Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bern, 27. Mai 2026

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

Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens

BK-D-BB8A3401/1090

Übersicht

Ausgangslage

Die Telekommunikationsinfrastruktur der Schweiz ist eine unverzichtbare und sicherheitspolitisch bedeutende Grundlage für Gesellschaft und Wirtschaft. Dies gilt insbesondere für das Mobilfunknetz. Während der Fokus in der Vergangenheit auf technischer Leistung wie Bandbreite und Qualität lag, rücken nun durch die zunehmende Digitalisierung und globale Vernetzung Sicherheitsrisiken in den Vordergrund.

Cyberbedrohungen und sonstige mittels Fernmeldeinfrastrukturen begangene Straftaten, Datenschutzverletzungen wie auch geopolitische Abhängigkeiten stellen wachsende Bedrohungen dar. Besonders problematisch sind ältere Netzgenerationen, die nicht auf die Verhinderung von Cyberangriffen ausgerichtet waren. Deshalb besteht Handlungsbedarf, um Sicherheitslücken in den heutigen, modernen Mobilfunknetzen möglichst frühzeitig zu vermeiden und den unabhängigen Betrieb, sowie die Stabilität der schweizerischen Kommunikationsinfrastruktur zu stärken.

Geschützt werden muss aber nicht nur die Infrastruktur. Auch die Konsumentinnen und Konsumenten sind mit der zunehmenden Digitalisierung und der technologischen Weiterentwicklung vermehrt Gefahren ausgesetzt, die es zu verhindern gilt.

Inhalt der Vorlage

Der Inhalt der Vorlage ergibt sich hauptsächlich aus der Erfüllung des verabschiedeten Postulats Pult (20.3984) «Digitale Infrastruktur. Geopolitische Risiken minimieren». Gemäss dem Auftrag, welcher der Bundesrat dem UVEK in diesem Zusammenhang erteilt hat, kann ein Teil der geforderten Sicherheitsmassnahmen gestützt auf den geltenden Artikel 48a Abs. 2 des Fernmeldegesetzes vom 30. April 1997 (FMG; SR 784.10) auf Stufe Verordnung umgesetzt werden. Die Vorlage bezweckt, die Sicherheit der Fernmeldeinfrastruktur zu erhöhen, um besser vor Cyber- und weiteren Sicherheitsbedrohungen geschützt zu sein. Um dieses Ziel zu erreichen, soll die Fernmeldeinfrastruktur resilienter, sicherer und diversifizierter betrieben werden müssen. Dazu werden die notwendigen Vorgaben auf Verordnungsstufe geschaffen. Darüber hinaus sind gestützt auf Artikel 28 Absatz 6 Buchstabe a und d FMG punktuelle Anpassungen im Bereich der Adressierungselemente vorgesehen. Dazu gehört ein verbesserter Schutz vor «Spoofing» und die Beschränkung von Unterzuteilung der Nummern. Auch diese Massnahmen sollen letztlich zu mehr Sicherheit für die Bevölkerung führen.

Inhaltsverzeichnis

Erläuternder Bericht

1 Ausgangslage

1.1 Handlungsbedarf und Ziele

Handlungsbedarf

Die aktuelle geopolitische Lage ist geprägt von zunehmenden Spannungen und Unsicherheiten und führt in zahlreichen Politik- und Wirtschaftsbereichen zu einem deutlich erhöhten Sicherheitsbedürfnis. Davon ist insbesondere auch der Bereich der Kommunikation betroffen. Sichere, verlässliche und jederzeit verfügbare Fernmeldeinfrastruktur bildet eine zentrale Voraussetzung für das Funktionieren von Staat, Wirtschaft und Gesellschaft. Technologische Abhängigkeiten können von ausländischen staatlichen oder staatsnahen Akteuren instrumentalisiert werden, um politischen oder wirtschaftlichen Druck auszuüben, kritische Infrastrukturen zu sabotieren oder strategische Informationen abzuschöpfen.

Die Fernmeldeinfrastruktur in der Schweiz, insbesondere die Infrastruktur des Mobilfunknetzes, hat sich zu einer allgegenwärtigen und kritischen Komponente des gesellschaftlichen und wirtschaftlichen Lebens entwickelt. Darum sollen jene Risiken minimiert werden, welche die Sicherheit der Schweiz gefährden können. Es besteht zudem ein öffentliches Interesse, dass Netzausfälle möglichst verhindert werden können.

Vor diesem Hintergrund hat das Parlament in den vergangenen Jahren verschiedene Vorstösse überwiesen, die von einem klaren Handlungsbedarf ausgehen. Diese zielen darauf ab, die Sicherheit von Fernmeldeinfrastrukturen und -diensten zu erhöhen und deren Resilienz gegen neue Bedrohungsformen nachhaltig zu stärken. Die fortschreitende Digitalisierung und die zunehmende Vernetzung von Systemen erhöhen zugleich die Angriffsflächen und damit die Verwundbarkeit durch hybride Bedrohungen, mit denen technologische Mittel zur Destabilisierung, Erpressung oder gezielten Einflussnahme eingesetzt werden. In diesem Kontext kommt einer resilienten, sicheren und diversifizierten Fernmeldeinfrastruktur eine zentrale Bedeutung zu. Sie ist eine wesentliche Voraussetzung für die Handlungsfähigkeit der Schweiz, die wirtschaftliche Stabilität sowie das Vertrauen der Bevölkerung in die Funktionsfähigkeit grundlegender Infrastrukturen.

Die technologische Entwicklung hat nicht nur wohlgesinnten Fachleuten sondern auch Cyberkriminellen neue Möglichkeiten eröffnet. Zudem könnten insbesondere Staaten, staatliche Cyber-Akteure und ausländische Nachrichtendienste, die aufgrund der geopolitischen Lage ein Interesse entwickeln, den Cyber-Raum für machtpolitische Zwecke sabotieren. Der Telekommunikationssektor steht deshalb im Visier von staatlichen Cyber-Akteuren. Das global vernetzte Internet, die sozialen Netzwerke und die künstliche Intelligenz verfügen neben einem enormen Nutzen- auch über ein sehr grosses Schadenspotenzial. Dadurch ist der Betrieb der eingesetzten Technologien mittlerweile mit erheblichen Sicherheitsrisiken durch Cyberbedrohungen verbunden. Dazu zählen insbesondere Verletzungen des Datenschutzes, der Datensicherheit sowie eine Reduktion der Kontroll- und Handlungsfähigkeit bezüglich dieser kritischen Infrastrukturen. Des Weiteren haben Cyberbedrohungen und Telefonbetrug in den letzten Jahren zugenommen und halten sich auf einem konstant hohen Niveau, weshalb immer mehr Fälle mit erheblichen finanziellen Schäden sowohl für natürliche als auch juristische Personen zu verzeichnen sind.

Die IT- und Telekommunikationsnetze älterer Generationen lassen sich nachträglich nur schwer anpassen, um Cyberangriffen oder Cyberspionage entgegenzuwirken. Ihre Sicherung wird häufig mit Behelfslösungen bewerkstelligt, da ein weltweiter, vollständiger Ersatz viel Zeit und Aufwand in Anspruch nimmt. Es muss deshalb bei den modernen Mobilfunknetzen dringend verhindert werden, dass sich fehlende Sicherheitsmerkmale und daraus resultierende Sicherheitsprobleme der älteren Generationen wiederholen.

Die vorliegende Vernehmlassungsvorlage trägt zur Umsetzung der Sicherheitspolitischen Strategie, der Nationalen Strategie zum Schutz kritischer Infrastrukturen[1] (SKI-Strategie) sowie der Nationalen Cyberstrategie NCS[2] gegen Cyberbedrohungen bei. Weiter werden gestützt auf Artikel 28 Absatz 6 Buchstaben a und d FMG Massnahmen zum Schutz schweizerischer Adressierungselemente eingeführt.

Ziele

Der Bundesrat schlägt im Rahmen der Umsetzung des Postulats Pult (20.3984) «*Digitale Infrastruktur. Geopolitische Risiken minimieren*» vor, einen Teil der geforderten Sicherheitsmassnahmen für die Fernmeldeinfrastruktur insbesondere für die Mobilfunknetze gestützt auf Artikel 48*a* Absatz 2 FMG auf Verordnungsstufe einzuführen. Die vorgeschlagenen Massnahmen sollen bereits im Hinblick auf die nächste Mobilfunkfrequenzvergabe in Kraft treten. Der Revisionsbedarf zum aktuellen Zeitpunkt ist somit insofern gegeben, als dass das Datum der Inkraftsetzung mit dem Vergabeverfahren für die Nutzung der Mobilfunkfrequenzen ab 2029 zu koordinieren ist, damit die neuen Rahmenbedingungen den Bieterinnen einer Auktion für die Nutzung der Frequenzen bekannt sein müssen. Eine Revision im Nachgang an die laufende FMG-Revision wäre hinsichtlich dieser Vorgabe somit zu spät.

Die Netzwerksicherheit in der Schweiz ist eng mit der globalen Vernetzung der Telekommunikationsinfrastrukturen verbunden. Um den Cyberbedrohungen wirksam zu begegnen, ist eine enge Zusammenarbeit zwischen den Akteuren der Telekommunikationsbranche unerlässlich. Die Bündelung von Kräften und Synergien ermöglicht eine konsistente und schnelle Umsetzung von Sicherheitsmassnahmen. Die Entwicklung von «*Best Practices*» und *«Guidelines*» sowie die Einrichtung einer gemeinsamen Datenbank für Schwachstellen, Angriffe und deren Abhilfemassnahmen sind entscheidende Schritte, um ein geordnetes Vorgehen gewährleisten zu können.

Die Übernahme und Umsetzung internationaler Regeln und Normen ist des Weiteren wichtig, um die Robustheit der betriebenen Netze zu verbessern. Die kontinuierliche Umsetzung dieser Massnahmen muss während der gesamten Lebensdauer der Systeme sowie bei technologischen Veränderungen sichergestellt werden. Die Mobilfunkkonzessionärinnen und die *Full Mobile Virtual Network Operator* (Full MVNO) – Full MVNO sind Mobilfunkanbieterinnen, die eigenständig Mobilfunk-Dienstleistungen anbieten, wobei sie jeweils das Funkzugangsnetz (*Radio Access Network* [RAN]) einer Mobilfunkkonzessionärin nutzen – müssen vor der Inbetriebnahme ihrer Infrastrukturen gewährleisten, dass diese nach dem Prinzip «*Secure by Design*» hergestellt und nach dem Prinzip «*Secure by Default*» konfiguriert sind, also dass die Systeme bereits sicher gebaut werden und von Anfang an mit sicheren Standardeinstellungen laufen. Dies

[1] *Bundesrat (2023b).*

[2] *Bundesrat (2023a).*

schliesst auch den Einsatz von Instrumenten zur Erkennung von unbefugtem Eindringen und von Kompromittierungen in Netzwerken mit ein.

Mittelfristig soll die Vorlage den Datenschutz, die Datensicherheit sowie die Kontroll- und Handlungsfähigkeit bezüglich kritischer Infrastrukturen in der Schweiz stärken. Dies wird mit dem Betrieb von Netzbetriebszentren- (*Network Operations Center* [NOC]) und Sicherheitsoperationszentren (*Security Operation Center* [SOC]) sowie der Kernfunktionen (*Core Networks*) der modernen Mobilfunknetze in der Schweiz erreicht.

Es soll die Möglichkeit geschaffen werden, die Verwendung von Netzwerkanlagen, die als kritisch eingestuft werden, in Telekommunikationsnetzen besser kontrollieren zu können und es sollen strengere Sicherheitsanforderungen zur Anschaffung von Komponenten des Core-Netzes eingeführt werden. Die Ziele sollen insbesondere mittels neuer oder angepasster Begriffsdefinitionen der Festlegung von Rahmenbedingungen sowie der Durchführung von Kontroll-, Risikobewertungs- und Konformitätsverfahren, die sich auf kritische Netzwerkanlagen beziehen, erreicht werden. Neu müssen beispielsweise die Hersteller von solchen Netzwerkanlagen eine Risikobewertung vornehmen sowie ein entsprechendes Konformitätsbewertungsverfahren mit Einbezug einer Drittstelle durchführen.

Mit den vorgeschlagenen Bestimmungen im Bereich der Adressierungselemente sollen die Nutzenden der modernen Kommunikationsmittel besser vor Cyberbedrohungen und weiteren mittels Fernmeldeinfrastrukturen begangener Straftaten geschützt werden. Dabei ist zu beachten, dass die anerkannten Probleme im Bereich der Strafverfolgung und auch der Prävention nicht im Fernmelderecht gelöst werden können. Dieses soll aber möglichst Regeln enthalten, welche die Strafverfolgungsbehörden unterstützen und der Prävention dienen, ohne dass das ordnungsgemässe Funktionieren der Kommunikation verhindert wird.

Die Einführung entsprechender Sicherheits- und Schutzmassnahmen bedingen eine Anpassung der geltenden Verordnungsbestimmungen. Erforderlich ist neben einer Teilrevision der Verordnung vom 9. März 2007[3] über Fernmeldedienste (FDV) auch eine Anpassung der Verordnung vom 25. November 2015[4] über Fernmeldeanlagen (FAV) sowie der dazugehörigen Verordnung des BAKOM vom 26. Mai 2016[5] über Fernmeldeanlagen (VFAV). Ebenfalls müssen punktuelle Änderungen in der Verordnung vom 6. Oktober 1997[6] über die Adressierungselemente im Fernmeldebereich (AEFV) erfolgen.

