standards orientiert und speziell die technische Umsetzbarkeit, die betrieblichen Auswirkungen, die Realisierbarkeit sowie die wirtschaftliche Tragbarkeit der damit verbundenen Kosten berücksichtigt. Er kann […]

14. Sicherheit von Fernmeldeinfrastrukturen (Art. 48b)

Die Fernmeldedienstanbieterinnen blicken auf eine langjährige Sicherheitskultur zurück und setzen eine Vielzahl von Massnahmen um, um die Cybersicherheit der Infrastrukturen und der Dienste sicherzustellen. Zentrale Element dieser Sicherheitskultur sind innerbetriebliche Sicherheits-Organisationen, welche anhand bewährter Management-Systeme unter Anwendung etablierter internationaler Normen und Standards die Cybersicherheit gewährleisten. In Art. 48b Abs. 1 fordert nun der Bundesrat, dass nur Fernmeldeinfrastrukturen verwendet werden, welche die Vertraulichkeit, Integrität und Verfügbarkeit von Fernmeldediensten gewährleisten. Diese Regulierung trägt der heutigen Cybersicherheitspraxis im Fernmeldebereich nicht Rechnung. Fernmeldeinfrastrukturen im Mobilfunk- und im Festnetzbereich bestehen aus unzähligen Komponenten und werden von den Netzbetreiberinnen nach eigenen Vorgaben konzipiert, konfiguriert und betrieben. Cybersicherheit entsteht nicht durch die Auswahl der Geräte, sondern in erster Linie durch die Netzbetreiberin im Betrieb unter Verwendung internationaler Standards, etablierter Frameworks oder der GSMA Knowledge Base.

In Art. 48b Abs. 2 geht der Bundesrat noch weiter und verpflichtet die Fernmeldedienstanbieterinnen zu einer Mehrlieferanten-Strategie für kritische Bestandteile der Fernmeldeinfrastruktur. asut lehnt diese Verpflichtung aus folgenden Gründen ab.

Wie bereits mehrfach festgehalten, ist ein Sicherheitsrisiko nicht eine fixe Eigenschaft eines «kritischen Bestandteils». Vielmehr liegt es an der Netzbetreiberin die verwendeten Hardware- und Software-Komponenten optimal zu konfigurieren und im Betrieb zu überwachen. So können allfällige Schwachstellen identifiziert und durch eine bessere Konfiguration oder einen Software-Patch behoben werden. Im Rahmen einer risikobasierten Analyse wird die Netzbetreiberin dabei kritische Systeme (z.B. den Core in einem Mobilfunknetz) vertiefter überwachen und managen. Die Liste der kritischen Bestandteile gemäss dem Entwurf zur «Verordnung des BAKOM über Fernmeldeanlagen (VFAV)» ist jedoch viel zu umfassend und enthält auch periphere Komponenten wie das Radio-Access-Network (RAN), das nicht zu den kritischen Bestandteilen gehört.

Die neue Mehrlieferanten-Strategie würde die Netzbetreiberinnen verpflichten, bei der Beschaffung kritischer Bestandteile mindestens zwei Lieferantinnen zu berücksichtigen, wobei mindestens eine Herstellerin ihren Sitz in einem Land mit angemessenem rechtlichem Datenschutz haben muss. Ein kausaler Zusammenhang zwischen dem gesetzlichen Datenschutz in einem Land und der Cybersicherheit in der Schweiz lässt sich jedoch nicht begründen. Vielmehr kann eine erzwungene Mehrlieferanten-Strategie auch zu weniger Sicherheit und mehr Ausfällen führen, da die technische Komplexität durch neue Schnittstellen sowie die zunehmende Anzahl verschiedener Komponenten zunimmt.

Die Einschränkung bei der Lieferantenwahl würde auch Länder wie China, Süd-Korea oder die USA betreffen, die eine wichtige Rolle bei der Entwicklung und Herstellung von Systemen und Komponenten spielen. Auch ist die Umsetzung der Mehrlieferanten-Strategie in der Praxis kaum praktikabel. Prozentsätze oder Anteile an der Infrastruktur, die jeweils von einer oder mehreren Herstellerinnen nicht überschritten werden dürfen, verkennen die Funktionsweise eines Fernmeldenetzes. So können die zentralen Systeme (z.B. Core) nicht auf zwei Lieferantinnen aufgeteilt werden und der parallele Betrieb mehrere Cores ist technisch nicht möglich.

