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 Erhöhung der Netzsicherheit und Schutz vor Cyberbedrohungen (Teilrevision der Verordnungen im Fernmeldebereich)

Sehr geehrter Herr Bundesrat,
sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 27. Mai 2026 eröffnete Vernehmlassung zur «Erhöhung der Netzsicherheit und Schutz vor Cyberbedrohungen (Teilrevision der Verordnungen im Fernmeldebereich)» 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 der Verordnungen betroffen und gerne übermitteln wir Ihnen hiermit fristgerecht unsere Einschätzung dazu.

Einleitende Bemerkungen

asut hat im Whitepaper «Mobilfunksicherheit in der Schweiz – eine Übersicht»[1] detailliert aufgezeigt, welche internationalen Normen, Standards und Best-Practices geeignet sind, die Cybersicherheit der Fernmeldeinfrastrukturen und Fernmeldedienste in der Schweiz zu gewährleisten. Erfolgsfaktoren für sichere Fernmeldeinfrastrukturen sind firmeninterne Sicherheitsorganisationen, Einführung und Betrieb von etablierten Managementsystemen sowie die Orientierung an international anerkannten Normen und Standards. asut ist daher offen gegenüber dem Anliegen des Bundesrates, die Netzsicherheit und den Schutz vor Cyberbedrohungen zu erhöhen.

Die vorgeschlagenen Änderungen in der Verordnung über Fernmeldeanlagen (FAV) sowie in der Verordnung des BAKOM über Fernmeldeanlagen (VFAV) müssen jedoch präzisiert werden. Insbesondere der Begriff der «Kritischen Netzwerkanlagen» und der entsprechende Anhang in der VAFV sind in der vorliegenden Form zu offen und unspezifisch und müssen risikobasiert und in enger Abstimmung mit den tatsächlichen Verhältnissen beim Betrieb der Infrastrukturen überarbeitet werden.

[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

Einschätzung zu den Änderungen in der Verordnung über Fernmeldedienste (FDV)

1. Übermittlung von Nummern (Art. 26a Abs. 6)

Im Rahmen einer freiwilligen Arbeitsgruppe der Branche wurde eine Lösung zur Bekämpfung von Anrufen aus dem Ausland mittels gefälschter oder missbräuchlich verwendeter Telefonnummern (Spoofing-Calls) entwickelt. Diese technischen Spezifikationen[2] sind gemäss einer Technisch Administrativen Verordnung des BAKOM seit dem 1. Januar 2026 zwingend umzusetzen. Dabei hat sich jedoch gezeigt, dass gemäss heute geltender Verordnung hohe Hürden bestehen, um die Übertragung der Nummer zu verhindern oder den Anruf zu unterbinden. Konkret müssten die Fernmeldedienstanbieterinnen Kenntnis haben, dass eine Nummer missbräuchlich verwendet wird. Mit der Anpassung in Art. 26a Abs. 6 werden die Anforderungen abgeschwächt und neu ist ein begründeter Verdacht ausreichend. Dies schafft Rechtssicherheit für die Schweizer Fernmeldedienstanbieterinnen, welche Anti-Spoofing-Massnahmen zum Schutz ihrer Kundinnen und Kunden umsetzen. asut begrüsst daher diese pragmatische Anpassung.

2. Geltungsbereich (Art. 96d)

Im Sinne einer technologieneutralen Regulierung verstehen wir, dass die Vorgaben zur Sicherheit der Mobilfunkinfrastruktur für alle Mobilfunkstandards unabhängig der Generation gelten. An dieser Stelle möchten wir darauf hinweisen, dass damit korrekterweise nicht nur die terrestrischen Mobilfunknetze reguliert werden, sondern auch die Kommunikation via Satelliten, falls diese dabei einen Mobilfunkstandard verwenden.

3. Sicherheitsmanagementsystem (Art. 96e Abs. 1)

Grundlage des Sicherheitsmanagementsystems und darauf aufbauend der Business-Continuity ist nach Art. 96e Abs. 1 eine Risikoanalyse. Wir begrüssen dieses Vorgehen, da in einer Risikoanalyse die unterschiedlichen Risiken der jeweiligen Marktteilnehmer berücksichtigt werden können und damit auch die darauffolgenden Massnahmen angemessen und verhältnismässig sind.