1.2 Geprüfte Alternativen und gewählte Lösung

Die nachfolgenden alternativen Handlungsoptionen wurden geprüft und verworfen:

- **Beibehaltung des Status Quo**
  Wenn keine neuen Sicherheitsregeln eingeführt werden, kann die Entwicklung der Telekommunikation mit dem technologischen Fortschritt nicht mithalten. Sicherheitslücken bleiben bestehen oder vergrössern sich sogar. Beim Missbrauch von Rufnummern könnten Anbieterinnen *Spoofing* weiterhin nur be-

[3] SR **784.101.1**

[4] SR **784. 101.2**

[5] SR **784. 101.21**

[6] SR **784.104**

kämpfen, wenn sie davon tatsächlich Kenntnis haben. Der Schutz vor betrügerischen Anrufen bliebe damit auf tieferem Niveau. Zudem bliebe die Nutzung von Schweizer Rufnummern durch eine kaum kontrollierbare Vielzahl von Anbieterinnen möglich und Unterzuteilungen wären weiterhin nur schwer zu beaufsichtigen.

- **Verstärkte Selbstregulierung statt verbindlicher Vorgaben**
  Empfehlungen oder freiwillige Branchenregeln reichen nicht aus, da sie oft nicht im Interesse der Anbieterinnen liegen. Zudem sind freiwillige Umsetzungen aufwendig und teuer. Wirksame Verbesserungen erfordern daher rechtlich verbindliche und durchsetzbare Vorgaben.
- **Zulassungspflicht für Kernnetzkomponenten durch das BAKOM**
  Eine Zulassungspflicht für zentrale Netzkomponenten und externe Prüfstellen ist mit hohem administrativem Aufwand und übermässigen Kosten verbunden.
- **Betrieb kritischer Funktionen unabhängig von anderen Rechtssystemen**
  Lediglich vorzuschreiben, dass Mobilfunkdienstanbieterinnen sicherstellen sollen, dass zentrale Funktionen wie NOC, SOC und der Betrieb moderner Netze für Schweizer Dienste unabhängig von ausländischen Rechtssystemen erfolgen, ist schwer überprüfbar und durchsetzbar.
- **Zentrale staatliche Cyberabwehr für private Anbieterinnen**
  Für eine zentrale staatliche Cyberabwehr für private Unternehmen fehlen aktuell die finanziellen Mittel.
- **Pflicht zu einem Firmensitz in der Schweiz**
  Die Verpflichtung für Mobilfunkanbieterinnen, einen Firmensitz in der Schweiz zu haben, würde keine zusätzlichen sicherheitsrelevanten Vorteile gegenüber einer Korrespondenzadresse oder einem Handelsregistereintrag bringen.
- **Erweiterte Kompetenzen für die ComCom bei der Frequenzvergabe**
  Die Idee, der ComCom mehr Spielraum zu geben, um bei der Frequenzvergabe sicherheitsrelevante Bedingungen vorzusehen, müsste auf Gesetzesstufe geregelt werden.
- **Obligatorische Mitgliedschaft bei der GSMA**
  Obwohl die GSM Association (GSMA) für ihre Mitglieder hilfreiche Mittel zur Verbesserung der Sicherheit bereitstellt und die Mitgliederbeiträge abhängig vom erzielten Umsatz sind, wurde aufgrund einer möglichen Verletzung der Vereinigungsfreiheit auf eine obligatorische Mitgliedschaft verzichtet.
- **Entlastungsmöglichkeiten für Unternehmen**
  Mobile Virtual Network Operator (MVNO) werden von einem Grossteil der Sicherheitsvorgaben ausgenommen. Weitere Entlastungsmöglichkeiten nach Artikel 4 Absatz 1 Buchstabe a des Bundesgesetzes vom 29. September 2023[7] über die Entlastung der Unternehmen von Regulierungskosten (UEG) sind nicht möglich. Ansonsten ist die Gefahr zu gross, dass Schwachstellen schnell lokalisiert würden und erhebliche Auswirkungen auftreten würden.

[7] SR **930.31**

Die gewählte Lösung besteht aus folgenden Elementen und ist in Ziffer 3 f. ausführlich beschrieben:

- **Strengere Sicherheitsanforderungen für kritische Netzwerkanlagen**
  Einführung verbindlicher Kontroll-, Risikobewertungs- und Konformitätsverfahren für kritische Netzwerkanlagen.
- **Konformitätsprüfungen kritischer Netzwerkanlagen**
  Die Hersteller müssen sicherstellen, dass ihre kritischen Netzwerkanlagen sicherheitskonform sind und deren Konformität mit den spezifischen Sicherheitsanforderungen anhand des geeigneten Verfahrens nachweisen.
- **Verpflichtung zu «*Secure by Design*» und Nutzung von «*Secure by Default*»-Funktionen**
  Mobilfunkkonzessionärinnen und Full MVNO müssen Netze betreiben, die von Beginn an sicher konzipiert sind und alle von den Herstellern bereitgestellten Sicherheitsfunktionen aktivieren.
- **Verpflichtende Zusammenarbeit und nationale Datenbank für Schwachstellen**
  Mobilfunkkonzessionärinnen und Full MVNO müssen aktiv zusammenarbeiten, auch mit dem Bund, und sich regelmässig über Schwachstellen und Cyberangriffe in ihren Netzen austauschen.
- **Pflicht zur Detektion von Angriffen und Kompromittierungen**
  Mobilfunkkonzessionärinnen und Full MVNO müssen Methoden und Tools einführen, um Angriffe und Manipulationen in Mobilfunknetzen zu erkennen.
- **Betrieb von Netzbetriebs- und Sicherheitsoperationszentren zwingend in der Schweiz**
  Netzbetriebs- und Sicherheitsoperationszentren (NOC und SOC) müssen in der Schweiz betrieben werden. Essenzielle Sicherheits- und Betriebsfunktionen müssen ebenfalls in der Schweiz liegen, wobei Auslandsstandorte als befristete Redundanz zulässig sind.
- **Erleichterte Bekämpfung von Rufnummernmissbrauch (*Spoofing*)**
  Anbieterinnen sollen schon bei blossen Indizien für Spoofing aktiv werden können, um Konsumentinnen und Konsumenten besser schützen zu können.
- **Beschränkung von Unterzuteilungen auf eine Stufe**
  Telefonnummern sollen nur noch einmal weitergegeben werden dürfen, um die Rückverfolgbarkeit sicherzustellen, Aufsichtsaufwand zu reduzieren und Missbrauch zu erschweren.
- **Beschränkung missbräuchlicher Verwendung von Adressierungsressourcen**
  Anpassungen bei der Nutzung von *Mobile Network Codes* (MNC), Nummernblöcken und *Global Titles* (GT) sollen verhindern, dass diese Ressourcen im Signalisierungsnetz für digitale Angriffe oder Standortverfolgung missbraucht werden.
- **Pflicht zur Einhaltung internationaler Sicherheitsstandards**
  Mobilfunkanbieterinnen und Full MVNO müssen die internationalen Sicherheitsstandards beachten.

Die vorgesehen Pflichten adressieren bisher teilweise ungeregelte Bereiche des Fernmeldemarktes. Der Handlungsbedarf ergibt sich wie in Ziffer 1.1 dargestellt aus den technologischen Entwicklungen und den sich daraus ergebenden Möglichkeiten für deren (missbräuchliche) Nutzung. Die dargestellten Entwicklungen führen nicht dazu, dass der Regelungsbedarf in anderen Bereichen des Fernmeldemarktes entfällt. Entsprechend gibt es keine Möglichkeiten, die betroffenen Unternehmen nach Artikel 4 Absatz 1 Buchstabe d UEG durch die Aufhebung von Regulierungen zu entlasten.

1.3 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates

Die Vorlage ist weder in der Botschaft vom 24. Januar 2024[8] zur Legislaturplanung, noch im Bundesbeschluss vom 6. Juni 2024[9] über die Legislaturplanung 2023–2027 angekündigt.

Die Teilrevision der genannten Verordnungen ist dennoch angezeigt, da die vorgeschlagenen Massnahmen zur Erfüllung des Ziels 20 des Bundesbeschlusses zur Legislaturplanung 2023–2027[10] beitragen. Gemäss diesem Ziel soll der Bund Cyberrisiken antizipieren und wirksame Massnahmen ergreifen, um die Bevölkerung, die Wirtschaft sowie die kritischen Infrastrukturen zu schützen. Mit den vorgeschlagenen Sicherheitsmassnahmen kann diesbezüglich ein wichtiger Beitrag geleistet werden.

Die Nationale Cyberstrategie NCS[11] gegen Cyberbedrohungen wie auch die Nationale Strategie zum Schutz kritischer Infrastrukturen[12], namentlich das Ziel «Sichere und verfügbare digitale Dienstleistungen und Infrastruktur»[13], greifen diesen präventiven Ansatz auf, beauftragen den Bundesrat aber zugleich, Cyberrisiken und -verwundbarkeiten zu analysieren und unter Berücksichtigung von Bedürfnissen und Gesetzeslücken notwendige Regelungen vorzuschlagen. Die vorliegende Vernehmlassungsvorlage steht nicht nur im Einklang mit diesen Strategien, sondern trägt auch zu deren Umsetzung bei.

1.4 Erledigung parlamentarischer Vorstösse

Mit der vorliegenden Vernehmlassungsvorlage werden die geforderten Sicherheitsanliegen gemäss Auftrag aus dem überwiesenen Postulat Pult (20.3984) «*Digitale Infrastruktur. Geopolitische Risiken minimieren*» auf Verordnungsstufe umgesetzt. Die Vorlage trägt überdies zur Umsetzung der Anliegen des Postulats Maret (24.3632) «*Unerwünschte Anrufe. Braucht es neue Massnahmen?*», der Motion Seiler-Graf (24.4392) «*Es braucht griffige Massnahmen gegen die missbräuchliche Verwendung von schweizerischen Rufnummern*» und der Motion Candinas (24.4391) «*Es braucht einen wirksamen Schutz gegen Call-ID-Spoofing von schweizerischen Rufnummern*!» bei.

---

8 BBl **2024** 525

9 BBl **2024** 1440

10 BBl **2024** 1440, Artikel 21. https://www.fedlex.admin.ch/eli/fga/2024/1440/de#art_21.

11 *Bundesrat (2023a).*

12 *Bundesrat (2023b).*

13 *NCS (2023).*

2 Rechtsvergleich, insbesondere mit dem europäischen Recht

Die Europäische Union (EU) ist ernsthaft besorgt um die Sicherheit ihrer digitalen Netzwerke und Informationssysteme als kritische Infrastrukturen für Wirtschaft und Gesellschaft. Das EU-Recht soll deshalb auf die Schaffung eines sicheren und resilienten digitalen Ökosystems ausgelegt werden. Dazu werden Sicherheitsanforderungen für die wichtigen Akteure festgelegt, die Zusammenarbeit zwischen den Mitgliedstaaten gefördert und Zertifizierungs-, Überwachungs- und Sanktionsmechanismen eingeführt. Bürgerinnen und Bürger, Unternehmen und Institutionen sollen so vor Cyberbedrohungen geschützt und das einwandfreie Funktionieren des digitalen Binnenmarkts sichergestellt werden.

Die gesetzlichen Grundlagen der EU bilden im Bereich der Sicherheit der digitalen Infrastrukturen einen umfassenden rechtlichen Rahmen und sind in drei Kategorien gegliedert: ausschliesslich der Cybersicherheit gewidmete Regelwerke, Rechtsakte, die Bestimmungen zur Cybersicherheit enthalten und Grundlagen, die auf die Cybersicherheit verweisen. Im Bereich der Sicherheit der Infrastrukturen, der Dienste und der Endgeräte massgeblich sind im Wesentlichen die Bestimmungen des Rechtsakts zur Cybersicherheit (*Cybersecurity Act*, CSA)[14], der Cyberresilienz-Verordnung (*Cyber Resilience Act*, CRA)[15], der NIS2-Richtlinie über die Sicherheit der Netz- und Informationssysteme[16] sowie des Konnektivitäts-Instrumentariums für 5G und schnelles Breitband der Europäischen Kommission («*5G-Toolbox*»)[17].

Das Abkommen zwischen der Schweizerischen Eidgenossenschaft und der EU über die gegenseitige Anerkennung von Konformitätsbewertungen (MRA Schweiz–EU)[18] ist ein Instrument zum Abbau technischer Handelshemmnisse bei der Vermarktung zahlreicher Industrieerzeugnisse zwischen der Schweiz und der EU, insbesondere im Sektor Funkanlagen und Telekommunikationsendgeräte (Kapitel 7). Entsprechend beinhaltet das MRA Schweiz–EU verschiedene Cybersicherheitsvorschriften, die im Einklang mit dem europäischen Recht stehen. Die Richtlinie 2014/53/EU über Funkanlagen (RED)[19], an welche die Schweiz ihre Gesetzgebung gestützt auf ihre internationale Verpflichtung gemäss MRA angeglichen hat, schafft einen Regelungsrahmen für das Inverkehrbringen von Funkanlagen, der technische Anforderungen für den Schutz der Privatsphäre, den Schutz personenbezogener Daten und den Schutz vor Betrug umfasst. Die Bestimmungen, die 2022 als zusätzliche grundlegende Anforderungen in die VFAV aufgenommen wurden (vgl. Art. 1 und Anhang 1 VFAV), erhöhen die Cybersicherheit bestimmter drahtloser Geräte (z.B. Smartphones, Smartwatches, Fitness-Tracker und drahtlose Spielzeuge), die auf dem Schweizer Markt erhältlich sind. Solche

---

[14] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), ABl. L 151 vom 7.6.2019, S. 15; geändert durch Verordnung (EU) 2025/37, ABl. L, 2025/37, 15.1.2025.

[15] Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), ABl. L, 2024/2847, 20.11.2024.

[16] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333 vom 26.12.2022, S. 80.

[17] *EU (2020).*

[18] SR **0.946.526.81**

[19] Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG, ABl. L 153 vom 22.5.2014, S. 62.

vernetzten Geräte müssen Funktionen aufweisen, die eine Beeinträchtigung des Kommunikationsnetzes verhindern, damit deren Resilienz gestärkt wird. Die Bestimmungen der VFAV gelten auch für 5G-Anlagen.