[2] https://asut.ch/asut/media/id/3047/type/document/20240130_Rechtsgutachten_Häner_Schutz_Mobilfunknetze_vor_Stromausfällen.pdf

Dies bedeutet jedoch nicht, dass die Fernmeldeanbieterinnen heute nur von einer Lieferantin abhängig sind. Vielmehr ist es die Regel, dass jede Netzbetreiberin mit verschiedenen Lieferantinnen in unterschiedlicher Zusammensetzung zusammenarbeitet. Beispielsweise beim zentralen Core, den Transportnetzen, den peripheren Systemen (z.B. RAN) oder den Rechenzentren, in denen diverse Systeme betrieben werden. Aus einer übergeordneten Perspektive hat der Infrastrukturwettbewerb dazu geführt, dass in der Schweiz eine Vielzahl von Lieferantinnen bzw. deren Komponenten im Einsatz sind und eine Schwachstelle oder ein Ausfall nicht alle Fernmeldeinfrastrukturen oder Fernmeldedienste betreffen würde.

Änderungsantrag zu Art. 48b Abs. 2
~~[2] Die kritischen Bestandteile der Fernmeldeinfrastruktur einer Anbieterin von Fernmeldediensten müssen von verschiedenen Herstellerinnen stammen, wobei mindestens eine Herstellerin in einem Staat einen Sitz haben muss, dessen Gesetzgebung einen angemessenen Datenschutz gewährleistet. Der Bundesrat regelt die Einzelheiten; er kann Kategorien, Anteile und Mindestprozentsätze festlegen.~~

Wie bereits beschrieben, können Sicherheitsrisiken durch eine Vielzahl von Massnahmen durch die Netzbetreiberin im Betrieb vermieden oder reduziert werden. Das in Art. 48b Abs. 3 festgehaltene Verbot der Inbetriebnahme von Komponenten mit einem Sicherheitsrisiko (gemäss Art. 48a) trägt dieser Praxis nicht Rechnung. Zudem erscheint es zweifelhaft, ob und wie das BAKOM die tatsächliche Sicherheitssituation im Netzbetrieb feststellen kann. Ein Verbot, eine Ausserbetriebnahme oder Entfernung sollte deshalb nur in Betracht fallen, wenn ein konkretes Sicherheitsrisiko auf Basis internationaler Standards anhand objektiver technischer Kriterien durch die Netzbetreibern festgestellt wurde und weniger einschneidende Massnahmen – insbesondere Konfigurationsanpassungen, Software-Updates oder andere technische Risikominderungsmassnahmen – nachweislich nicht ausreichen. Zudem sollen auch die betroffenen Systemlieferantinnen angehört werden.

Änderungsantrag zu Art. 48b Abs. 3
Stellt das BAKOM gestützt auf anerkannte internationale Standards und auf objektiven, überprüfbaren Kriterien sowie evidenzbasiert ein begründetes Sicherheitsrisiko fest, so ordnet es bei Bedarf risikobasiert angemessene Massnahmen an. Es kann ~~verbietet es~~ den Anbieterinnen von Fernmeldediensten verbieten, betroffene kritische Bestandteile in Betrieb zu nehmen, wenn keine weiteren Massnahmen zur Risikominderung möglich sind. Nach Anhörung der betroffenen Fernmeldedienstanbieterinnen und der betroffenen Lieferantinnen ~~Es~~ veröffentlicht es eine Liste der verbotenen kritischen Bestandteile. Es kann die Ausserbetriebnahme oder Entfernung verbotener Bestandteile verfügen, wobei Übergangsfristen vorzusehen und die betroffenen Fernmeldedienstanbieterinnen angemessen zu entschädigen sind. ~~Bei Bestandteilen, die für die Fernmeldeüberwachung nach dem BÜPF von Belang sind, nimmt das BAKOM vorgängig Rücksprache mit dem Dienst ÜPF.~~

15. Massnahmen betreffend Fernmeldeinfrastrukturen bei geopolitischen Risiken (Art. 48c)

Neu möchte der Bundesrat mit Art. 48c die Grundlage schaffen, Erwerb, Inbetriebnahme oder den Betrieb von Bestandteilen der Fernmeldeinfrastruktur zu verbieten, wenn die Herstellerin ein geopolitisches Risiko darstellt oder sich im Besitz, unter der Kontrolle oder dem Einfluss eines ausländischen Staates befindet, der für die Schweiz ein geopolitisches Risiko darstellt. Angesichts der geopolitischen Verwerfungen der letzten Jahre ist es nachvollziehbar, dass der Bundesrat nach Instrumenten sucht, um bei geopolitischen Risiken Massnahmen ergreifen zu können.

