

Generelle Bemerkungen zu den Änderungen der FDV

Eher Ablehnung

Wir unterstützen das generelle Ziel, die Cybersicherheit und die Widerstandsfähigkeit der Fernmeldeinfrastrukturen zu verbessern sowie den Schutz vor Cyberbedrohungen zu erhöhen. Zu diesem Zweck sind neue Sicherheitsmassnahmen vorgesehen. Die gesetzliche Erfassung der Mobilfunkanbieterinnen im Modell Full MVNO sowie deren grundsätzliche Gleichbehandlung mit den Mobilfunkkonzessionärinnen bezüglich Sicherheitsvorgaben ist sachgerecht, insofern diese Anbieterinnen über eigene Mobilfunkinfrastruktur verfügen und diese betreiben. Für die mitbenutzten Infrastrukturteile können sie naturgemäss die Verantwortung nicht übernehmen. Die anlässlich dieser Ergänzungen mitangepasste Vorschrift zur Standortpflicht in der Schweiz lehnen wir jedoch ab. Die geplante Vorschrift ist unverhältnismässig, da sie keinen ersichtlichen Sicherheitsgewinn bringt. Sollte an der Vorgabe jedoch festgehalten werden, sind lange Übergangsfristen vorzusehen.

Für unsere konkreten Änderungsanträge verweisen wir auf die detaillierte Stellungnahme zu den Verordnungen. Keine Bemerkungen haben wir zu den geänderten Bestimmungen, die wir nicht kommentieren.

Detaillierte Stellungnahme FDV (Änderungsanträge)

Betrieb sicherheitskritischer Fernmeldeanlagen: Art. 96f Abs. 2 E-FDV

Ablehnung

Begründung:

Absatz 2: Im erläuternden Bericht wird auf Seite 16 (Mitte) angeführt, dass die Schweizer Mobilfunkinfrastruktur durch eine neue zwingende Standortpflicht für Netzbetriebszentren (NOC) und Sicherheitsoperationszentren (SOC), etc. in der Schweiz sicherer werde. Warum dem so sein soll, wird hingegen nicht weiter ausgeführt. Durch die neue Vorgabe soll der Datenschutz, die Datensicherheit sowie die Kontroll- und Handlungsfähigkeit gestärkt werden (vgl. erläuternder Bericht, Seite 6, oben).

Das Geschäftsmodell von Full MVNO unterscheidet sich hinsichtlich der Betriebsstruktur grundsätzlich von jenem einer Mobilfunkkonzessionärin mit eigenem RAN (Funkzugangsnetz). Um erfolgreich am Markt zu sein, sind Full MVNO oft auf grenzüberschreitend organisierte Betriebsmodelle angewiesen. Wie der erläuternde Bericht richtig anführt, würde eine starre Vorgabe in Bezug auf den Standort von NOC (Netzbetriebszentren) und SOC (Sicherheitsoperationszentren), etc., in vielen Fällen zu einer Beeinträchtigung des Geschäftsmodells von Full MVNO führen. Dies gefährdet die Anbietervielfalt in der Schweiz, und überdies auch rein schweizerische Anbieterinnen, die zur betriebswirtschaftlichen Optimierung ihres Mobilfunkangebots allenfalls auch grenzüberschreitende Dienste nutzen. Alle MVNO leisten einen wichtigen Beitrag zur Angebotsvielfalt und zum funktionierenden Wettbewerb im Mobilfunkmarkt in der Schweiz. Mobilfunkangebote auf MVNO-Basis befinden sich regelmässig auf den vordersten Plätzen bei Kundenzufriedenheits-Umfragen (vgl. beispielsweise kürzlich bei Comparis.ch).

Der erläuternde Bericht bleibt sehr vage bei der Begründung, warum die bisherige Regelung von Art. 96f Abs.