4. Betrieb sicherheitskritischer Fernmeldeanlagen (Art. 96f)

Dass die im Rahmen der Risikoanalyse identifizierten sicherheitskritischen Fernmeldeanlagen dem Stand der Technik entsprechen sollen, ist eine pragmatische Pflicht zur Stärkung der Sicherheit. Die Kompetenz des BAKOM zur Festlegung der sicherheitskritischen Fernmeldeanlagen soll jedoch nur nach Anhörung der Mobilfunkkonzessionärinnen und der MVNO und unter Berücksichtigung der Risikoanalyse erfolgen.

> **Änderungsantrag zu Art. 96f Abs. 1**
> [1] Die Mobilfunkkonzessionärinnen und die Full MVNO müssen sicherstellen, dass die von ihnen betriebenen sicherheitskritischen Fernmeldeanlagen dem Stand der Technik entsprechen. Das BAKOM kann die betroffenen Anlagen nach Anhörung der Mobilfunkkonzessionärinnen und der Full MVNO unter Berücksichtigung der Risikoanalyse festlegen.

Neu sollen nach Art. 96f Abs. 2 das Network-Operations-Center (NOC), das Security-Operations-Center (SOC) sowie die für den Betrieb, die Verwaltung und Steuerung wesentlichen Fernmeldeanlagen ausschliesslich in der Schweiz betrieben werden. Nur für den Notbetrieb wäre es zulässig, auf die entsprechend redundanten NOC, SOC und Fernmeldeanlagen im Ausland zurückzugreifen, wobei dieser Notbetrieb strengen Auflagen unterliegt (z.B. zeitlich befristet, Verschlüsselung, vergleichbarer gesetzlicher Datenschutz etc.).

Bei von dieser Regelung betroffenen Unternehmen, die Mitglied der asut sind, gibt es unterschiedliche Sichtweisen zu den vorgeschlagenen Änderungen. Mobilfunkkonzessionärinnen, welche all ihre Systeme bereits in der Schweiz betreiben, sind damit einverstanden, dass die Kernaufgaben kritischer Fernmeldeanlagen von der Schweiz aus wahrgenommen werden, da dies zur Stärkung der Versorgungssicherheit beitragen kann. Kleinere Unternehmen hingegen, darunter auch Full MVNOs,

[2] https://asut.ch/asut/media/id/3611/type/document/Swiss+TSP+Anti-Spoofing+Argreement+V2.0+20260701.pdf

basieren oftmals auf einem Geschäftsmodell, wonach sie die Mobilfunksysteme und -dienste zentral in einem europäischen Land für die verschiedenen Zielmärkt wie die Schweiz betreiben.

Aus einer risikobasierten Sicht sind diese Unternehmen der Ansicht, dass insbesondere Full MVNOs, weiterhin die Möglichkeit haben sollen, die wesentlichen Fernmeldeanlagen sowie NOC, SOC oder Teile davon im Europäischen Ausland zu betreiben, solange sie dieselben Anforderungen an die Cybersicherheit einhalten, wie in der Schweiz. Dabei soll auch die Kritikalität der von ihnen erbrachten Dienste für die Schweiz berücksichtigt werden. Grundlage für eine Risikoabschätzung bietet auch hier die Risikoanalyse gemäss Art. 96e.

5. Sicherheitsmassnahmen (Art. 96f^{bis})

Es ist grundsätzlich richtig, Hardware- und Softwarekomponenten zu verwenden, die nicht gefährdet sind sowie die standardisierten Sicherheitsfunktionen zu nutzen. Es ist jedoch nicht zweckmässig, wenn alle Sicherheitsfunktionen pauschal implementiert und aktiviert sein müssen. Dies könnte sogar zu Störungen und Qualitätseinbussen führen. Vielmehr sollen die Mobilfunkkonzessionärinnen und die Full MVNO auf Basis einer risikobasierten Prüfung abklären, welche Sicherheitsfunktionen notwendig sind.