Die vorgeschlagene Regelung wirft grundlegende Fragen hinsichtlich Verhältnismässigkeit, Rechtssicherheit und Verfahren auf. Insbesondere sind die Kriterien nach Art. 48c Abs. 2 zu wenig bestimmt und ermöglichen weitreichende Eingriffe auch ohne ein konkret festgestelltes technisches oder betriebliches Sicherheitsrisiko. Problematisch ist zudem, dass Art. 48c unabhängig von den technischen und organisatorischen Sicherheitsmassnahmen nach Art. 48a und 48b zur Anwendung kommen kann. Es ist daher zweifelhaft, ob geopolitische Risiken überhaupt Gegenstand einer sektorspezifischen Cybersicherheitsregulierung sein sollen. Insbesondere, da der Bundesrat gemäss Verfassung bereits über ausreichende Notverordnungs- und Notverfügungskompetenzen verfügt. Auf jeden Fall müsste berücksichtigt werden, dass ein erzwungener Austausch bereits installierter Komponenten erhebliche wirtschaftliche Auswirkungen und mögliche Entschädigungsfragen im Zusammenhang mit der Eigentumsgarantie mit sich bringen kann. Aus diesen Gründen lehnt asut FMG Art. 48c ab und die entsprechende Regelung soll gestrichen werden.

Änderungsantrag zu Art. 48c
~~*Art. 48c Massnahmen betreffend Fernmeldeinfrastrukturen bei geopolitischen Risiken*~~
~~*[1] Der Bundesrat kann den Anbieterinnen von Fernmeldediensten den Erwerb, die Inbetriebnahme und den Betrieb von Bestandteilen von Fernmeldeinfrastruktur verbieten, die von Herstellerinnen stammen, die für die Schweiz ein geopolitisches Risiko darstellen oder die sich im Besitz, unter der Kontrolle oder dem Einfluss eines ausländischen Staates befinden, der für die Schweiz ein geopolitisches Risiko darstellt.*~~
~~*[2] Er berücksichtigt bei der Beurteilung des geopolitischen Risikos die innere und äussere Sicherheit sowie den Schutz des Werk , Wirtschafts- und Finanzplatzes der Schweiz unter Einbezug:*~~
~~*a. der direkt oder indirekt verhängten Sanktionen gegen die Herstellerinnen nach dem Embargogesetz vom 22. März 200212;*~~
~~*b. der wirtschaftlichen, technologischen und sicherheitsbezogenen Abhängigkeiten in Bezug auf die Herstellerinnen oder die Lieferkette;*~~
~~*c. der sicherheitsrelevanten Gefährdungslage durch Cyberangriffe, Sabotage und nachrichtendienstliche Aktivitäten;*~~
~~*d. der Androhung von Sanktionen oder Embargos, die die Sicherheit oder die Wirtschaft der Schweiz beeinträchtigen würden.*~~
~~*[3] Der Bundesrat kann die Anbieterinnen von Fernmeldediensten verpflichten, Bestandteile, die von Herstellerinnen nach Absatz 1 stammen, aus ihrer Fernmeldeinfrastruktur zu entfernen. Er trägt dabei den wirtschaftlichen Auswirkungen Rechnung.*~~

16. Bearbeitung von Daten und Zusammenarbeit (Art. 48d)

Mit Art. 48d erhält das BAKOM weitreichende Kompetenzen zur Bearbeitung von allenfalls besonders schützenswerten Personendaten (z.B. biometrische Daten) sowie zur Durchführung von Profilings. Der Text in Art. 48d Abs. 1-2 sowie Abs. 4-5 ist dabei gleichlautend mit Art. 30a. Es ist jedoch unklar, wieso das BAKOM für die Aufgaben nach Art. 48a und Art. 48b überhaupt Personendaten nutzen muss. Sollten damit auch Sicherheitsrisiken durch Personen identifiziert werden können (z.B. Hacker, Saboteure etc.), dann würde dies vermutlich nicht im Hoheitsbereich des BAKOM liegen, sondern des Nachrichtendienstes oder der Strafverfolgungsbehörden. Es soll daher geprüft werden, ob diese umfangreiche Kompetenz tatsächlich notwendig und zweckmässig ist.

Begrüsst wird hingegen die in Art. 48d Abs. 3 erwähnte Möglichkeit der Zusammenarbeit innerhalb der Branche sowie mit privaten und öffentlichen Stellen, um Gefährdungen durch Cyberbedrohungen festzustellen und zu beurteilen. Offen bleibt jedoch, wieso die gemeinsame Bekämpfung von Cyberbedrohungen nicht ebenfalls ermöglicht werden soll.