3 Grundzüge der Vorlage

3.1 Die beantragte Neuregelung

Die Neuregelungen bringen im Weiteren strengere Sicherheitsanforderungen für die Anschaffung und den Betrieb von Fernmeldeanlagen wie z. B. Mobilfunkantennen und Software mit sich. Dies betrifft sowohl die Mobilfunkkonzessionärinnen als auch die Full MVNO. Dies insbesondere deshalb, weil durch die Definition des Begriffs «kritische Netzwerkanlagen» und der damit verbundenen Sicherheitsanforderungen in der FAV Kontroll-, Risikobewertungs- und Konformitätsverfahren eingeführt werden, die sich auf «mobile und feste Netzwerkgeräte/-einrichtungen» beziehen. Die Herstellerinnen werden zur Abgabe einer Kopie der technischen Unterlagen verpflichtet, welche die Konformität der kritischen Netzwerkanlagen mit den erhöhten Sicherheitsanforderungen nachweist. Die mit dieser Revision eingeführten neuen Sicherheitsmassnahmen betreffen ausschliesslich die öffentlichen Fernmeldenetze, die für die Erbringung von Fernmeldediensten für Endkunden genutzt werden (Art. 2, Art. 28*b* und 28*c* FAV).

Zudem wird für die Mobilfunkkonzessionärinnen und Full MVNO eine Verpflichtung geschaffen, regelmässig die Konformität ihres Kernnetzes und ihrer anderen kritischen Netzwerkanlagen gemäss den Technischen und administrativen Vorschriften (TAV) für die Sicherheit mobiler Telekommunikationsnetze zu überprüfen sowie auch den Nachweis zu erbringen, dass sie konform mit den verschiedenen harmonisierten internationalen Normen sind (Art. 96*f*^{bis} FDV). Dem BAKOM wird es ermöglicht, Kontrollen der technischen Unterlagen, die in Besitz der Betreiberinnen sind, durchzuführen (Art. 28*b* und 28*c* FAV).

Die Mobilfunkkonzessionärinnen und die Full MVNO werden des Weiteren verpflichtet, sogenannte «*Secure by Design*»-Telekommunikationsnetze zu betreiben und alle Sicherheitsoptionen und -funktionen zu implementieren, die von den Herstellerinnen der Netzwerkanlagen «*Secure by Default*» zur Verfügung gestellt werden (Art. 96*f*^{bis} FDV).

Mit der Vorlage wird für die Mobilfunkkonzessionärinnen und die Full MVNO zudem die Pflicht eingeführt, im Bereich der Sicherheit der Fernmeldenetze und -dienste aktiv untereinander und mit den zuständigen Stellen des Bundes zusammenzuarbeiten. Ausserdem wird angestrebt, dass sie eine nationale Datenbank über unbefugtes Eindringen und von Schwachstellen in Mobilfunknetzen aufbauen und betreiben. Überdies müssen die Mobilfunkkonzessionärinnen und die Full MVNO Methoden und Instrumente zur Erkennung von unbefugtem Eindringen und von Kompromittierungen in Mobilfunknetzen einrichten und einsetzen (Art. 96*f*^{bis} FDV).

Ferner wird mit der geplanten Vorlage die Voraussetzung geschaffen, dass die Mobilfunkkonzessionärinnen und die Full MVNO ihre Netzbetriebszentren (NOC) und ihre Sicherheitsoperationszentren (SOC) in der Schweiz betreiben müssen. Die Mobilfunkkonzessionärinnen und die Full MVNO müssen des Weiteren neu sicherstellen, dass die für die Sicherheit und den Betrieb ihrer Netze essenziellen Funktionen in der Schweiz betrieben werden, wobei im Falle eines Ausfalles zeitlich befristet redundante Systeme im Ausland betrieben werden können (Art. 96*f* FDV).

Aufgrund des Gefahrenpotenzials zum Missbrauch von Schweizer Rufnummern sollen Anbieterinnen präventiver aktiv werden. In der Regel liegen den Anbieterinnen Anhaltspunkte und Indizien vor, dass eine Nummer «gespooft» wird, ohne dass sie Kenntnis im Sinne eines vorliegenden Beweises haben. Dies macht es einfacher, Konsumentinnen und Konsumenten zu schützen. Die Tatsache, dass Schweizer Nummern in der Bevölkerung eine hohe Vertrauenswürdigkeit erwecken, wird von Betrügern bewusst ausgenutzt. Das schweizerische Fernmelderecht kennt liberale Nutzungs- und Zuteilungsbedingungen von Telefonnummern. Diese Vorgaben waren in Zeiten der Marktöffnung angezeigt und notwendig, um den Wettbewerb zu fördern. Mit der zunehmenden Digitalisierung und Globalisierung der Telekommunikation erschweren die geltenden regulatorischen Bedingungen jedoch sowohl die fernmelderechtliche Aufsicht wie auch die Arbeiten der Strafverfolgungsbehörden. Verschiedene Länder in Europa (z. B. Deutschland, Frankreich, Österreich, Finnland) haben bereits Massnahmen zum Schutz ihrer Nummernbereiche ergriffen. Auch wenn Anpassungen der fernmelderechtlichen Vorgaben die Problematik allein nicht zu lösen vermögen, tragen sie dennoch zur Eindämmung und effizienteren Verfolgung von Cyberbedrohungen und anderen mittels Telekommunikationsinfrastruktur begangenen Straftaten bei (Art. 26*a* Abs. 6 FDV).

Gemäss geltendem Recht kann eine Inhaberin eines Nummernblocks ihrerseits Nummern an registrierte Anbieterinnen nach Artikel 4 FMG zum Erbringen von Fernmeldediensten zuteilen. Obschon entsprechende Unterzuteilungen dem BAKOM im Rahmen der Auslastungserhebungen gemeldet werden müssen, zeigt sich bei der fernmelderechtlichen Aufsicht und auch der Strafverfolgung, dass die Rückverfolgung der Inhaberin bei mehrfach erfolgter Weitergabe (Kaskade) teils schwer oder nicht mehr möglich ist. Dies insbesondere, wenn mehrere Stufen von Unterzuteilungen ins und im Ausland erfolgen. Seitens Behörden fällt oftmals ein enormer Aufwand an, die Kaskaden an Unterzuteilungen nachzuvollziehen und nachzuführen, respektive die Anbieterinnen ins Recht zu fassen. Die Korrespondenz mit ausländischen Unternehmen ist dabei oftmals sehr aufwändig und selten zielführend. Gegenüber Unternehmen, die sich überall auf der Welt befinden können, ist die Durchsetzung der fernmelderechtlichen Vorgaben nahezu ausgeschlossen, auch wenn diese theoretisch dem Schweizer Fernmelderecht unterliegen. Es ist daher vorgesehen, die Bekämpfung von missbräuchlichen Verwendungen schweizerischer Nummern mittels punktueller Vorgaben auf Verordnungsstufe zu unterstützen. Als Massnahme soll deshalb inskünftig nur noch eine einstufige Unterzuteilung von der Nummernblockinhaberin an eine einzige weitere Anbieterin (mit Sitz im In- oder Ausland) möglich sein, damit eine Identifikation der aktuellen Inhaberin jederzeit gewährleistet ist. Mit der Beschränkung der Unterzuteilung auf lediglich eine Stufe soll der administrative und aufsichtsrechtliche Aufwand und dessen Kosten gesenkt werden sowie gleichzeitig die Kontrolle über die Nutzung von Schweizer Nummern erhöht werden. Dies dient auch der Missbrauchsbekämpfung, da Schweizer Telefonnummern oft in Zusammenhang mit Betrugsfällen, namentlich um gefälschte Nutzerkonten auf Online-Plattformen (Soziale Medien, Messenger-Apps wie WhatsApp) in Erscheinung treten oder bei Banken und Bezahldiensten (wie z. B. Twint) zur Registrierung benutzt werden (Art. 23 Abs. 2 Bst. a und b AEFV).

Weiter wird eine Anpassung betreffend die in den Mobilfunknetzen verwendeten Adressierungselemente vorgeschlagen. Mit der vorgesehenen Änderung von Artikel 47 AEFV soll die Zuteilung von Adressierungselementen (MNC und Nummernblöcke des Nummerierungsplans E.164) eindeutig mit der Zusammensetzung eines *Global Title* (GT) verknüpft werden. Der GT muss daher ausdrücklich einen Teil der Kennungen enthalten, die den zugewiesenen E.164-Nummernblöcken sowie den MNC zugeordnet sind.

Der GT wird in einem Signalisierungssystem verwendet, um die Weiterleitung von Anrufen über die Mobilfunknetze sicherzustellen. Mit den Massnahmen soll verhindert werden, dass GT, die offensichtlich nicht ausdrücklich den zugewiesenen Adressierungselementen zugeordnet sind, für betrügerische Zwecke im Signalisierungsnetz der Mobilfunknetze – beispielsweise zur Standortverfolgung von Mobilfunkkundinnen und Mobilfunkkunden – verwendet werden.

Die Einführung einer Verpflichtung für die Mobilfunkkonzessionärinnen und Full MVNO, die internationalen Sicherheitsstandards zu beachten, soll schliesslich ebenfalls zur Stärkung der Sicherheit und damit des Standorts Schweiz beitragen (Art. 96*f*^{bis} FDV).

3.2 Umsetzungsfragen

Die vorgesehenen Massnahmen hinsichtlich Sicherheitsrisiken orientieren sich hauptsächlich an der «*5G-Toolbox*» der EU. Entsprechend sind diese für international tätige Anbieterinnen ohnehin zu berücksichtigen. Zudem basieren sie auf internationalen technischen Normen und Standards. Es ist deshalb von einer einfachen Umsetzbarkeit auszugehen und höhere regulatorische Anforderungen als bei vergleichbaren Regulierungen im Ausland werden vermieden (vgl. Artikel. 4 Absatz 1 Buchstabe. b UEG).

Inwiefern der Vollzug der Regulierungen gemäss Artikel 4 Absatz 1 Buchstabe c UEG mit elektronischen Mitteln vereinfacht werden kann, lässt sich nicht abschliessend beurteilen. Interaktionen mit den Behörden finden nur in geringem Mass statt. Die Massnahmen betreffen in erster Linie die betriebliche Organisation von rund 15 Mobilfunkbetreiberinnen sowie einer unbekannten, maximal zweistelligen Anzahl von (internationalen) Herstellerinnen von Netzwerkanlagen für Mobilfunknetze. Den betroffenen Unternehmen steht es frei, mit welchen Mitteln sie die vorgegebenen Ziele erreichen.

4 Erläuterungen zu einzelnen Artikeln

4.1 Verordnung vom 9. März 2007 über Fernmeldedienste

Art. 1 Bst. e Begriffe

In Artikel 1 Buchstabe e wird neu definiert, was unter Full MVNO zu verstehen ist, nämlich eine Fernmeldedienstanbieterin, die unabhängig Mobilfunkdienste über das Funkzugangsnetz (*Radio Access Network* [RAN]) einer Mobilfunkkonzessionärin anbietet. Es handelt sich also um eine Anbieterin eines vollständigen virtuellen Mobilfunknetzes, die das RAN einer Mobilfunkkonzessionärin mietet. Ein Full MVNO kann somit gemäss folgender Kriterien definiert werden:

- Registrierung als Fernmeldedienstanbieterin (FDA) beim BAKOM;
- Inhaberin eines vom BAKOM verwalteten MNC ohne Einschränkungen;
- Inhaberin eines vom BAKOM verwalteten Adressierungselementes des Nummerierungsplans E.164;
- Partei eines nationalen Roaming-Abkommens (*National Roaming Agreement* [NRA]) mit einer FDA, die Konzessionärin von Funkfrequenzen ist;
- teilweiser oder vollständiger Besitz und Betrieb eines oder mehrerer eigener Mobilfunk-Kernnetze (*Core Network*).

Art. 26a Abs. 6 Übermittlung von Nummern

Anrufe von Betrügern mit gefälschter Schweizer Anrufernummer (*Calling Line Identification*, [CLI]) sind ein weit verbreitetes Ärgernis mit erheblichem Schädigungspotenzial. Sie erwecken ungerechtfertigtes Vertrauen, das ausgenützt wird, um Angerufene in der Schweiz auf verschiedenste Weise zu betrügen und finanziell zu schädigen. Diese von diesen Betrügereien ausgehende Gefahr muss schnell, präventiv und wirksam bekämpft werden können. Darum sollen Massnahmen, welche die Anbieterinnen bereits heute gegen solche «gespoofte» Anrufe ergreifen müssen, nicht erst bei deren Kenntnis möglich sein, sondern schon bei begründetem Verdacht. Die Anbieterinnen haben keine Möglichkeit, tatsächlich Kenntnis von solchen betrügerischen Anrufen zu erhalten, da insbesondere eine inhaltliche Überwachung, welche dazu gegebenenfalls nötig wäre, durch die Anbieterinnen grundsätzlich unzulässig ist. Tatsächliche Kenntnis kann oftmals erst im Nachhinein vorliegen, wenn bereits ein Schaden entstanden ist.

Neu reicht es bereits aus, dass Anbieterinnen den begründeten Verdacht haben, dass eine übermittelte Nummer ungültig ist oder ohne Nutzungsrecht verwendet wird und somit «gespooft» ist. Die Anforderungen für eine Unterdrückung einer Nummer oder für die Unterbindung eines Anrufs werden somit gelockert, damit ein schnelleres Tätigwerden möglich ist.