2 FDV in Bezug auf Sicherheitsbelange der Infrastruktur nicht mehr ausreichend sein sollte. Das Ziel, den Datenschutz und die Datensicherheit zu erhöhen, ist zwar nachvollziehbar; es lässt sich aber auch durch eine mildere Massnahme erreichen: Dazu könnte die Vorgabe von Art. 96f Abs. 2 FDV weiter auf Länder eingegrenzt werden, die der europäischen Datenschutzgrundverordnung (DSGVO) unterliegen, was Länder im EU- und EWR-Raum einschliessen würde. Da die DSGVO allgemein als strenge Datenschutzregulierung gilt, wäre dies als eine Verstärkung des Datenschutzes und der Datensicherheit - somit als eine strengere Bedingung - zu betrachten.

Zum anderen wird im erläuternden Bericht das allgemeine und abstrakte Ziel einer besseren Kontroll- und Handlungsfähigkeit bezüglich kritischer Infrastrukturen angeführt. Was dies im Detail bedeutet und inwiefern dies nach Umsetzung der Bedingungen der Fall wäre, wird jedoch nicht weiter substantiiert. Wenn eine Full MVNO alle Sicherheitsanforderungen in ihrem Mobilfunknetz umsetzt, ist nicht ersichtlich, warum Standorte, die sich physisch auf EU- oder EWR-Gebiet befinden, nicht auch einbezogen werden dürften. Entscheidend kann nur sein, ob die gewählte Gesamtarchitektur, auch unter Einbezug von Georedundanzen, ein ausreichendes Niveau in Bezug auf Verfügbarkeit, tatsächliche Kontrolle, Datenschutz, Datensicherheit, Kontrolle über Verschlüsselungen und Konfigurationen, vollständige Auditierbarkeit sowie Krisenfestigkeit ausweist. Dies wird nicht durch eine formale Anforderung erreicht, alle essentiellen Betriebsfunktionen in der Schweiz zu betreiben. Sodann ist mit Blick auf Absatz 3 nicht nachvollziehbar, warum zur Gewährleistung der Betriebskontinuität - also in einem Störfall in der Schweiz - redundante Systeme im Ausland vorgesehen werden dürfen. Es müsste konzeptionell gerade umgekehrt sein.

Zusammenfassend bestehen aus unserer Sicht keine hinreichenden sicherheitstechnische Gründe für eine derart folgenreiche Änderung der Vorgaben zum örtlichen Betrieb von SOC und NOC, etc. Zweck des vorliegenden Verordnungsprojektes ist die Erhöhung der Sicherheit von Fernmeldeinfrastrukturen und -diensten und der Schutz vor Cyberbedrohungen (vgl. erläuternder Bericht, Ausgangslage). Es besteht jedoch keine Kompetenz des Bundesrates auf Verordnungsebene, den Wettbewerb durch die Beseitigung von Marktverzerrungen zu beeinflussen, wie dies als positiver Nebeneffekt für die neu geplanten Standortvorgaben angeführt wird (vgl. erläuternder Bericht, Seite 30, oben). Zudem sei daran erinnert, dass die Mobilfunkkonzessionärinnen von Gesetzes wegen nicht dazu verpflichtet sind, ein Full MVNO auf ihren Netzen zuzulassen. Demgegenüber müsste also klar ausgewiesen sein, dass strengere Standortvorgaben wirklich einen zusätzlichen Sicherheitsgewinn zur Folge haben. Daran mangelt es aber vorliegend. Wie angeführt, sehen wir allein eine allgemeine Anhebung des datenschutzrechtlichen Schutzniveaus durch eine weitere Eingrenzung der Standortstaaten als sachgerecht an.