Antrag zu Art. 48d
Notwendigkeit und Zweckmässigkeit der umfassenden Kompetenz zur Bearbeitung von Personendaten (inkl. Profiling) soll überprüft werden.

Änderungsantrag zu Art. 48d Abs. 3
[3] Die Anbieterinnen von Fernmeldediensten können untereinander und mit für Cybersicherheit anerkannten privaten und öffentlichen Stellen nach Artikel 29 zusammenarbeiten, um Gefährdungen durch Cyberbedrohungen festzustellen, ~~und~~ zu beurteilen und zu bekämpfen.

17. Nationaler Breitbandatlas (Art. 59a)

Die jährliche Fernmeldestatistik sowie der Evaluationsbericht gemäss Art. 3b (bisher Art. 3a) sind wichtige Instrumente und Datenquellen zur Beurteilung des Schweizer Fernmeldemarktes. Dazu gehört auch der Breitbandatlas, welcher umfangreiche und detaillierte Daten zur Breitbandversorgung der Schweiz enthält. asut begrüsst, dass mit Art. 59a eine gesetzliche Grundlage für den Breitbandatlas geschaffen wird. Wichtig bei der Umsetzung ist ein breit akzeptiertes und praxisrelevantes Datenmodell. Damit kann der Breitbandatlas eine zentrale Rolle im Rahmen des Breitbandfördergesetzes spielen, zu dem der Bundesrat am 9. September 2026 die Botschaft verabschiedet hat.

Zusätzliche Revisionsvorschläge aus Sicht der Telekommunikationsbranche

18. Versorgungslücken vermeiden und Netzausbau vereinfachen

Die aufwändige Suche nach geeigneten Grundstücken sowie Liegenschaften als Mobilfunkstandorte sowie die langwierigen Bewilligungsverfahren tragen massgeblich zur langsamen Modernisierung der Mobilfunknetze bei. Dies betrifft den Neubau sowie die Modernisierung oder den Ersatz bestehender Anlagen. Mit der «Teilrevision des Fernmeldegesetzes im Bereich Mobilfunk» hat der Bundesrat bereits eine Lösung für einfachere und raschere Baubewilligungsverfahren vorgeschlagen. Die Branche begrüsst diesen Lösungsansatz und fordert den Bundesrat und anschliessend das Parlament auf, rasch die notwendigen Rahmenbedingungen für einfachere und raschere Bewilligungsverfahren zu schaffen.

Eine deutliche Lücke besteht jedoch weiterhin bei der Suche nach Mobilfunkstandorten für neue Anlagen oder Ersatzbauten. Das Postulat «Keine Versorgungslücken im Mobilfunk mehr!» (Po 23.3764), das vom Nationalrat angenommen wurde, fordert den Bundesrat auf, Massnahmen vorzuschlagen, mit denen neue oder bestehende Versorgungslücken unter Anwendung von FMG Art. 35 geschlossen werden können.

Aus Sicht der Branche bieten sich zwei Lösungsansätze dafür an. Einerseits die Inanspruchnahme von öffentlichem Grund und Boden für mobilfunkbasierte Fernmeldeanlagen. Damit würden Mobilfunkanlagen den leitungsgebundenen Anlagen gleichgestellt, was durch eine Anpassung des heutigen FMG Art. 35 einfach erreicht werden kann.

Zusätzlich besitzt die öffentliche Hand, d.h. Bund, Kantone, Gemeinden sowie öffentlich-rechtliche Anstalten, eine grosse Anzahl an Liegenschaften und Grundstücken, die sich als Mobilfunkstandort eignen könnten. Diverse Mobilfunkanlagen wurden bereits auf Grundstücken oder Liegenschaften der öffentlichen Hand erstellt. Dies bietet den Besitzern in der Regel eine Mitbestimmungsmöglichkeit bei der Standortwahl. Durch einen neuen FMG Art. 35bis soll die Nutzung dieser Liegenschaften und Grundstücke für Mobilfunkanlagen sowie die Rahmenbedingungen gesetzlich verankert werden.