> ***Änderungsantrag zu Art. 96f^{bis} Abs. 2***
> *^{2} Sie müssen sicherstellen, in ihren Netzen Hard- und Softwarekomponenten in Betrieb zu nehmen, die nicht gefährdet sind. Sie müssen ~~alle~~ standardisierten Sicherheitsoptionen installieren und implementieren*

Art. 96f^{bis} Abs. 4 fordert von den Mobilfunkkonzessionärinnen und den Full MVNO eine enge Zusammenarbeit hinsichtlich Schwachstellen und Cybervorfällen (Informationen, fachliche Praxis etc.). Damit entstehen Doppelspurigkeiten zum Informationssicherheitsgesetz, welches bereits eine Meldepflicht für Cybervorfälle vorsieht. Daher regen wir an, dass der Fachaustausch durch das BACS sichergestellt wird.

Detaillierte Einschätzung zu den Änderungen in der Verordnung über Fernmeldeanlagen (FAV)

6. Begriffe (Art. 2)

In FAV Art. 2 wird der Begriff der «Kritischen Netzwerkanlagen» auf Verordnungsstufe definiert. Zusätzlich werden in der FAV diverse Anforderungen zur Sicherheit, Konformität und Nutzung festgelegt und das BAKOM verfügt über die Kompetenz, diese Anforderungen weiter auszugestalten. Damit kann diese Verordnung erhebliche Auswirkungen auf die Betreiberinnen der Fernmeldeinfrastrukturen haben.

Angesichts der umfangreichen Normen, Standards, Best-Practices im Bereich der Cybersicherheit von Fernmeldeinfrastrukturen stellt sich die Frage, ob es überhaupt notwendig ist, spezielle «kritische Netzwerkanlagen» zu bestimmen und zu regulieren. Im Rahmen des Risikomanagement der Betreiberinnen der Fernmeldeinfrastruktur werden sicherheitskritische Systeme identifiziert und entsprechende Massnahmen umgesetzt. Die Überwachung der Systeme erfolgt durch entsprechende Managementsysteme in den dafür vorgesehenen Strukturen (SOC, NOC etc.). Es ist daher fraglich, welchen zusätzlichen Schutz die Einführung dieser neuen Kategorie von Anlagen in der Praxis tatsächlich bietet.

> ***Antrag zu Art. 2 Abs. c^{bis}***
> *Art. 2 Abs. c^{bis} soll gestrichen werden und auf den Begriff der «Kritischen Netzwerkanlagen» soll verzichtet werden.*

Sollte der Bundesrat an den «Kritischen Netzwerkanlagen» festhalten, dann muss Art. 2 Abs. c^{bis} zwingend präzisiert werden. Im Zentrum sollen Störungen oder Fehlfunktionen stehen, die das gesamte System zum Ausfall bringen oder den Betrieb der Fernmeldeinfrastrukturen schweizweit verunmöglichen.

> **Eventualiter: Änderungsantrag zu *Art. 2 Abs.***
> *c^{bis} kritische Netzwerkanlage: alle Fernmeldeanlagen, die Teil eines Netzes sind, das für die Bereitstellung von Fernmeldediensten genutzt wird, und deren Störung oder Fehlfunktion zu einem systemweiten Ausfall oder einer ~~erheblichen~~ massiven Beeinträchtigung des Betriebs von Fernmeldeinfrastrukturen führen oder die öffentliche Sicherheit gefährden kann. Die Beurteilung der Netzwerkanlage nach ihrer Kritikalität erfolgt in Konsultation entsprechender Fachgremien und unter Berücksichtigung internationaler Standards;*

7. Grundsätze (Art. 28b)

In Art. 28b wird festgehalten, dass «kritische Netzwerkanlagen» nur in den Verkehr gebracht oder betrieben werden dürfen, wenn sie spezifische Sicherheitsanforderungen einhalten. Diese werden jedoch nicht weiter ausgeführt, sondern das BAKOM erhält die Kompetenz, diese unter Berücksichtigung internationaler Normen und Praxis festzulegen. Da sich die FAV auf das heutige FMG stützt, fehlt jedoch eine ausreichende gesetzliche Grundlage für eine solche Marktzugangsbeschränkung. Zudem kann das BAKOM eine Liste der Anlagen erstellen. Die konkrete Ausgestaltung bleibt weiterhin offen, was eine grosse Rechtsunsicherheit schafft, die Planung erschwert und Investitionen in Infrastrukturen verzögert.