Gestützt auf Artikel 26*a* Absatz 6 FDV haben die Anbieterinnen die Möglichkeit, die Übermittlung einer Nummer entweder zu verhindern (Unterdrückung der CLI) oder die Verbindung vollständig zu unterbinden. Der Verordnungsgeber räumt diesen Spielraum ein, weil es für die Anbieterinnen in der Praxis kaum möglich ist, im Vorfeld für jede mögliche Konstellation, in der Schweizer Nummern genutzt werden, mit Sicherheit festzustellen, ob eine angezeigte Rufnummer ungültig ist, weil sie «gespooft» ist oder weil ein technischer Übertragungsfehler vorliegt. Andererseits haben die Anbieterinnen nur in Zusammenhang mit dem ihnen zugeteilten eigenen Nummernbereich und ihren Kundinnen und Kunden die Möglichkeit, mit Sicherheit festzustellen, ob eine Nummer mit Nutzungsrecht eingesetzt wird. Es gibt beispielsweise keine Datenbank, welche den Anbieterinnen eine übergreifende Überprüfung erlauben würde. Dies kann von Anrufenden gezielt ausgenutzt werden, indem sie eine Nummer einer Kundin der Anbieterin A «spoofen», um potenziell Opfer zu erreichen, die Kunde bei Anbieterin B sind. Die konkreten Umstände können von Anruf zu Anruf und je nach Situation und Anbieterin (z.B. Grösse, Netzwerktechnologie etc.) erheblich variieren, weshalb den Anbieterinnen die freie Wahl zwischen den beiden Möglichkeiten zuzustehen ist.

In der Regel dürften sich die Anbieterinnen daher auf die Unterdrückung der CLI beschränken, da dies die mildere Massnahme darstellt. Eine weitergehende Blockierung eines Anrufs kommt wohl erst dann in Betracht, wenn der Anbieterin Informationen vorliegen, die praktisch keinen anderen Schluss zulassen, als dass es sich um einen betrügerischen Anruf handelt. Dies kann beispielsweise der Fall sein, wenn der eigene Nummernbereich betroffen ist. Dann kann eine Anbieterin feststellen, dass sich der entsprechende Kunde, beziehungsweise dessen zugewiesene Nummer nicht im Ausland befinden kann, etwa weil die Nummer oder das Gerät gleichzeitig im eigenen Netz in der Schweiz aktiv ist. Dies gilt auch bezüglich Ziffernfolgen, die als Rufnummer gar nicht existieren können, weil sie die Voraussetzungen der E.164-Nummernblockbestimmungen nicht erfüllen, oder z.B. für Notrufnummern wie 117 oder 118. Weiter können auch Anrufmuster darauf hindeuten, dass die angezeigten Nummern «gespooft» sind, so zum Beispiel eine extrem hohe Frequenz identischer Anrufe innerhalb weniger Sekunden («Wellencharakter») gleichen Ursprungs mit systematisch wechselnden

Nummern. In solchen eindeutig gelagerten Fällen wäre auch eine vollständige Blockierung der Anrufe angezeigt. Da jedoch nur selten alle relevanten Informationen vorliegen und die Bewertung laufend sowie in Echtzeit erfolgen muss, wird in den meisten Fällen weiterhin ein Rest an Unsicherheit verbleiben. Aus diesem Grund steht es den Anbieterinnen letztlich immer frei, stattdessen das mildere Mittel – die Unterdrückung der CLI – anzuwenden.

Art. 96d Geltungsbereich

Die Revision der Verordnung über Fernmeldedienste von 2022, die in Anlehnung an die in der EU laufenden Arbeiten betreffend Sicherheit der Fernmeldenetze erfolgte, umfasste nur die Mobilfunknetze der fünften Generation (5G). Aktuell wird die Gesetzgebung im Bereich der Netzsicherheit wie in manchen EU-Mitgliedstaaten auf alle Mobilfunkgenerationen oder auch auf die Festnetze ausgeweitet.

Solange weltweit Netze älterer Generationen betrieben werden, müssen die Schweizer Betreiberinnen die Interkonnektion gewährleisten. Sie müssen deshalb bestimmte Netzknoten oder Funktionalitäten früherer Technologien (analoge Netze) weiterbetreiben, die ursprünglich nicht für ein derart umfassendes und spezialisiertes Cybersicherheitsumfeld ausgelegt waren.

Ebenso können sich die von den Artikeln dieser Verordnung (Art. 96*e*, 96*f*, 96*f*^{bis} und 96*g*) erfassten betroffenen Rechtssubjekte heute nicht mehr nur auf die Mobilfunkkonzessionärinnen (MNO) beschränken. Neu gelten die Verpflichtungen deshalb auch für die Full MVNO, da sie bestimmte kritische Netzknoten und -funktionalitäten unabhängig von ihrer MNO betreiben (Art. 96*d* Abs. 2 Bst. b).

Grundsätzlich betreffen die neuen Sicherheitsmassnahmen, die den Mobilfunkkonzessionärinnen und den Full MVNO auferlegt werden, nur diejenigen Unternehmen, die ein oder mehrere öffentliche Fernmeldenetze betreiben, die für die Erbringung von Fernmeldediensten für Endkunden genutzt werden.

Art. 96e Sicherheitsmanagementsystem

Absatz 1 dieser Bestimmung wird dahingehend ergänzt, dass nicht nur die Mobilfunkkonzessionärinnen ein Informationssicherheits-Managementsystem auf Grundlage einer Risikoanalyse und der daraus abgeleiteten Sicherheitsziele entwickeln, implementieren und kontinuierlich überprüfen müssen, sondern auch die Full MVNO diese Pflicht haben. Da Full MVNO ebenfalls einen grossen Teil der Netzinfrastruktur selbst betreiben, müssen für die Full MVNO dieselben Regeln gelten wie für die Mobilfunkkonzessionärinnen.

Art. 96f Betrieb sicherheitskritischer Fernmeldeanlagen

Absatz 1:

In Absatz 1 werden nun auch die Full MVNO explizit verpflichtet, sicherzustellen, dass die von ihnen betriebenen kritischen Netzwerkanlagen dem Stand der Technik entsprechen.

Für die Definition, welche Anlagen als kritische Netzwerkanlagen im Sinne dieser Bestimmung gelten, ist die Legaldefinition in Artikel 2 Absatz 1 Buchstabe *c*^{bis} FAV massgebend.

Absatz 2:

Die geografische Vorgabe zum Betrieb sicherheitskritischer Fernmeldeanlagen in der Schweiz soll die für den Betrieb, die Steuerung und Verwaltung wesentlichen Fernmeldeanlagen umfassen. Davon betroffen ist beispielsweise das sogenannte 5G-Kernnetz (*5G core network*). Dieses ist *cloud native* konzipiert, was bedeutet, dass dessen Funktionen oder Instanzen grundsätzlich in einem anderen geografischen Gebiet betrieben werden können als die Mobilfunkantennen (*radio access network* [RAN]). Während Erstere durch die Möglichkeit der virtualisierten Bereitstellung ortsungebunden sind, müssen sich Letztere physisch an dem Ort befinden, an welchem die Mobilfunkdienste erbracht werden. Für den RAN-Teil eines Mobilfunknetzes erübrigen sich daher geografische Vorgaben. Das geografische Gebiet für den Betrieb der sicherheitskritischen Fernmeldeanlagen, insbesondere der Netzbetriebs- und Sicherheitsoperationszentren, ist grundsätzlich auf die Schweiz beschränkt. Dies gilt neu sowohl für die Mobilfunkkonzessionärinnen wie auch für die Full MVNO.

Die Pflicht, dass bestimmte kritische Infrastrukturen oder Betriebszentren aus Sicherheitsgründen in der Schweiz sein müssen, ist gemäss der Artikel XIV Buchstabe a (Schutz der öffentlichen Ordnung), XIV Buchstaben c iii und XIV^{bis} (Sicherheit) des Anhangs 1B des Abkommens zur Errichtung der Welthandelsorganisation WTO[20] (Allgemeines Abkommen über den Handel mit Dienstleistungen, GATS) zulässig. Sie zielt darauf ab, die vom WTO-Recht geforderte Konformität mit den schweizerischen Gesetzen und Vorschriften im Bereich der Telekommunikationssicherheit (Art. 48*a* FMG) sicherzustellen. Ferner erfüllt die Pflicht das Erfordernis der Notwendigkeit nach WTO-Recht, da es sowohl aus technischen und operativen Gründen als auch angesichts der geo- und sicherheitspolitischen Gegebenheiten wichtig ist, die schweizerische Fernmeldeinfrastruktur durch eine Standortpflicht sicherer zu machen. Diese Erhöhung der Sicherheit erfolgt neu durch geografische Vorgaben für kritische Fernmeldeinfrastrukturen und die Pflicht, für die Telekommunikation essenzielle Betriebszentren in der Schweiz zu betreiben. So können die Betriebskontinuität und die Sicherheit der Telekommunikation von der Schweiz aus gewährleistet werden. Dem Verhältnismässigkeitsprinzip wird insofern Rechnung getragen, als Absatz 3 den Mobilfunkkonzessionärinnen und Full MVNO die Möglichkeit gibt, unter bestimmten Voraussetzungen über redundante Systeme in Staaten zu verfügen, die einen angemessenen Datenschutz garantieren.

Absatz 3:

Gemäss Buchstabe a dürfen redundante Systeme nur in Ländern betrieben werden, die einen angemessenen Datenschutz gewährleisten. Eine entsprechende Liste von Staaten, in welchen ein redundantes System betrieben werden darf, findet sich in Anhang 1 der Verordnung vom 31. August 2022[21] über den Datenschutz.

Zweck der Bedingung in Buchstabe b ist, dass die sicherheitskritischen Fernmeldeanlagen auch dann weiter funktionieren, wenn die Verbindungen in andere Staaten gestört sind. Dies beispielsweise aufgrund diplomatischer Verwerfungen oder politischer Entwicklungen, die zu einer Sperre internationaler Fernmeldeverbindungen führen. Darüber hinaus soll verhindert werden, dass kryptografische Schlüssel durch die Ausübung von politischem oder juristischem Druck in die Hände von anderen Staaten fallen können.

[20] SR **0.632.20**

[21] SR **245.11**

Buchstabe c soll sicherstellen, dass die durch die Mobilfunkkonzessionärinnen und Full MVNO bereitgestellten Dienste der Sprachtelefonie und des Internetzugangs auch dann funktionieren, wenn die Verbindungen zu den redundanten Systemen gestört oder nicht mehr möglich sind. Zudem soll verhindert werden, dass die Gewährleistung der zuvor genannten Dienste durch korrumpierte Systeme, deren Betriebsstandort einer ausländischen Gesetzgebung untersteht, nicht eingeschränkt werden können. Hierzu trägt die geografische Verortung der Kontrolle und damit der Verwaltung der für den Betrieb notwendigen digitalen Schlüssel und Zertifikate entscheidend bei. Die Verwaltungshoheit in der Schweiz festzulegen, ist eine logische Konsequenz davon. Da bei sicheren Verbindungen in der Regel auf beiden Seiten private Schlüssel vorhanden sein müssen, ist es hingegen zulässig, dass von der Schweiz aus verwaltete Schlüssel auch in anderen Staaten gespeichert werden können.

Die Kontrolle der digitalen Schlüssel umfasst damit sowohl die Erstellung, die Verteilung, die Nutzung und die Deaktivierung sowie die Vorgabe von Richtlinien für die Speicherung. Es muss sichergestellt sein, dass Schlüssel jederzeit von der Schweiz aus deaktiviert werden können. Gleiches gilt prinzipiell für die Vergabe von signierten digitalen Zertifikaten, die für den Betrieb notwendig sind. Diesbezüglich ist sicherzustellen, dass die Stammzertifizierungsstelle (*root certification authority*) als oberste und vertrauenswürdigste Instanz in der Schweiz lokalisiert ist und ein Widerruf von ausgegebenen Zertifikaten (*revocation*) von der Schweiz aus jederzeit möglich ist. Für kryptografische Schlüssel und Zertifikate, die der Verschlüsselung von gespeicherten Daten dienen, ist in den Richtlinien zur Speicherung vorzusehen, dass diese nur in der Schweiz gespeichert werden. Ihre Verwaltung hat unter Verwendung von in der Schweiz betriebenen und nach anerkannten Normen zertifizierten Hardware-Sicherheitsmodulen zu erfolgen. Damit werden vollständig cloudbasiert Schlüssel-Verwaltungs-Systeme (*Key Management Systems* [KMS]) ausgeschlossen.

Im Ergebnis soll sichergestellt sein, dass ein Unterbruch internationaler Verbindungen die Gewährleistung des öffentlichen Telefondienstes und des Zugangsdienstes zum Internet in der Schweiz nicht stört. Die Fernmeldenetze sollen in ihrer Grundfunktion nicht beeinträchtigt werden und die Fernmeldedienstanbieterinnen sollen die in ihrem Verantwortungsbereich liegenden Dienste vom Unterbruch unberührt gewährleisten können. Nicht adressiert werden damit Abhängigkeiten zu Diensten, die über das Internet erbracht werden und deren Bereitstellung von Servern im Ausland abhängt. Diese liegen nicht im Verantwortungsbereich der Fernmeldedienstanbieterinnen (Bst. d).

Absätze 4 und 5:

Das BAKOM ist spätestens 48 Stunden nach Beginn eines Notbetriebes zu informieren. Je nach Art und Schwere des Ausfalls legt das BAKOM die maximale Dauer fest, während derer der Betrieb über die redundanten Systeme im Ausland erfolgen darf. Es kann die Dauer jeweils verlängern, wobei darauf jedoch kein Anspruch besteht.

Absatz 6:

Abgeleitete kryptografische Schlüssel und Zertifikate zeichnen sich dadurch aus, dass jederzeit ein weiterer Schlüssel oder ein weiteres Zertifikat besteht, welches die Nutzung des abgeleiteten Schlüssels oder Zertifikats einschränken oder unterbinden kann. Bei den temporären Schlüsseln und Zertifikaten kommt ergänzend hinzu, dass diese nur kurzfristig gültig sind und nach einem definierten Zeitraum verfallen. Das BAKOM wird in technischen administrativen Vorschriften einen angemessenen Zeitraum festlegen.

