Swico
Lagerstrasse 33
CH-8004 Zürich

Tel.: +41 44 446 90 90
www.swico.ch
info@swico.ch

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

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

Zürich, 17.09.2026

Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit & Erhöhung der Netzsicherheit und Schutz vor Cyberbedrohungen (Teilrevision der Verordnungen im Fernmeldebereich)

Sehr geehrter Herr Bundesrat Rösti
Sehr geehrte Damen und Herren

Gerne nehmen wir die Möglichkeit wahr, zu den beiden Teilrevisionen 2026/38 «Fernmeldegesetz (FMG) im Bereich Sicherheit» und 2026/39 «Erhöhung der Netzsicherheit und Schutz vor Cyberbedrohungen» Stellung zu nehmen. In diesem Dokument äussern wir uns gebündelt zu beiden Vernehmlassungen.

Swico ist der Wirtschaftsverband der Digitalindustrie und vertritt die Interessen etablierter Unternehmen sowie Start-ups in Politik, Wirtschaft und Gesellschaft und betreibt das nationale Rücknahmesystem «Swico-Recycling» für Elektro- und Elektronikgeräte. Swico zählt über 750 Mitglieder aus der ICT- und Internetbranche. Diese Unternehmen beschäftigen rund 60'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von über 40 Milliarden Franken.

Zusammenfassung:

Swico anerkennt die sicherheitspolitische Zielsetzung der Vorlage. Der Schutz von Fernmeldeinfrastrukturen vor Cyberbedrohungen ist für eine sichere, leistungsfähige und vertrauenswürdige digitale Schweiz von zentraler Bedeutung. Swico unterstützt deshalb eine Weiterentwicklung der regulatorischen Rahmenbedingungen, sofern diese wirksam, risikobasiert, technologieneutral, verhältnismässig, international anschlussfähig und wirtschaftlich tragbar ausgestaltet wird. In der vorliegenden Form gehen die Vorlagen jedoch in wesentlichen Punkten über diese Grundsätze hinaus. Swico fordert daher eine grundlegende Überarbeitung sowie die Präzisierung und Anpassung einzelner Bestimmungen. Zudem fordern wir die Durchführung einer umfassenden Regulierungsfolgenabschätzung.

Die kritischsten Punkte lassen sich wie folgt zusammenfassen:

- **Art. 48a–48d VE-FMG –Sicherheit, geopolitische Risiken und Datenbearbeitung:** Die genannten Artikel sind grundlegend zu überarbeiten. Übergeordnet fordern wir, dass die Artikel 48a bis 48d nicht in eine Botschaft einfliessen, bevor bessere Grundlagen vorliegen und die Umsetzung sowie die Folgen der Regulierung klar aufgezeigt sind.