Unter Berücksichtigung unseres Vorschlages wäre zudem gewährleistet, dass unser Mitglied, die Telecom Liechtenstein AG, den geplanten Betrieb als Full MVNO in der Schweiz aufnehmen könnte. Hierfür wurde eine georedundante Mobilfunk-Core-Architektur mit Standorten in Zürich und Vaduz aufgebaut. Liechtenstein gehört formell zwar nicht zum Schweizer Staatsgebiet, die tiefgehenden und vielfältigen staatsvertraglichen Beziehungen, die bestehenden gesellschaftlichen Verflechtungen, die tief verankerte Zusammenarbeit der Verwaltung und Administration, die teilweise identischen Rechtsgrundlagen, die zum Teil institutionelle Anerkennung von Schweizer Behörden (beispielsweise des BAKOM bei der Vertretung des Liechtensteinischen Amtes für Kommunikation in internationalen Gremien) und Organisationen (beispielsweise der schweizerischen Verwertungsgesellschaften im Bereich der Kollektivverwertung von Urheberrechten und verwandte Schutzrechten) und nicht zuletzt auch die gleiche Währung und das gemeinsame Zollgebiet, machen Liechtenstein gleichwertig zur Schweiz. Als EWR-Staat hat Liechtenstein auch die DSGVO übernommen. Würden weitergehend auch geopolitische Überlegungen angestellt, um sogar einen physischen Zugriff auf Betriebseinrichtungen in benachbarten Staaten in jeglicher Form auszuschliessen, müsste für Liechtenstein aufgrund des eng verflochtenen Wirtschafts- und Rechtsraums eine Ausnahme gelten. Als zugelassenen Standort würde Liechtenstein eine geografische Resilienz sogar eher stärken.

Sollte im Grundsatz an den neuen Standortvorgaben festgehalten werden, wäre aufgrund von Verhältnismässigkeitsüberlegungen eine differenzierte Regelung vorzusehen, die sich nach der Größe und der wirtschaftlichen Bedeutung der FDA richtet. Denn gerade bei kleineren Full MVNO verursachen starre Vorgaben zur Ausgestaltung des Betriebsmodells erhebliche Fix- und Zusatzkosten. Diese fallen unabhängig von Kundenzahl und Marktanteilen an.

Änderungsantrag:

² Die Mobilfunkkonzessionärinnen und die Full MVNO betreiben ihre Netzbetriebszentren (Network Operations Center [NOC]), ihre Sicherheitsoperationszentren (Security Operations Center [SOC]) sowie die für den Betrieb, die Steuerung und die Verwaltung ihrer Netze wesentlichen Fernmeldeanlagen ausschliesslich in der Schweiz oder in Staaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraumes (EWR).

Sicherheitsmassnahmen: Art. 96f^{bis} Abs. 2	Ablehnung
---	------------------

Begründung:

Absatz 2: Gemäss der geplanten Vorgabe müssen auf allen Hard- und Softwarekomponenten sämtliche standardisierten Sicherheitsoptionen installiert und aktiviert werden. Welche Sicherheitsoptionen sinnvollerweise installiert und aktiviert sein sollten, hängt jedoch vom jeweiligen konkreten Einsatz- und Nutzungsbereich ab. Die starre Vorschrift, sämtliche Sicherheitsoptionen in jedem Fall zu installieren und zu aktivieren, ist daher nicht sachgerecht. Wir beantragen deshalb, die aus unserer Sicht bessere Formulierung des neuen Art. 48b des Vorentwurfs zum FMG zu übernehmen.

Absatz 4: Die von der Schweizer Telekommunikationsbranche entwickelten Best Practices sind international anerkannt und gehören zu den führenden Standards. Die FDA pflegen bereits heute einen intensiven Austausch untereinander sowie mit dem Bundesamt für Cybersicherheit (BACS) zu allfälligen Schwachstellen und Angriffsmustern. Es ist richtig, diesen Informationsaustausch weiter zu fördern und auszubauen. Die Bestimmung in Absatz 4 bezieht sich auf die Mobilfunkkonzessionärinnen und Full MVNO, wobei auch die Festnetzbetreiberinnen je nach Gegenstand über gewonnene Erkenntnisse unter Wahrung von Vertraulichkeit, Geheimnis- und Datenschutz auf dem Laufenden gehalten werden sollten. Diese Informationen sollten idealerweise zentral gebündelt und koordiniert werden, wobei ganz allgemein ein «Single Entry Point» für solche Themen, Anliegen, Vorfälle und Meldungen geschaffen werden sollte, wie es im Übrigen auch die vom Parlament angenommene Motion Nr. 25.4715 für die Erfüllung der diversen Meldepflichten fordert.