Dabei stellt sich erneut die Frage, ob es überhaupt zusätzliche Sicherheitsanforderungen braucht, wenn die internationalen Normen und Standards sowie Best Practices für Fernmeldeinfrastrukturen bereits verfügbar sind. Zudem besteht die Gefahr, dass neben den internationalen Normen zusätzliche Schweizer Anforderungen gestellt werden, was zu erheblichen Mehraufwänden führt, da die Komponenten und Systeme gemäss internationalen Standards für den globalen Markt produziert werden.

Daher soll auf spezifische Sicherheitsanforderungen verzichtet werden und stattdessen soll das BAKOM auf die relevanten Normen, Standards und Best-Practices verweisen, die risikobasiert zur Anwendung kommen sollen.

> **Antrag zu Art. 28b**
> *Wenn Art. 2 Abs. c^{bis} gestrichen und auf den Begriff «Kritische Netzwerkanlagen» verzichtet wird, dann muss Art. 28b entsprechend angepasst werden.*

Eventualiter: Änderungsantrag zu Art. 28b Grundsätze
[1] Unter Vorbehalt der Bestimmungen dieses Abschnitts gelten für die Bereitstellung kritischer Netzwerkanlagen auf dem Markt die Bestimmungen des zweiten und des dritten Kapitels.
[2] Eine kritische Netzwerkanlage darf nur in Verkehr gebracht oder betrieben werden, wenn sie spezifische Sicherheitsanforderungen erfüllt.
[3] ~~Das BAKOM kann eine Liste dieser Anlagen erstellen und die spezifischen Anforderungen unter Berücksichtigung der anerkannten internationalen Normen und Praxis festlegen.~~ Die spezifischen Sicherheitsanforderungen entsprechen anerkannten internationalen Normen und Praktiken.

8. Konformitätserklärung und technische Unterlagen (Art. 28c)

Die Betreiberinnen der Fernmeldeinfrastrukturen orientieren sich an anerkannten internationalen Standards bei der Planung und Umsetzung von Sicherheitsmassnahmen. Daher sollen sich die Anforderungen zur Konformitätserklärung an den Vorgaben und Standards von Organisationen wie ISO, ITU, GSMA oder 3GPP orientieren.

Antrag zu Art. 28c
Die Anforderungen bei der Konformitätserklärung basieren auf den Vorgaben und Standards internationaler Organisationen wie ISO, ITU, GSMA oder 3GPP.

9. Übergangsbestimmungen und Änderungen (Art. 44b)

Die Bestimmungen in der FAV können zur Folge haben, dass «kritische Netzwerkanlagen» ausgetauscht werden müssen. Betrifft dies zentrale und umfassende Systeme, dann ist ein ausreichend lange Übergangsbestimmung vorzusehen, damit der Betrieb der Fernmeldeinfrastruktur aufrechterhalten werden kann. Die vorgesehenen zwei Jahre sind deutlich zu kurz und die Frist soll auf fünf Jahre verlängert werden.

Änderungsantrag zu Art. 44b
Für kritische Netzwerkanlagen, die bei Inkrafttreten der Änderung vom ... auf dem Markt erhältlich sind, gelten die in den Artikeln 28b Absatz 2 und 28c vorgesehenen Pflichten nach Ablauf einer Frist von ~~zwei~~ fünf Jahren.