Absatz 7:

Zu protokollieren sind insbesondere Datum und Uhrzeit des Zugriffs, IP-Adresse von Quelle und Ziel, der Benutzername und Prozess, unter welchem der Zugriff erfolgt sowie relevante Meldungen zum Ereignis.

Art. 96f^bis Sicherheitsmassnahmen

Absatz 1:

Diese Sicherheitsmassnahme umfasst mehrere Themen, die alle gleich wichtig sind. In technischer Hinsicht stellen die Mobilfunkkonzessionärinnen und die Full MVNO sicher, dass sie Geräte und Software bei verlässlichen Lieferanten beschaffen. Sie müssen gewährleisten, dass ihre Infrastrukturen ausreichend redundant ausgelegt sind. Ausserdem wenden sie auf sämtliche ihrer Infrastrukturen kontinuierlich die Prinzipien «*Zero Trust*», Segmentierung multipler Entitäten (Netzknoten) oder Funktionalitäten (*Network Functions*), Verschlüsselung und Schutz (*Firewalls*) an.

Da Sicherheit nicht nur von Geräten, sondern auch von Menschen abhängt, gewähren die Mobilfunkkonzessionärinnen und die Full MVNO ihren eigenen oder den im Rahmen eines Unterauftrags tätigen Technikerinnen und Technikern nur eingeschränkten Zugang zu den Räumlichkeiten und Infrastrukturen ihrer IT- und Fernmeldenetze. Sie erstellen Handbücher mit detaillierten Beschreibungen des Vorgehens im Falle von Cyberbedrohungen oder -angriffen und stellen diese dem betroffenen Personal zur Verfügung.

Die Cyberwelt kennt keine Grenzen und ist ständig Bedrohungen ausgesetzt. Wachsamkeit rund um die Uhr ist deshalb zwingend. Die Mobilfunkkonzessionärinnen und die Full MVNO stellen in ihren Netzen kontinuierlich sicher, dass einerseits Anomalien und Schwachstellen erkannt und andererseits Spionage, Sabotage und der Abfluss besonders schützenswerter Personendaten ihrer Kundinnen und Kunden bekämpft werden. Sie sind bestrebt, ihre Anlagen auf dem neuesten Stand zu halten, und wenden unverzüglich alle verfügbaren Lösungen an, um Schwachstellen zu beheben.

Absatz 2:

Netzinfrastrukturen können definiert werden als die Hard- und Software-Ausstattung, welche die Erbringung von drahtlosen Kommunikationsdiensten (Sprache, Nachrichten, Internet) für Mobilfunknutzerinnen und Mobilfunknutzer ermöglicht. Es handelt sich dabei um alle Anlagen der Zugangsnetze (RAN), Kernnetze (*Core Network*) und Transportnetze (*Transport Network*) aller Generationen von Mobilfunknetzen (2G, 3G, 4G, 5G und folgende).

Die Netzinfrastrukturen müssen zwingend so genau wie möglich getestet werden, damit Abweichungen von den Spezifikationen der Herstellerinnen/Lieferanten und den international anerkannten Standards vor ihrer Inbetriebnahme erkannt werden.

Besonderes Augenmerk sollte auf allfällige Hintertüren (*Backdoors*) gelegt werden, um die Manipulation von Netzelementen und den Abfluss von Daten im Zusammenhang mit Abonnementskundinnen und Abonnementskunden oder anderer Informationen zu verhindern, welche die Integrität und Sicherheit von Personen, Unternehmen, Wirtschaft oder Staat beeinträchtigen können. Netzinfrastruktur darf nicht in Betrieb ge-

nommen werden, solange Zweifel am Bestehen solcher Bedrohungen nicht ausgeräumt sind. Das gilt auch für die Inbetriebnahme wichtiger System-Aktualisierungen zu einem späteren Zeitpunkt.

Die Mobilfunkkonzessionärinnen und die Full MVNO überprüfen alle ihre Kommunikationsnetze so häufig wie nötig mit leistungsstarken Scannern auf Kompromittierungen. Sie treten auf nationaler oder internationaler Ebene mit mindestens zwei weiteren anerkannten Betreiberinnen, die über vergleichbare Infrastrukturen verfügen, in Verbindung, um sich über mögliche bekannte oder vermutete Kompromittierungen auszutauschen.

Alle von den Herstellerinnen/Lieferanten entwickelten standardisierten Optionen für die Netzsicherheit (Hard- oder Software) müssen in allen Kommunikationsnetzen der Mobilfunkkonzessionärinnen und der Full MVNO implementiert werden (Abs. 1, letzter Satz). Der Begriff «standardisiert» bezieht sich beispielsweise auf die technischen Spezifikationen 3GPP «TS 33.501»[22] und auf die Empfehlungen «FS.40 – 5G Security Guide» der GSM Association[23].

Absatz 3:

Die Überwachung wird in allen Teilen der Netze durchgeführt: im Funkzugangsnetz (RAN), Kernnetz (*Core Network*) und Transportnetz (*Transport Network*). Sie betrifft sowohl die Mobilfunknetze als auch die Signalisierungs- und Interkonnektionsnetze.

Die Mobilfunkkonzessionärinnen und die Full MVNO setzen kontinuierlich geeignete Instrumente ein, um Logfiles aller ihrer Netzknoten zu erstellen, zu sammeln und auszuwerten und so Schwachstellen, Anomalien und unbefugtes Eindringen zu erkennen.

Anomalien werden anhand zweier grundlegender Prinzipien festgestellt: der Korrelation mehrerer disparater, aber unwahrscheinlicher Ereignisse sowie einer ungewöhnlichen Abweichung vom normalen Systemverhalten.

Bedroht eine durch diese Überwachung erkannte Gefahr unmittelbar die Sicherheit von Bevölkerung, Unternehmen, Wirtschaft oder Staat, melden die Mobilfunkkonzessionärinnen und die Full MVNO dies unverzüglich den Polizeibehörden und den zuständigen Bundesbehörden. Sie arbeiten aktiv mit diesen zusammen, um die Risiken zu minimieren und die Bedrohung zu beseitigen.

Absatz 4:

Für die Netzsicherheit gelten nicht die üblichen Gesetze von Markt und Wettbewerb. In diesem Bereich sind Solidarität und Zusammenarbeit besonders wichtig. Bei der Bekämpfung von Cyberangriffen zum Schutz von Bevölkerung, Unternehmen, Wirtschaft und Staat ist der Informationsaustausch entscheidend.

Die Anbieterinnen von Fernmeldediensten sind nach Artikel 96 FDV verpflichtet, Cyberangriffe mit einem gewissen Umfang (mindestens 10 000 betroffene Abonnentinnen und Abonnenten) der Nationalen Alarmzentrale (NAZ) zu melden und sich gegenseitig

[22] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169.

[23] https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/5g-security-guide-version-3-0/.

über die Art des Angriffs, die verursachten Schäden und die vorhergesehenen Massnahmen für die rasche Wiederherstellung des sicheren Normalbetriebs zu informieren.

Soweit möglich und unter Wahrung von Vertraulichkeit und Datenschutz unterstützen sich die Mobilfunkkonzessionärinnen und die Full MVNO gegenseitig. Ferner sollten sich ihre Abteilungen für Cybersicherheit mehrmals jährlich treffen, um unter Beachtung von Vertraulichkeit und Datenschutz Erfahrungen auszutauschen und wirksame Schutzmassnahmen gegen Cyberangriffe zu erarbeiten.

Falls notwendig führen die Mobilfunkkonzessionärinnen und die Full MVNO im Beisein von Bundesstellen wie dem Bundesamt für Cybersicherheit (BACS) oder dem BAKOM jährlich einen oder mehrere Workshops durch.

Es sollte eine gemeinsame Datenbank eingerichtet werden, in der Schwachstellen, Anomalien und unbefugtes Eidringen protokolliert werden und die von jeder Mobilfunkkonzessionärin und Full MVNO fortlaufend aufgrund neuer Erkenntnisse und aktueller Ereignisse ergänzt wird.

Absatz 5:

Die Mobilfunkkonzessionärinnen und die Full MVNO setzen kontinuierlich und systematisch ein «*SMS Home Routing*»-System ein, um die Verbreitung von betrügerischen SMS- und Signalisierungsnachrichten zu bekämpfen.

«*SMS Home Routing*» ist eine Netzfunktion, die sicherstellt, dass jede für eine Abonnentin oder einen Abonnenten bestimmte SMS-Nachricht zuerst an das «*Mobile Switching Center*» (MSC) oder das «*Short Message Service Center*» (SMSC) ihres oder seines Heimnetzes geleitet wird, auch wenn sie oder er sich im Roaming befindet.

Das «*SMS Home Routing*»-System der Mobilfunkkonzessionärinnen und der Full MVNO zwingt ihr «*Home Location Register*» (HLR), immer mit einer Heimadresse zu antworten, die auf ihr «*Home-Mobile Switching Center*» (H-MSC) oder ihr «*Home-Short Message Service Center»* (H-SMSC) verweist, und niemals den tatsächlichen Standort, d. h. die Adresse des ausländischen «*Visitor-Mobile Switching Center*» (VMSC) der Abonnentin oder des Abonnenten, die oder der sich im Roaming befindet, preiszugeben.

Indem die SMS-Nachrichten der sich im Roaming befindenden Nutzerinnen und Nutzer zuerst auf die Netze der heimischen Mobilfunkanbieterin zurückgeleitet werden, bevor sie an die Empfängerin oder den Empfänger übermittelt werden, haben die heimischen Mobilfunkanbieterinnen die Möglichkeit, anormale oder betrügerische Nachrichten effizient zu filtern.

Ohne ein solches System werden SMS von der Mobilfunkanbieterin des Landes, in dem sich die Abonnentinnen und Abonnenten im Roaming befinden, direkt an die Empfängerin oder den Empfänger zugestellt, ohne dass die heimische Mobilfunkanbieterin eine Möglichkeit zur Kontrolle der Sicherheit hat. Je nach Seriosität der Roaming-Betreiberin beziehungsweise abhängig davon, ob sie Sicherheitsfilter einsetzt oder nicht, können betrügerische Nachrichten ihr Ziel mit potenziell unangenehmen (unerwünschte Werbung und Phishing usw.) oder gefährlichen Folgen (Ortung von Personen, Abfangen oder Manipulation von Daten usw.) erreichen.

Absatz 6:

Solange weltweit analoge Fest- oder Mobilfunknetze betrieben werden, erfordert deren Interkonnektion Signalisierungsprotokolle. Einige dieser Protokolle wurden zu einer Zeit erstellt, in der sie nur von einer kleinen Zahl von vertrauenswürdigen Akteurinnen und Akteuren genutzt wurden, und nicht mit erweiterten Sicherheitsmechanismen versehen waren. Mit dem Aufkommen der mobilen Kommunikation und des Internets haben immer mehr Akteurinnen und Akteure aller Art Zugang zu diesen Protokollen und zu den Netzen erhalten. Da diese Sicherheitslücken nicht auf globaler Ebene kontrolliert werden können, muss jede Mobilfunkkonzessionärin und jede Full MVNO Massnahmen für ihre eigene Infrastruktur ergreifen.

Bei den Filterinstrumenten handelt es sich um Signalisierungs-Firewalls, die auf den Signalisiertransferpunkten der einzelnen Netztypen und -generationen installiert sind. Falls nötig, werden auch direkt auf dem HLR oder dem MSC Filteroperationen vorgenommen. Da sich die Cyberbedrohungslage ständig verändert, sind auch die Filterregeln nicht statisch. Die Mobilfunkkonzessionärinnen und die Full MVNO passen ihre Filterregeln laufend an die technologische Entwicklung und die neuen Bedrohungen an.

Selbst bei der Abschaltung bestimmter Generationen von Mobilfunknetzen (2G, 3G) betreiben die Mobilfunkkonzessionärinnen und die Full MVNO manche Knoten (Beispiel: Knoten «*Signalling Transfer Points*» [STP] für die 2G-Netze) dieser veralteten Netze weiter, um die Interkonnektion sicherzustellen. In diesem Fall betreiben sie auch die damit verbundenen Firewalls weiter.

Die Mobilfunkkonzessionärinnen und die Full MVNO verwenden die international anerkannten technischen Normen und Best Practices für Betrieb und Sicherheit.

Im Bereich der Sicherheit der Signalisierungsnetze sind unter anderem die folgenden Dokumente relevant:

- 3GPP: TS 33.501;
- 3GPP: 5G Security Evolution in 3GPP Release 18;
- 3GPP: Overview of 5G Security Evolution in 3GPP Release 19;
- GSMA: FF.09 Introduction to SMS Fraud;
- GSMA: FS.07 SS7 and SIGTRAN Network Security;
- GSMA: FS.11 SS7 Interconnect Security Monitoring Guidelines;
- GSMA: FS.21 Interconnect Signalling Security Recommendations;
- GSMA: FS.36 5G Interconnect Security;
- GSMA: IR.70 SMS SS7 Fraud;
- GSMA: IR.71 SMS SS7 Fraud Prevention;
- GSMA: IR.82 SS7 Security Network Implementation Guidelines;
- GSMA: SG.22 SMS Firewall Best Practices and Policies;
- ENISA: 5G Threat Landscape for 5G Networks;
- ENISA: Signalling Security in Telecom SS7/Diameter/5G.

Eine weitere Pflicht zur Betrugsbekämpfung in den Signalisierungsnetzen wurde in Artikel 47*g* (Verbot der Vermietung von Global Titles) AEFV aufgenommen.

Art. *96g Abs. 2* Anwendbare Vorschriften, Normen und Aufsicht

In Absatz 2 werden neu auch die Full MVNO aufgeführt. Das BAKOM kann nun neben den Mobilfunkkonzessionärinnen auch sie verpflichten, sich auf eigene Kosten einer Prüfung durch eine qualifizierte Stelle zu unterziehen oder ihre Fernmeldeanlagen überprüfen zu lassen, wenn ein begründeter Verdacht auf einen Rechtsverstoss besteht und dies zur Feststellung des Sachverhalts erforderlich ist.