Änderungsantrag:

² Sie müssen sicherstellen, in ihren Netzen Hard- und Softwarekomponente in Betrieb zu nehmen, die nicht gefährdet sind. ~~Sie müssen alle standardisierten Sicherheitsoptionen installieren und implementieren. Die Sicherheitseinstellungen müssen standardmässig konfiguriert und aktiviert sein und auf dem neusten Stand gehalten werden.~~

Übergangsbestimmung: 108e	Ablehnung
----------------------------------	------------------

Begründung:

Wir beantragen vorstehend die Änderung von Art. 96f Abs. 2 E-FDV. Sollte an der geplanten Vorschrift zum Standort von NOC und SOC etc. festgehalten werden, so muss eine deutlich längere Umsetzungsfrist vorgesehen werden. Für diesen Fall beantragen wir eine Erhöhung der Übergangsfrist auf 60 Monate.

Änderungsantrag:

¹ Die Mobilfunkkonzessionärinnen und die Full MVNO müssen die Anforderungen nach Artikel 96f Absätze 2 und 3 spätestens ~~24~~ 60 Monate nach Inkrafttreten dieser Verordnung erfüllen.

Detaillierte Stellungnahme FAV (Änderungsanträge)

Begriffe: Art. 2 Abs. 1 Bst. c^{bis}	Ablehnung
---	------------------

Begründung:

Bei der Beurteilung, ob eine Fernmeldeanlage als kritisch einzustufen ist, sollte unbedingt auf internationale Standards Rücksicht genommen und entsprechende Fachgremien für die Beurteilung hinzugezogen werden. Die Auswirkungen eines Ausfalls einer kritischen Anlage müssen von erheblicher Tragweite sein und dürfen nicht nur zu teilweisen oder lokal begrenzten Betriebsbeeinträchtigungen führen. Dies wird durch die Beispiele im erläuternden Bericht (vgl. Seite 23) verdeutlicht. Entsprechend sollte die Definition präzisiert und ergänzt werden.

Die Einführung des Begriffs auf Verordnungsstufe, verbunden mit spezifischen Konformitäts-, Nutzungs- und Sicherheitsanforderungen, deren nähere Bestimmung in die Kompetenz des BAKOM fallen soll (vgl. Art. 28b Abs. 3 sowie Anhang 8 zu Art. 8a E-VFAV), sowie die daraus abgeleiteten Vorschriften, können für die Netzbetreiberinnen und Herstellerinnen erhebliche Auswirkungen haben. Art. 48a FMG bildet zwar eine allgemeine Grundlage für Massnahmen gegen die unbefugte Manipulation von Fernmeldeanlagen und für technische Schutzmassnahmen. Er enthält jedoch keine hinreichend bestimmte Delegation zur Schaffung einer neuen, eigenständigen Kategorie «kritischer Netzwerkanlagen» mit weitreichenden regulatorischen Folgen für Betreiberinnen und Herstellerinnen. Unseres Erachtens sollten deshalb die Grundzüge der Regelung stufengerecht im Gesetz festgelegt werden. Dies würde der bundesgerichtlichen Rechtsprechung entsprechen, wonach wesentliche fernmelderechtliche Pflichten einer genügenden Grundlage im formellen Gesetz bedürfen. Gleichzeitig könnte auch präzisiert und geklärt werden, wie dieser Begriff zu dem mit der Teilrevision des FMG auch vorgesehenen Begriff der «kritischen Bestandteile einer Fernmeldeinfrastruktur» steht (falls der Begriff im Gesetzesentwurf weiterhin verwendet werden sollte).