Detaillierte Einschätzung zu den Änderungen in der Verordnung des BAKOM über Fernmeldeanlagen (VFAV)

10. Kritische Netzwerkanlagen (Anhang 8)

Im Anhang 8 zur VFAV werden die «kritischen Netzwerkanlagen» aufgeführt. Dabei sollte es sich aus Sicht der asut um diejenigen Anlagen handeln, bei denen Störungen oder Fehlfunktionen zu einem systemweiten Ausfall oder zu massiven Beeinträchtigungen der Fernmeldeinfrastruktur führen oder die öffentliche Sicherheit gefährden können. Unter Berücksichtigung vergleichbarer Regelungen in Europa gehören dazu das Core-Netz, zentrale Transortnetze sowie Sicherheits- und Managementfunktionen zur Netzsteuerung. Wobei selbst kritische Komponenten weiterhin genutzt werden können, wenn entsprechende Sicherheitsmassnahmen ergriffen werden. Aus Sicht des Verbandes gehören periphere Anlagen wie beispielsweise das Radio-Access-Network nicht zu den kritischen Netzwerkelementen. Die Liste in Anhang 8 soll daher kritisch überprüft und auf die relevanten Komponenten reduziert werden.

In der «Teilrevison des Fernmeldegesetzes (FMG) im Bereich Sicherheit» wird im Vorschlag zur Art. 48b Abs. 2 in Bezug auf die neue Pflicht zur Mehrlieferanten-Strategie explizit auf «kritische Bestandteile» der Fernmeldeinfrastruktur verwiesen. Obwohl sich die Begriffe leicht unterscheiden, ist davon auszugehen, dass Anhang 8 der VFAV den materiellen Rahmen der Mehrlieferanten-Strategie vorgibt. Der vorliegende Anhang ist jedoch zu umfangreich und gleichzeitig zu unspezifisch, da jede Komponente für sich risikobasiert, technologieneutral und unter Berücksichtigung der Netzarchitektur sowie der Massnahmen, welche die Infrastrukturbetreiberin ergriffen hat, beurteilt werden müsste. Pauschale Kategorien sind dazu nicht geeignet. asut lehnt daher den vorliegenden Anhang 8 ab.

Antrag zu Anhang 8
Der Anhang 8 wird zur vollständigen Überarbeitung zurückgewiesen.

Detaillierte Einschätzung zu den Änderungen in der Verordnung über die Adressierungselemente im Fernmeldebereich (AEFV)

11. Untergeordnete Zuteilung (Art. 23)

Die liberale Handhabung der Unterzuteilung von Nummern im Geschäftskundenumfeld ist weiterhin eine wichtige Dienstleistung, die insbesondere international tätige Unternehmen nutzen. Die im erläuternden Bericht aufgeführten Schwierigkeiten bei der Identifikation der aktuellen Nutzerin der Nummern (Empfängerin) lässt sich im professionellen Geschäftskundenbereich einfacher lösen als durch eine drastische Einschränkung der Unterzuteilung. So gilt bereits heute, dass Nummern nur an beim BAKOM registrierte Anbieterinnen weitergegeben werden dürfen. Zusätzlich soll die weitergebende Inhaberin verpflichtet werden, auf Anfrage des BAKOM oder des Dienstes Überwachung Post- und Fernmeldeverkehr die aktuelle Nutzerin der Nummern bekannt zu geben.

Änderungsantrag zu Art. 23 Abs. 2
[2] Sie muss dafür sorgen, dass die Empfängerinnen der Nummern:
a. die ihr auferlegten Bedingungen einhalten;
b. ~~die~~ Nummern nicht ohne ihre Einwilligung weiteren Anbieterinnen zuteilen;
[3] Sie muss dafür sorgen, dass sie die Empfängerin der Nummern gegenüber dem BAKOM oder dem Dienst ÜPF benennen kann.

Eventualiter soll die Weitergabe von Nummern durch die Inhaberin auf zwei Stufen begrenzt werden.

12. Zuteilung eines MNC (Art. 47)

Neben den SBB, welche die Systemführerschaft für FRMCS ausüben, werden weitere Bahnen (z.B. Schmalspurbahnen) eigene 5G-basierte Netze im Frequenzspektrum von FRMCS, jedoch ohne Interoperabilität mit FRMCS betreiben. Daher können mehrere Betreiberinnen einen MNC benötigen.

Änderungsantrag zu Art. 47 Abs. 2
[2] Es kann ~~einer Betreiberin~~ Betreiberinnen eines privaten Funknetzes GSM-R oder FRMCS (Future Railway Mobile Communication System) je einen MNC zuteilen, wenn diese keine Fernmeldedienste anbietet.

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