Antrag zu Art. 35
Art. 35 FMG Inanspruchnahme von Grund und Boden
[1] Die Eigentümerinnen und Eigentümer von Boden im Gemeingebrauch (wie Strassen, Fusswege, öffentliche Plätze, Flüsse, Seen sowie Ufer) sind verpflichtet, den Anbieterinnen von Fernmeldediensten die Benutzung dieses Bodens für Bau und Betrieb von leitungsgebundenen oder mobilfunkbasierten Fernmeldeanlagen ~~Leitungen~~ und ~~öffentlichen Sprechstellen~~ zu bewilligen, sofern diese Einrichtungen den Gemeingebrauch nicht beeinträchtigen.
[2] Anbieterinnen von Fernmeldediensten nehmen Rücksicht auf den Zweck und die Nutzung des in Anspruch genommenen Grundstücks und tragen die Kosten für die Wiederherstellung des ursprünglichen Zustandes. Sie sind verpflichtet, ihre Fernmeldeanlagen ~~Leitungen~~ zu verlegen, wenn von der Grundeigentümerin oder vom Grundeigentümer eine Benützung des Grundstücks beabsichtigt ist, die sich mit den Fernmeldeanlagen ~~der Leitungsführung~~ nicht verträgt.
[3] Der Bundesrat regelt die Einzelheiten, namentlich die Koordinationspflicht der Anbieterinnen sowie die Voraussetzungen für die Verlegung der Fernmeldeanlagen ~~von Leitungen und öffentlichen Sprechstellen.~~
[4] Die Bewilligung ist in einem einfachen und raschen Verfahren zu erteilen. Ausser kostendeckenden Gebühren darf eine Entschädigung für die Inanspruchnahme von Grund und Boden, soweit sie den Gemeingebrauch nicht beeinträchtigt, nicht verlangt werden.

Antrag zu Art. 35bis
neu Art. 35bis Inanspruchnahme von Grundstücken und Gebäuden des Verwaltungs- und Finanzvermögens für Mobilfunk-Antennenstandorte
[1] Eigentümerinnen und Eigentümer von Grundstücken und Gebäuden im Verwaltungsvermögen sowie im Finanzvermögen sind verpflichtet, Mobilfunkkonzessionärinnen auf Anfrage geeignete Standorte für den Bau und Betrieb von mobilfunkbasierten Fernmeldeanlagen (Mobilfunkanlagen) zu fairen und angemessenen Bedingungen sowie gegen eine markt- bzw. branchenübliche Abgeltung einzuräumen.
[2] Der Bau und Betrieb der Mobilfunkanlagen darf den Zweck und die Nutzung der in Anspruch genommenen öffentlichen Sachen nicht unzulässig beeinträchtigen.
[3] Die Inanspruchnahme kann nur in Ausnahmefällen und bei Vorliegen wichtiger Gründe verweigert werden. Eine Verweigerung ist hinreichend zu begründen und muss mit objektiven Gründen gerechtfertigt werden können.
[4] Wird die Inanspruchnahme verweigert, entscheidet die ComCom auf Gesuch der Mobilfunkkonzessionärin über die Rechtmässigkeit der entsprechenden Verweigerung.

19. Rechtsgrundlage schaffen zur Verlängerung bestehender Mobilfunkkonzessionen

Am 1. September 2026 hat die ComCom über die Ausschreibung zur Vergabe der Mobilfunkfrequenzen informiert, welche 2029 frei werden. Dazu soll erneut ein Auktionsverfahren durchgeführt werden, obwohl sich die Branche für eine Verlängerung der bestehenden Konzessionen stark gemacht hat, falls keine zusätzliche Nachfrage am Markt besteht (d.h. keine zusätzliche Mobilfunknetzbetreiberin). Grundsätzlich wäre eine Verlängerung rechtlich möglich, jedoch nur zu denselben Preisen wie bei der Vergabe 2014. Da die ComCom höhere Mindestpreise ansetzen möchte, führt dies konsequenterweise zu einer aufwändigen Auktion.

Viele europäische Länder sind in einer vergleichbaren Situation, haben sich jedoch für eine Verlängerung der Konzessionen ausgesprochen. Dies schafft für die Netzbetreiberinnen Planungs- und Investitionssicherheit. Kann doch eine Auktion zu deutlich höheren Kosten führen, was zulasten der Investitionen im Netzausbau geht. Zudem besteht das Risiko, dass die Betreiber andere Frequenzen zugeschlagen bekommen als heute. Dies führt zu aufwändigen Umstellungen in den Netzen, was sich auch in Versorgungseinbussen äussern kann.

Der Bundesrat soll daher im Rahmen der vorliegenden Revision die gesetzlichen Grundlagen schaffen, damit zukünftig eine einfache Verlängerung von Mobilfunkkonzessionen möglich ist.

Wir danken Ihnen bestens für die Berücksichtigung unserer Anliegen und stehen bei Fragen gerne zur Verfügung.

asut – Schweizerischer Verband
der Telekommunikation

Judith Bellaiche
Präsidentin

Christian Grasser
Geschäftsführer