Art. 108e Übergangsbestimmung zur Änderung vom …

Damit den Mobilfunkkonzessionärinnen sowie den Full MVNO genügend Zeit bleibt, um die geforderten Änderungen gemäss Artikel 96*f* Absatz 2 und 3, insbesondere den Betrieb der Netzbetriebs- und Sicherheitsoperationszentren, in der Schweiz zu betreiben, ist eine angemessene Übergangsfrist vorzusehen. Diese beträgt 24 Monate ab Inkrafttreten der entsprechenden Änderung.

4.2 Verordnung vom 25. November 2015 über Fernmeldeanlagen

Die Artikel 28*b* und 28*c* sind Teil des neuen Abschnitts 1*a* über kritische Netzwerkanlagen im 4. Kapitel der FAV («Besondere Bestimmungen»).

Grundsätzlich betreffen die neuen Sicherheitsmassnahmen die Herstellerinnen von kritischen Netzwerkanlagen, die bestimmt sind für den Betrieb in Fernmeldenetzen, welche für die Erbringung von öffentlichen Fernmeldediensten für Endkunden genutzt werden.

Die Fernmeldeinfrastruktur nach Artikel 48*a* Absatz 2 FMG umfasst allgemein alle Produkte mit digitalen Elementen im Sinne der Cyberresilienz-Verordnung der EU (CRA). Dadurch kann dem Umstand Rechnung getragen werden, dass die Cybersicherheitsanforderungen neu weitgehend horizontal und unabhängig von den betroffenen Branchen ausgestaltet sind. In diesem Zusammenhang ist es sinnvoll, sich auch auf die technischen Normen der europäischen Komitees für Normung zu stützen. In Anbetracht des MRA Schweiz–EU, das Handelshemmnisse zwischen der Schweiz und der EU verhindert, sollte zudem die schweizerische Gesetzgebung über Fernmeldeanlagen und -infrastrukturen mit dem europäischen Recht und mit den Zertifizierungssystemen im Bereich der Cybersicherheit insbesondere für 5G harmonisiert werden, welche die EU-Agentur für Cybersicherheit (*European Network and Information Security Agency*, ENISA) konzipiert hat.

Art. 2 Abs. 1 Bst. c und c^{bis} Begriffe

Zunächst wird der Begriff der Fernmeldeendeinrichtung in Artikel 2 Absatz 1 Buchstabe c FAV präzisiert: Es kann sich um Funkanlagen oder um leitungsgebundene Anlagen handeln, die dazu bestimmt sind, direkt oder indirekt an Schnittstellen von ganz oder teilweise für die Erbringung von Fernmeldediensten genutzten Fernmeldenetzen angeschlossen zu werden. Der Verweis auf Artikel 3 Buchstabe b FMG erübrigt sich und wird gestrichen.

Weiter ist in Artikel 2 Absatz 1 Buchstabe *c^{bis}* FAV der Begriff der kritischen Netzwerkanlage zu definieren, auf die sich die Bestimmungen in diesem neuen Abschnitt beziehen. Es handelt sich um jede Anlage, die Teil eines Netzes ist, das für die Bereitstellung von Fernmeldediensten (vgl. Art. 3 Bst. b FMG) genutzt wird und deren Störung oder Fehlfunktion zu einem Ausfall oder einer erheblichen Beeinträchtigung des Betriebs von Fernmeldeinfrastrukturen führen oder die öffentliche Sicherheit gefährden kann. Es ist Aufgabe der Herstellerin, zum Zeitpunkt des Inverkehrbringens

der Anlage deren bestimmungsgemässe Nutzung zu definieren. Sache der Netzbetreiberin ist es wiederum, Anlagen zu verwenden, die dazu bestimmt sind, in ein Netz integriert und darin betrieben zu werden.

Als Ausfälle oder erhebliche Beeinträchtigungen der Infrastrukturen gelten insbesondere eine weitreichende Panne im Mobilfunknetz (4G/5G), die Anrufe, SMS und den Internetzugang grossflächig verunmöglicht, eine längere Unterbrechung der Notfallnetze, welche die Kommunikation mit den Rettungsdiensten verhindert, grossangelegte Cyberangriffe (z. B. *Denial-of-Service-Angriff*), die die Fernmeldenetze einer Betreiberin lahmlegen, erhebliche physische Schäden (Brand, Überschwemmung, Sabotage) an Telefonzentralen, Glasfaserleitungen oder Relaisstationen oder auch der Ausfall der Signalisierungs- oder Routingsysteme, der weiträumig zu fehlerhafter, verzögerter oder verlorener Kommunikation führt. Ein Angriff auf die öffentliche Sicherheit besteht zum Beispiel dann, wenn Systeme zur Warnung der Bevölkerung (SMS-Alarmierung, Sirenen, Verbreitung über Radio/TV) im Falle einer Naturkatastrophe oder einer unmittelbaren Gefährdung nicht zur Verfügung stehen und so die Information und den Schutz der Bevölkerung verhindern.

Eine Netzwerkanlage unterliegt den Anforderungen nach Artikel 28*b* und Artikel 28*c* FAV, wenn sie zu den kritischen Netzwerkanlagen gehört (das BAKOM führt eine Liste der kritischen Netzwerkanlagen) und für die Integration und den Betrieb innerhalb eines Fernmeldenetzes bestimmt ist.

Art. 28b Grundsätze

Artikel 28*b* Absatz 1 FAV legt das Bewertungsverfahren fest, das den Herstellerinnen ermöglicht, die für kritische Netzwerkanlagen geltenden Sicherheitsanforderungen zu erfüllen. Um den Aufwand möglichst klein zu halten, ist ein Verfahren auf eigene Verantwortung der Herstellerinnen vorgesehen. Letztere bewerten die Konformität ihrer Anlagen mit den Sicherheitsanforderungen und erstellen die technischen Unterlagen, die unter anderem eine Analyse der Sicherheitsrisiken enthalten.

Die Bewertung beruht auf einer international, insbesondere auf europäischer Ebene, anerkannten Methode. Als Referenz dienen kann namentlich die *5G-Toolbox* der EU (Abs. 2). Die Herstellerin legt die technischen Unterlagen einer anerkannten Konformitätsbewertungsstelle zur Beurteilung vor. Anhand der eingereichten technischen Unterlagen und ihrer Analyse entscheidet die Konformitätsbewertungsstelle, ob die Konformität mit den Sicherheitsanforderungen nachgewiesen wurde. Ist dies der Fall, stellt sie eine Konformitätserklärung aus, welche die technischen Unterlagen vervollständigt. Dieses Verfahren ähnelt einem Audit und stützt sich auf ein Verfahren, das für Funkanlagen bereits angewendet wurde und sich bewährt hat. Die Bewertung muss durchgeführt werden, bevor die Anlage in Verkehr gebracht wird.

Gemäss Absatz 3 kann das BAKOM unter Berücksichtigung der internationalen Praxis in der VFAV definieren, welche Anlagen kritische Netzwerkanlagen sind, und unter Beachtung der anerkannten internationalen Normen und Praxis die spezifischen Anforderungen festlegen. In Anhang 8 VFAV werden die kritischen Netzwerkanlagen aufgeführt, die einer Konformitätsbewertung in Bezug auf die Sicherheit zu unterziehen sind. Aufgrund der mit Artikel 48*a* Absatz 2 FMG vorgesehenen Kompetenzdelegation im Bereich der Infrastrukturen kann der Bundesrat diese Regelung der FAV und VFAV auf Infrastrukturen anwenden bzw. ausweiten, die keine Fernmeldeanlagen im engeren

Sinne darstellen. Dabei handelt es sich etwa um Software, elektrische Geräte oder Betriebssysteme und andere Systeme zur Verwaltung der Cybersicherheit (vgl. Anhang 8 VFAV).

Art. 28c *Konformitätserklärung und* technische Unterlagen

Herstellerinnen, die eine Konformitätsbewertung nach Artikel *28b* Absatz 1 FAV durchführen, müssen die technischen Unterlagen während zehn Jahren aufbewahren und sie dem BAKOM auf Verlangen vorlegen können. Diese für das Inverkehrbringen von Industrieprodukten geltende Standarddauer geht aus dem neuen EU-Rechtsrahmen («*New Legislative Framework*» [NLF]) hervor. Die technischen Unterlagen belegen, dass das Produkt die grundlegenden gesetzlichen Anforderungen erfüllt. Während dieser zehn Jahre können die Behörden von der Herstellerin den Nachweis fordern, dass das Produkt zum Zeitpunkt des Inverkehrbringens konform war. Die Marktaufsichtsbehörden können den Zugang zu den Unterlagen unter anderem im Falle eines Audits, nach einem Unfall oder bei Zweifeln an der Konformität eines Produkts verlangen (Abs. 1).

Da dieser Bereich international nicht harmonisiert ist und insbesondere die einzelnen EU-Mitgliedstaaten unterschiedlich vorgehen, kann das BAKOM andere Verfahren als gleichwertig anerkennen. Dabei kann es sich unter anderem um Verfahren handeln, die auf Zertifizierungssystemen beruhen und ein gleichwertiges Sicherheitsniveau gewährleisten wie dasjenige, das in der schweizerischen Gesetzgebung gefordert wird. Es soll vermieden werden, dass eine kritische Anlage, die bereits «sicher» ist, einem erneuten Konformitätsbewertungsverfahren unterzogen wird (Abs. 2).

Die für das Inverkehrbringen verantwortliche Person muss der Betreiberin des Fernmeldenetzes, in das die kritische Anlage integriert ist, eine Kopie der technischen Unterlagen abgeben (Abs. 3).

Art. 44b Übergangsbestimmung zur Änderung vom …

Eine zweijährige Übergangsfrist lässt den Herstellerinnen die notwendige Zeit, um die Konformitätsbewertung der kritischen Netzwerkanlagen vorzunehmen. Bei den Netzwerkanlagen wird für bereits in Netze integrierte Anlagen nur dann eine Konformitätsbewertung verlangt, wenn sie noch auf dem Markt bereitgestellt werden.

4.3 Verordnung vom 6. Oktober 1997 über die Adressierungselemente im Fernmeldebereich

Art. 23 Abs. 2 Bst. a und b Untergeordnete Zuteilungen

Gemäss geltender Vorgabe kann eine Inhaberin eines Nummernblocks ihrerseits Nummern an registrierte Anbieterinnen nach Artikel 4 FMG zum Erbringen von Fernmeldediensten weitergeben und somit unterzuteilen. Obschon entsprechende Unterzuteilungen dem BAKOM im Rahmen der jährlichen Auslastungserhebungen gemeldet werden müssen, zeigt sich im Rahmen der fernmelderechtlichen Aufsicht und auch der Strafverfolgung, dass die Rückverfolgung der Inhaberin bei mehrfach erfolgter Weitergabe (Kaskade) teils schwer oder nicht mehr möglich ist. Dies insbesondere, wenn mehrere Stufen von Unterzuteilungen ins und im Ausland erfolgen.

Seitens BAKOM fällt oftmals ein enormer Aufwand an, diese Kaskaden an Unterzuteilungen nachzuvollziehen und nachzuführen, respektive die Anbieterinnen ins Recht zu

fassen. Die Korrespondenz mit ausländischen Unternehmen ist oftmals sehr aufwändig und selten zielführend. Gegenüber diesen Unternehmen, die sich irgendwo auf der Welt befinden können, ist eine Durchsetzung der fernmelderechtlichen Vorgaben nahezu ausgeschlossen, auch wenn diese aufgrund der Nutzung von schweizerischen Nummern auch dem Schweizer Fernmelderecht unterliegen. Es soll inskünftig nur noch eine einstufige Unterzuteilung von der Nummernblockinhaberin an eine einzige weitere Anbieterin (mit Sitz im In- oder Ausland) möglich sein, damit eine Identifikation der aktuellen Inhaberin jederzeit gewährleistet ist.

Art. 47 Abs. 2, 4 und 5 Zuteilung eines MNC

Absatz 2:

Der Internationale Eisenbahnverband (*Union Internationale des Chemins de fer;* UIC) fördert die Zusammenarbeit und den Austausch zwischen den Eisenbahngesellschaften weltweit. Zu seinen Zielen gehört die Verbesserung der Sicherheit und Effizienz des Schienenverkehrs. Er setzt sich zudem für die Entwicklung technischer Standards und Innovationen ein, die zur Modernisierung der Infrastruktur und der Dienstleistungen beitragen. Durch die Förderung von Innovation trägt der UIC ausserdem zur Integration und Vernetzung des weltweiten Schienennetzes bei.

Um eine sichere und zuverlässige Kommunikation zwischen Zügen und Betriebszentralen zu gewährleisten, hat der UIC in Zusammenarbeit mit verschiedenen europäischen Eisenbahngesellschaften und Mobilfunkanbieterinnen in den 1990 Jahren ein spezielles Funkkommunikationssystem für den Eisenbahnsektor namens *Global System for Mobile Communications – Rail(way)* (GSM-R oder GSM-Rail) geschaffen. Dieses Funkkommunikationssystem basiert auf der damals vorherrschenden GSM-Technologie (2G), die an die spezifischen Anforderungen der Bahnkommunikation und die speziellen Bedürfnisse des Bahnschienenverkehrs angepasst wurde. GSM-R ermöglicht die Übertragung von Sprach- und Datenkommunikation und trägt zur Effizienz und Sicherheit des Bahnschienenverkehrs bei. Es wird weltweit in vielen Ländern eingesetzt, um die Betriebsabläufe zu optimieren und die Interoperabilität zwischen verschiedenen nationalen Eisenbahnsystemen zu gewährleisten.