Änderungsantrag:

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

Grundsätze: Art. 28b Abs. 3	Ablehnung
------------------------------------	------------------

Begründung:

Das BAKOM soll die Möglichkeit erhalten, die Sicherheitsanforderungen an diese kritischen Netzwerkanlagen festzulegen und eine Liste der Anlagen zu erstellen, die diese Anforderungen erfüllen. Im erläuternden Bericht (Seite 23) wird hierzu auf international anerkannte Methoden verwiesen. Aus unserer Sicht bringt eine vom BAKOM geführte Liste keinen zusätzlichen Mehrwert. Zudem ist fraglich, ob damit rasch und flexibel genug

auf technische Entwicklungen und neue Bedrohungen reagiert werden kann. Die Einhaltung international anerkannter Sicherheitsstandards und Best Practices ist aus unserer Sicht ausreichend. Absatz 3 ist entsprechend anzupassen.

Änderungsantrag:

³ ~~Das BAKOM kann eine Liste dieser Anlagen erstellen und die spezifischen Anforderungen unter Berücksichtigung der anerkannten internationalen Normen und Praxis festlegen. Die spezifischen Sicherheitsanforderungen entsprechen anerkannten internationalen Normen und Best Practices.~~

Übergangsbestimmung zur Änderung vom ...: Art. 44b	Ablehnung
---	------------------

Begründung:

Sollte eine bereits im Betrieb befindliche Anlage ersetzt werden müssen, könnte eine Übergangsfrist von zwei Jahren je nach Art der Anlage nicht ausreichend sein. Dies gilt beispielsweise für Elemente des Core-Netzes. Aus Sicht unserer Mitglieder ist eine Frist von fünf Jahren realistisch.

Änderungsantrag:

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

Detaillierte Stellungnahme VFAV (Änderungsanträge)

Kritische Netzwerkanlagen: Art. 8a	Ablehnung
---	------------------

Begründung:

Aufgrund des Antrags zu Art. 28b Abs. 3 E-FAV ist der vorliegende Verweis auf Anhang 8 zu streichen.

Änderungsantrag:

~~Die kritischen Netzwerkanlagen im Sinn von Art. 28b FAV sind in Anhang 8 aufgeführt.~~

Anhang 8	Ablehnung
-----------------	------------------

Begründung:

In Anhang 8 zur Verordnung sollen gemäss Art. 8a die kritischen Netzwerkanlagen aufgeführt werden. Wir beantragen die Streichung der Delegationsnorm in Art. 28b Abs. 3 E-FAV sowie des Verweises auf Anhang 8 in Art. 8a E-VFAV und beantragen deshalb auch die ersatzlose Streichung von Anhang 8.

Nach der Definition in Art. 2 Bst. c^{bis} FAV, der 5G-Toolbox der EU und internationaler und europäischer Praxis gelten primär das Core-Netz, zentrale Transportnetze sowie netzsteuernde Sicherheits- und Managementfunktionen als kritische Netzwerkanlagen. Das Funkzugangsnetz (RAN) wird hingegen nicht als kritische Komponente eingestuft. Die vorgeschlagene Liste würde also teilweise sogar über die europäische Praxis hinausgehen. Und selbst in Bezug auf das Kernnetz unterscheiden sich die europäischen Ansätze erheblich. Mehrere

Mitgliedstaaten erlauben weiterhin auch den Einsatz «heikler» Lieferanten in sämtlichen oder einzelnen Teilen des Kernnetzes, sofern technische und organisatorische Sicherheitsmassnahmen eingehalten werden.

Eine Präzisierung der kritischen Netzwerkanlagen in der VFAV sollte unbedingt eng an die entsprechende Definition – vorzugsweise im Gesetz – angelehnt sein und sich auf Anlagen beschränken, deren Störung oder Fehlfunktion zu einem systemweiten Ausfall, einer erheblichen Beeinträchtigung des Betriebs von Fernmeld-einfrastrukturen oder einer Gefährdung der öffentlichen Sicherheit führen kann.

Änderungsantrag:

Streichung von Anhang 8