Die technologische Entwicklung leistungsfähigerer Funkkommunikationssysteme für Bahnanwendungen, die Digitalisierung, die ständig steigenden Anforderungen an Sicherheit, Übertragungsgeschwindigkeit und Datenaustausch zwischen den beteiligten Akteuren im Bahnschienenverkehr sowie die mittelfristige Abschaltung der GSM-Technologie (2G) hat die UIC dazu bewogen, das GSM-R Funkkommunikationssystem durch ein neues Funkkommunikationssystem namens *Future Railway Mobile Communication System* (FRMCS), das die 5G-Mobilfunktechnologie unterstützt, abzulösen.

FRMCS soll bis 2035 voll funktionsfähig sein und bis dahin parallel zu GSM-R betrieben werden. GSM-R soll dabei schrittweise ausser Betrieb genommen werden. Artikel 47 Absatz 2 ist somit anzupassen und das Akronym FRMCS hinzuzufügen, da dieses die neue Mobilfunktechnologie für Eisenbahnnetze definiert.

Absätze 4 und 5:

Im Rahmen des Betriebs ihrer Netze haben die Mobilfunkbetreiberinnen vor mehreren Jahren ein Signalisierungsprotokoll eingeführt und nutzen dieses seither für die Weiterleitung von Nachrichten, die den Austausch verschiedener Informationen (Identifika-

tionsdaten, Zieldaten, SMS-Nachrichten usw.) zwischen den einzelnen Mobilfunkbetreiberinnen ermöglichen. Dieses Signalisierungsprotokoll wurde ohne Sicherheitsvorrichtungen konzipiert, da die Vertrauenswürdigkeit der Netzbetreiberinnen vorausgesetzt wurde. Aufgrund der intrinsischen Schwachstellen des Protokolls können böswillige Nutzerinnen und Nutzer mit Zugang zu den Signalisierungsnetzen heute bestimmte Sicherheitslücken ausnutzen.

Die Fachpresse[24] hat Ereignisse aufgegriffen, bei denen unseriöse Mobilfunkbetreiberinnen das Signalisierungsnetz zu betrügerischen Zwecken nutzen. Angesichts dieser Vorfälle hat die GSMA Verhaltenskodizes[25] verfasst, die in erster Linie darauf abzielen, die Sicherheit, die Vertrauenswürdigkeit und den Schutz der im Mobilfunknetz übermittelten Daten zu gewährleisten. Mit der Übernahme dieser Kodizes verpflichten sich die Betreiberinnen eines Fernmeldenetzes, ihren Grundsätzen entsprechende Massnahmen umzusetzen, zusammenzuarbeiten, um das Vertrauen innerhalb der weltweiten Mobilfunkbranche zu stärken, und die technischen Ressourcen (wie die GT, siehe Ziffer 4.1) nur zu den vorgesehenen Zwecken zu nutzen, ohne rechtswidrige Aktivitäten zu begünstigen.

Vor diesem Hintergrund sieht Absatz 4 vor, dass die in den Absätzen 1 und 1bis genannten Fernmeldedienstanbieter und Betreiber von Telekommunikationsnetzen die erforderlichen technischen, organisatorischen und betrieblichen Massnahmen gegen die missbräuchliche Verwendung eines MNC ergreifen müssen. Sie halten sich dabei an die anerkannten internationalen Normen, Empfehlungen und Praktiken in diesem Bereich, was bedeutet, dass sie die Verhaltenskodizes der GSMA übernehmen müssen (Abs. 4; vgl. auch Art. 96*f*^{bis} Abs. 6 FDV). Das BAKOM kann die erforderlichen technischen und administrativen Vorschriften erlassen, insbesondere bei Bedarf die erforderlichen internationalen Empfehlungen und Praktiken festlegen (Abs. 5).

Art. 47g Global Titles

Absatz 1:

Ein GT dient der Weiterleitung der im Signalisierungsprotokoll verwendeten Signalisierungsnachrichten und stellt so den Informationsaustausch zwischen den verschiedenen Knotenpunkten der Mobilfunknetze sicher. Auf diese Weise können Informationen von Anrufen, SMS, Identifikationsdaten usw. zwischen den Betreiberinnen übermittelt werden. Diese Netzwerkadresse ermöglicht zusammen mit einem MNC, der einer Mobilfunknetzbetreiberin zugeteilt wurde, ein Mobilfunknetz in einem bestimmten Land eindeutig zu identifizieren und Signalisierungsnachrichten über das Signalisierungsnetz der Mobilfunknetze zu übertragen. Dies dient der Verwaltung der Authentifizierung, Standortidentifikation und Rechnungsstellung sowie des Roamings zwischen Mobilfunknetzen einer Betreiberin, der eine Abonnentin oder ein Abonnent oder ein Mobilfunkgerät zugeordnet ist.

Die GT werden von den E.164-Nummern abgeleitet, die das BAKOM den Mobilfunkbetreiberinnen zuteilt. Folglich dürfen nur Fernmeldedienstanbieterinnen, denen Adressierungselemente (Nummernblöcke des Nummerierungsplans E.164 nach Arti-

[24] https://www.lighthousereports.com/investigation/ghost-in-the-network/.

[25] https://www.gsma.com/newsroom/wp-content/uploads//FS.52-v1.0.pdf.

kel 20 AEFV) für die Erbringung von Mobilfunkdiensten zugewiesen wurden, von diesen Elementen abgeleitete GT zur Verwendung in Signalisierungs- und Interkonnektionsnetzen erstellen.

Absatz 2:

Bei der Vermietung von GT handelt es sich um eine Praxis, bei der eine Mobilfunkbetreiberin ihre GT an Dritte (beispielsweise SMS-Aggregatoren oder Unternehmen) vermietet und diesen so ermöglicht, Signalisierungsnachrichten weiterzuleiten, ohne einen eigenen GT zu besitzen. Dadurch müssen diese Dritten keine Investitionen in eine vollständige Infrastruktur tätigen. Diese Praxis birgt jedoch gewisse Risiken, insbesondere im Falle einer potenziell illegalen oder betrügerischen Verwendung der vermieteten GT, bei der mitunter besonders schützenswerte Personendaten offengelegt und die Reputation der Betreiberin, der die GT ursprünglich gehören, geschädigt werden.

Eine unangemessene Verwendung der vermieteten GT ermöglicht namentlich dem Mieter, SMS, einschliesslich Einmalcodes für die Authentifizierung (*One Time Password*, OTP), abzufangen oder zu lesen, indem die Sicherheitslücken des Signalisierungsprotokolls ausgenutzt werden. Ferner ist es dadurch möglich, Abonnentinnen und Abonnenten durch Ausnutzung von Standortanfragen zu Überwachungszwecken zu verfolgen und zu lokalisieren, die Herkunft von Nachrichten zu verschleiern, was Betrug oder Identitätsmissbrauch erleichtert, und die eigene wahre Identität im Signalisierungsnetzwerk zu verbergen. Untersuchungen haben gezeigt, dass eine missbräuchliche Verwendung von GT mit schweren Verbrechen wie Tötungen oder gesetzeswidriger Überwachung in Verbindung gebracht wurde. Die Reglementierung ihrer Nutzung trägt somit zur Bekämpfung solcher Aktivitäten bei.

Absatz 2 bezweckt daher ein Verbot der Vermietung von GT, um so weit wie möglich zu verhindern, dass Lücken im Signalisierungssystem der Mobilfunknetze ausgenutzt werden. Diese Lücken könnten Betrügerinnen und Betrügern oder böswilligen Akteurinnen und Akteuren ermöglichen, Nachrichten und Anrufe abzufangen oder umzuleiten oder Nutzerinnen und Nutzer zu orten. Die betroffenen Betreiberinnen dürfen die GT, die sie von eigenen E.164-Nummern ableiten, folglich nicht an Dritte vermieten. In klar dokumentierten Einzelfällen kann das BAKOM, sofern alle Sicherheitsmassnahmen bei der Verwendung der GT gewährleistet sind, keine anderen Alternativen bestehen und die Nutzung der vermieteten GT den Empfehlungen der GSMA entspricht, Ausnahmen vorsehen und spezifische Regeln dazu erlassen, wie die vermieteten GT verwendet werden müssen.

Diese Massnahmen verringern die Sicherheitsrisiken für die Mobilfunknetze erheblich, indem sie den nicht kontrollierten Zugang zum weltweiten Mobilfunknetz einschränken und so die Möglichkeiten für böswillige Aktivitäten wie das Abfangen von Kommunikation, das unrechtmässige Tracking oder den Versand von Spam reduzieren. Sie sorgen für eine grössere Transparenz und Nachvollziehbarkeit des Signalisierungsverkehrs und erleichtern es so, die heute im Zusammenhang mit der Vermietung von GT festgestellten Missbräuche zu erkennen und zu bekämpfen. Zudem verringern diese Massnahmen die Reputationsrisiken für die Mobilfunkanbieterinnen, die dadurch vermeiden, mit betrügerischen oder gesetzeswidrigen Nutzungen ihrer Ressourcen in Verbindung gebracht zu werden. Die Einschränkung der Vermietung von GT ermöglicht, gegen Betrug vorzugehen, die Sicherheit zu erhöhen und die Integrität und das Vertrauen in das nationale und internationale mobile Ökosystem zu wahren.

Art. 56d Übergangsbestimmung zur Änderung vom …

Absatz 1:

Mit Absatz 1 der Übergangsbestimmungen wird den Anbieterinnen von Fernmeldediensten eine Frist von zwei Jahren ab Inkrafttreten eingeräumt, um mehrstufige Unterzuteilungen rückabwickeln zu können. Die Anbieterinnen, welche Nummern von der Nummernblockinhaberin erhalten und daraus wiederum Nummern unterzugeteilt haben, erhalten diese Frist, um die bestehenden Verträge mit ihren weiteren Partnerinnen zu kündigen und die Unterzuteilungen rückgängig zu machen. Dabei müssen die Nummern an die Nummernblockinhaberin oder die Anbieterin der ersten Stufe der Unterzuteilung übertragen werden. Die Kundinnen und Kunden, welche die Nummern nutzen, sollen somit genügend Zeit erhalten, ein Angebot bei einer dieser beiden Anbieterinnen (Nummernblockinhaberin oder Anbieterin der ersten Stufe) einzuholen oder ganz auf die Nutzung zu verzichten.

Absatz 2:

Anbieterinnen, die vor Inkrafttreten der vorliegenden Verordnung GT an Dritte vermietet haben und keine Bewilligung des BAKOM erhalten haben, sind verpflichtet, die Vermietung innerhalb von 12 Monaten nach Inkrafttreten der vorliegenden Verordnung oder zum nächsten möglichen vertraglich vereinbarten Kündigungstermin zu kündigen, sofern dieser Termin vor dem 27. Mai 2026 vereinbart wurde. Ausnahmegenehmigungsgesuche nach Artikel 47*g* Absatz 2 AEFV müssen innerhalb von 3 Monaten nach Inkrafttreten der vorliegenden Verordnung eingereicht werden. Damit bleibt den Anbieterinnen genügend Zeit, Vertragskündigungen vorzunehmen bzw. ein Gesuch nach Artikel 47*g* Absatz 2 AEFV zu stellen.

Anhang Begriffe und Abkürzungen

Die folgenden Begriffe und Abkürzungen werden neu in das Kapitel «Begriffe und Abkürzungen» der AEFV aufgenommen:

- FRMCS (*Future Railway Mobile Communication System*): Zukünftiges Bahnmobilkommunikationssystem für die europäischen Schienennetze.

- *Global Title*: Netzwerkadresse, die vom Signalisierungsprotokoll zur Weiterleitung von Signalisierungsnachrichten (SMS, Anrufe, andere Mobilfunkdienste) zwischen verschiedenen Betreiberinnen verwendet wird.

5 Auswirkungen

5.1 Auswirkungen auf den Bund

Mit der Umsetzung der geplanten Massnahmen zur Erhöhung der Netzsicherheit und zum Schutz vor Cyberbedrohungen entsteht ein personeller oder finanzieller Mehraufwand für den Bund, welcher mit den bestehenden Ressourcen bewältigt werden kann. Die erforderlichen Arbeiten infolge der vorgeschlagenen Änderungen und Neuerungen können somit durch die bestehenden Personal- und Finanzressourcen im BAKOM getragen werden. Für die Initialphase fallen voraussichtlich keine spezifischen Kosten an. Für allfällige wiederkehrende Aufsichtstätigkeiten fallen pro Jahr voraussichtlich bis zu 270 000 Franken Aufwand an.

5.2 Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete

Die geplante Vorlage hat keine spezifischen finanziellen oder personellen Auswirkungen auf Kantone, Gemeinden, urbane Zentren, Agglomerationen oder Berggebiete.

5.3 Auswirkungen auf die Volkswirtschaft

Die vorgesehenen Anpassungen der Verordnungen entfalten volkswirtschaftliche Wirkungen, die über den sicherheitspolitischen Nutzen hinausreichen. Mit der Verbesserung der technischen und organisatorischen Massnahmen im Bereich der Informations- und Kommunikationstechnologie wird die Widerstandsfähigkeit kritischer digitaler Infrastrukturen erhöht. Eine höhere Systemsicherheit reduziert das Risiko von Unterbrüchen, Cyberangriffen oder technischen Ausfällen, was gesamtwirtschaftlich die Kontinuität zentraler staatlicher und privatwirtschaftlicher Leistungen stärkt. Dies insbesondere durch zeitgemässe Sicherheitsstandards und klare Zuständigkeiten für den Betrieb kritischer IT-Infrastrukturen. Stabil funktionierende digitale Dienste wirken sich positiv auf die Standortattraktivität aus und schaffen verlässliche Rahmenbedingungen für Unternehmen, die auf sichere Daten- und Kommunikationsinfrastrukturen angewiesen sind. Gleichzeitig fördert die verbesserte Resilienz das Vertrauen von Bevölkerung, Wirtschaft und internationalen Partnern in staatliche digitale Dienstleistungen, was Transaktionskosten senkt und die Effizienz erhöht.

Die Regulierungskosten nach Artikel 5 UEG, die den betroffenen Unternehmen durch die neuen Sicherheitsanforderungen im Mobilfunkbereich entstehen, lassen sich nur schwer präzise berechnen oder abschätzen. Dies hängt insbesondere damit zusammen, dass die Betreiberinnen sehr unterschiedlich organisiert sind und viele der vorgeschlagenen Sicherheitsmassnahmen bereits teilweise umgesetzt haben. Zudem beeinflussen sich technische und organisatorische Faktoren gegenseitig, was eine einheitliche Bewertung zusätzlich erschwert. Für eine präzise Ermittlung der Kosten wären Einzelbefragungen sämtlicher Unternehmen nötig. Ein solches Vorgehen würde sowohl die Firmen als auch die Behörden erheblich belasten und letztlich zu einer Vielzahl von Einzelfallbeurteilungen führen. Für ein solches Verfahren stehen weder die benötigte Zeit noch die erforderlichen personellen Ressourcen zur Verfügung. Den grössten Einfluss auf die regulatorischen Zusatzkosten haben mit hoher Wahrscheinlichkeit die Massnahmen im Bereich NOC und SOC. Auf Basis einer groben Annahme ist mit Kosten von bis zu 2 Millionen Franken pro Jahr und Mobilfunkanbieterin zu rechnen. Dabei handelt es sich primär um Personalkosten. Während die Unternehmen zwar alle mit denselben Anforderungen und je nach aktueller Situation mit zusätzlichen Kosten konfrontiert werden, kann davon ausgegangen werden, dass diese zusätzlichen Kosten positive Effekte für die Arbeitnehmenden entfalten, weil Arbeitsplätze in die Schweiz verlagert werden.

Die neuen Anforderungen an die Betreiberinnen von Mobilfunknetzen führen zudem dazu, dass Sicherheitsstrategien überarbeitet und teilweise erheblich ausgeweitet werden müssen. Insbesondere im Zusammenhang mit der Weiterentwicklung hin zu echten 5G-Kernnetzen ist sehr wahrscheinlich mit zusätzlichen Investitionen zu rechnen. Diese können kurzfristig zu Mehrkosten führen, mittelfristig jedoch den technologischen Wandel beschleunigen, indem Anreize geschaffen werden, veraltete und kostenintensive Technologien wie z.B. 3G schneller ausser Betrieb zu nehmen. Volkswirtschaftlich wirken solche Modernisierungsschritte dämpfend auf langfristige Betriebs- und Wartungskosten und steigern die Innovations- und Wettbewerbsfähigkeit des gesamten Sektors.

Die Gleichbehandlung von Mobilfunkkonzessionärinnen und Full MVNO kann in Einzelfällen dazu führen, dass das Geschäftsmodell der Full MVNO beeinträchtigt wird. Da dadurch aber faire Wettbewerbsbedingungen geschaffen und gleichzeitig Risiken reduziert werden, rechtfertigt sich eine Gleichbehandlung aus gesamtwirtschaftlichen Kosten-Nutzen-Überlegungen. Letztlich werden dadurch vorhandene Marktverzerrungen beseitigt. Anbieterinnen sollen keine Wettbewerbsvorteile daraus ziehen können, dass sie auf sicherheitsrelevante Massnahmen verzichten. Dies stärkt das Vertrauen der Konsumentinnen und Konsumenten, die unabhängig von der Anbieterin auf sichere Dienstleistungen angewiesen sind. Ein funktionierender und transparenter Telekommunikationsmarkt bildet eine wesentliche Grundlage für wirtschaftliche Stabilität und die verlässliche Bereitstellung kritischer digitaler Dienste, insbesondere vor dem Hintergrund der zunehmenden Abhängigkeit von digitalen Wertschöpfungsketten.

Die Pflicht, eine Konformitätsbewertung für kritische Netzwerkanlagen durchzuführen gilt für die (meist internationalen) Hersteller, deren Anzahl maximal im tiefen zweistelligen Bereich geschätzt wird, und wird deren Aufwand erhöhen. Der zusätzliche zeitliche Aufwand ist schwierig abzuschätzen, dürfte sich aber für eine grosse Herstellerin mit vielen angebotenen Produkten mit grosser Wahrscheinlichkeit auf maximal eine Vollzeitstelle belaufen. Die Vorgaben des vorliegenden Entwurfs orientieren sich an der Entwicklung der internationalen Rahmenbedingungen, wodurch ein Grossteil dieser zusätzlichen Kosten für die Hersteller ohnehin anfällt. Zudem entstehen auf Seiten der Mobilfunkbetreiber Mehrkosten, weil die Projekte für den Netzausbau länger dauern werden. Gleichzeitig erhöht eine konsequente sicherheitstechnische Überprüfung die Wahrscheinlichkeit, dass Infrastrukturen langfristig ohne gravierende Störungen betrieben werden können. Eine höhere Zuverlässigkeit reduziert gesamtwirtschaftliche Risiken wie Produktionsausfälle, Datenverluste oder Versorgungsengpässe und wirkt stabilisierend auf vernetzte Wirtschaftsprozesse. Werden dabei schwerwiegende Kompromittierungen entdeckt, können zwar weitere Kosten entstehen; zugleich wird verhindert, dass unsichere Systeme in Betrieb gehen und potenziell wesentlich höhere volkswirtschaftliche Schäden verursachen.

Insgesamt stärken die vorgesehenen Massnahmen die digitale Souveränität der Schweiz, fördern stabile und faire Marktbedingungen und reduzieren sicherheitsbedingte Risiken für Wirtschaft und Gesellschaft. Die daraus resultierenden volkswirtschaftlichen Effekte zeigen sich in Form erhöhter Sicherheit, verbesserter Effizienz und einer langfristigen Stärkung des Wirtschaftsstandorts Schweiz.

5.4 Auswirkungen auf die Gesellschaft

Mit den beantragten Neuregelungen wird der Schutz der Endkundendaten verbessert. Auch führt die Vorlage zu einer höheren Ausfallsicherheit der Fernmeldeanlagen. Die Auswirkungen auf die Gesellschaft, insbesondere auf die Endkundinnen und Endkunden der Mobilfunknetze, sind als positiv zu betrachten. Beispielsweise werden durch die Beschränkung der Vermietung von GT auf Mobilfunkanbieterinnen oder Betreiberinnen von Telekommunikationsnetzen missbräuchliche Nutzungen wie der Massenversand von Spam-Nachrichten, «*Smishing*» oder betrügerischer SMS-Verkehr, der die Reputation des legitimen GT nutzt, eingeschränkt. Daher wird es bei missbräuchlicher oder unangemessener Nutzung einfacher sein, die fehlbare Betreiberin zu identifizieren und Massnahmen zu ergreifen, um die Aktivitäten der beteiligten Stellen zu beschränken oder zu stoppen und so Abonnentinnen und Abonnenten oder Konsumentinnen und Konsumenten zu schützen.

Die Konsumentinnen und Konsumenten werden durch die Anpassung der Bestimmung zur Übermittlung von Nummern besser vor betrügerischen, unlauteren und lästigen

Anrufen geschützt. Hingegen sehen sich Konsumentinnen und Konsumenten durch die Neuregelung betreffend Unterzuteilung allenfalls gezwungen, die Anbieterin zu wechseln, beziehungsweise ihre Nummer zu einer anderen Anbieterin portieren zu lassen.

5.5 Andere Auswirkungen

Auswirkungen auf die Umwelt oder andere Auswirkungen sind nicht zu erwarten.

6 Rechtliche Aspekte

6.1 Delegation von Rechtsetzungsbefugnissen und Erlassform

Mit den vorliegenden Bestimmungen wird insbesondere Artikel 48*a* Absatz *2* Buchstaben a und b sowie Artikel 28 Absatz 6 Buchstaben a und d FMG umgesetzt. Diese Bestimmungen räumen dem Bundesrat zum Schutz vor Gefahren, zur Vermeidung von Schäden und zur Minimierung von Risiken die Möglichkeit ein, Regelungen über die Sicherheit von Informationen, von Fernmeldeinfrastrukturen und -diensten sowie Adressierungselementen zu erlassen. Der Bundesrat kann insbesondere Bestimmungen erlassen bezüglich Verfügbarkeit, Betrieb, Sicherstellung von redundanten Infrastrukturen, Meldung von Störungen, Nachvollziehbarkeit von Vorgängen und Umleitung oder Verhinderung von Verbindungen sowie Unterdrückung von Informationen nach Absatz 1. Diese Gesetzesbestimmung gibt dem Bundesrat einen relativ grossen Spielraum der Bereiche, in denen er legiferieren kann.

Die vorliegenden Bestimmungen stützen sich zudem auf die nach den Artikeln 31 Absatz 1, 32, 32*a* und 33 Absatz 2 FMG vorgesehenen Kompetenzdelegationen. Auf dieser Grundlage kann der Bundesrat Vorschriften über das Importieren, das Anbieten, das Bereitstellen auf dem Markt und die Inbetriebnahme von Fernmeldeanlagen festlegen, insbesondere hinsichtlich grundlegender Anforderungen im Bereich der technischen Sicherheit und der Konformitätsbewertung.

Die Vorlage enthält rechtsetzende Bestimmungen, die nach Artikel 182 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999[26] (BV) in Form einer Bundesratsverordnung soweit er durch Verfassung oder Gesetz dazu ermächtigt ist, zu erlassen sind. Mit diesen im vorliegenden Revisionsprojekt angepassten Verordnungsbestimmungen nutzt der Bundesrat die Kompetenz, in den Bereichen Sicherheit von Fernmeldeanlagen sowie Verfügbarkeit und Betrieb von sicherheitsrelevanten Fernmeldeinfrastrukturen, Bestimmungen zu erlassen. In Artikel 62 Absatz 2 FMG (siehe auch Art. 105 Abs. 1 FDV und 41 Abs. 1 FAV) ist vorgesehen, dass der Bundesrat dem BAKOM die Aufgabe übertragen kann, die notwendigen technischen und administrativen Vorschriften zu erlassen. Dabei muss das BAKOM die international geltenden Normen berücksichtigen.

6.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Die Vorlage schafft keine Unvereinbarkeit mit den internationalen Verpflichtungen der Schweiz. So fallen namentlich die geplanten Massnahmen für Netzwerkanlagen nicht unter das Abkommen zwischen der Schweiz und der EU über die gegenseitige Anerkennung von Konformitätsbewertungen[27] und stellen somit keine technischen Handelshemmnisse dar. Die Vorlage ist damit mit den internationalen Verpflichtungen der Schweiz, die aus dem MRA Schweiz-EU resultieren, vereinbar.

[26] SR **101**

[27] SR **0.946.526.81**

Die Pflicht nach Artikel 96*f* Absatz 2 FDV, bestimmte Infrastrukturen oder Betriebszentren aus Gründen der technischen Sicherheit in der Schweiz anzusiedeln, ist gemäss der Artikel XIV Buchstabe a (Schutz der öffentlichen Ordnung), XIV Buchstabe c iii und XIV^{bis} (Sicherheit) des GATS (siehe entsprechende Ausführungen zu Art. 96*f* Abs. 2) zulässig. Das gilt auch für die neuen Sicherheitsanforderungen für Fernmeldeanlagen gemäss Artikel XIV Buchstabe a Ziffer i (Sicherheit) des Anhangs 1A des Abkommens zur Errichtung der WTO (Allgemeines Zoll- und Handelsabkommen, GATT) sowie der Artikel 2.10, 5.4 und 5.7 (Nationale Sicherheit) des Anhangs 1A.6. de l'Accord instituant l'OMC (*Accord sur les obstacles techniques au commerce* OTC).

6.3 Unterstellung unter die Ausgabenbremse

Mit der Vorlage werden weder neue Subventionsbestimmungen noch neue Verpflichtungskredite oder Zahlungsrahmen beschlossen. Die Vorlage ist somit nicht der Ausgabenbremse (Art. 159 Abs. 3 Bst. b BV) unterstellt.

6.4 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz

Das Subsidiaritätsprinzip und das Prinzip der fiskalischen Äquivalenz sind von der Vorlage nicht betroffen.

6.5 Datenschutz

Die geplanten Massnahmen wurden datenschutzrechtlichen Risikovorprüfungen unterzogen. Das Ausmass der vorgesehenen Datenbearbeitung erfordert keine weitergehende Datenschutzfolgeabschätzung.

6.6 Abkürzungsverzeichnis

BAKOM	Bundesamt für Kommunikation
BJ	Bundesamt für Justiz
ComCom	Eidgenössische Kommunikationskommission
ENISA	European Network and Information Security Agency
EU	Europäische Union
Full MVNO	Full Mobile Virtual Network Operator
GSMA	GSM Association
GT	Global Title
MNC	Mobile Network Code
NCS	Nationale Cyberstrategie
BACS	Bundesamt für Cybersicherheit
RAN	Radio Acess Network
TAV	Technische und administrative Vorschriften
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation

6.7 Literaturverzeichnis

Bundesrat (2023a): Nationale Cyberstrategie (NCS), https://www.newsd.admin.ch/newsd/message/attachments/76793.pdf, 04.2023.

Bundesrat (2023b): Nationale Strategie zum Schutz kritischer Infrastrukturen, https://www.babs.admin.ch/de/ski, 16.06.2023.

NCS (2023): Ziel: Sichere und verfügbare digitale Dienstleistungen und Infrastruktur, https://www.ncsc.admin.ch/ncsc/de/home/strategie/ziele-massnahmen/ncs-ziel-sichere-verfuegbare-digitale-dl-infrastruktur.html, letztmals abgerufen am 01.05.2026.

EU (2020): Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures, 23.01.2020.