- **Art. 48a VE-FMG (Cybersicherheit):** Im Grundsatz unterstützt. Die Vorgaben sind auf risikobasierte IKT-Mindeststandards zu beschränken, die weite Delegation nach Abs. 4 ist einzugrenzen, und Doppelspurigkeiten mit dem BACS sind zu vermeiden.
- **Art. 48b VE-FMG (Sicherheit der Infrastrukturen):** In der vorliegenden Form ist dieser Artikel nicht tragbar. Die Mehrlieferantenstrategie sowie die neuen Aufsichts- und Verbotskompetenzen des BAKOM werden abgelehnt. Weitergehende Anforderungen müssen zwingend die aktuellen Marktverhältnisse berücksichtigen.
- **Art. 48c VE-FMG (geopolitische Risiken):** Ersatzlose Streichung. Für ausserordentliche Fälle genügt das verfassungsrechtliche Notrecht, das im Gegensatz zu Art. 48c die parlamentarische Kontrolle wahrt. Darüber hinaus würde die neue Bestimmung mehr Probleme schaffen als sie löst.
- **Art 48d VE-FMG (Bearbeitung von Daten und Zusammenarbeit):** Streichung des Artikels. Die weitreichenden Befugnisse des BAKOM zur Bearbeitung und Weitergabe besonders schützenswerter Personendaten sowie zum Profiling sind für die Aufgaben nach Art. 48a und 48b nicht ausreichend begründet und gesetzlich zu wenig begrenzt.
- **Art 6b VE-FMG (missbräuchlicher Verkehr und Domain-Blockierungen):** Im Grundsatz unterstützt, jedoch prozedural zu präzisieren. Massnahmen dürfen nur auf Anordnung des fedpol nach Abklärung eines begründeten Betrugsverdachts erfolgen. Bei Domain-Namen ist zudem konsequent von «Blockierung» zu sprechen und der Begriff der Registerbetreiberin auf die Registry zu beschränken.
- **Fragwürdige Verknüpfung von Cybersicherheit, Datenschutz und Herkunft:** Die staatlich verordnete Multi-Vendor-Strategie in der jetzigen Form ist nicht zielführend: Sie bringt mehr Abhängigkeiten und Anforderungen an Sitzstaat, Herkunft oder Datenschutzangemessenheit sind nicht nachvollziehbar. Massnahmen müssen sich auf konkret nachweisbare technische Sicherheitsrisiken abstellen.
- **Weitreichende staatliche Eingriffsbefugnisse:** Mehrere Bestimmungen übertragen Bundesrat und BAKOM erhebliche Kompetenzen ohne die Voraussetzungen und Grenzen auf Gesetzesstufe ausreichend präzise festzulegen. Wir hinterfragen diese neuen Kompetenzen ausdrücklich.
- **Ausweitung der Datenbearbeitungsbefugnisse:** Die vorgesehenen Grundlagen für die Bearbeitung von Daten juristischer Personen, besonders schützenswerten Personendaten und Profiling schaffen erhebliche Rechtsunsicherheiten und gefährden Geschäftsgeheimnisse, Datensparsamkeit und informationelle Selbstbestimmung.
- **Nationale Sondervorgaben in den Verordnungen:** Vorgaben zu Konformitätsbewertungen, Zertifizierungsstandards sowie zum Betrieb von NOC und SOC dürfen internationale Sicherheitsmodelle nicht schwächen oder globale Sicherheitsorganisationen durch nationale Insellösungen ersetzen.

1 Allgemeine Würdigung

Angesichts der zunehmenden Cyberbedrohungen und der geopolitischen Verwerfungen anerkennt Swico ausdrücklich die Bedeutung des Schutzes der Fernmeldeinfrastrukturen vor Cyberbedrohungen. Darum können wir die grundsätzliche Stossrichtung der Vorlage nachvollziehen und die Überlegungen im Grundsatz unterstützen. Swico betont in diesem Zusammenhang, dass die Unternehmen der Digitalwirtschaft in den vergangenen Jahren entsprechende Massnahmen umgesetzt und eng mit den Behörden gegen Bedrohungen zusammengearbeitet haben.

Swico unterstützt grundsätzlich eine Weiterentwicklung der bestehenden regulatorischen Rahmenbedingungen, sofern diese verhältnismässig, unbürokratisch, praxistauglich und

international abgestimmt erfolgt. Für die stark international vernetzte Digitalwirtschaft sind insbesondere Rechtssicherheit, Kompatibilität mit internationalen Standards sowie ein innovationsfreundliches Umfeld von zentraler Bedeutung. Wir möchten betonen, dass die Vorlage sehr unterschiedliche Regulierungsziele, von der Cybersicherheit über geopolitische Risiken bis hin zur Betrugsbekämpfung und zum Netzausbau angeht. Dabei wird für jeden dieser Bereiche der konkrete Handlungsbedarf sowie die Erforderlichkeit und Verhältnismässigkeit der vorgeschlagenen Instrumente nicht durchgehend hergeleitet.

Kritische Prüfung der Kompetenzen des Staates
Der vorliegende Vorentwurf wird den genannten Anforderungen in wesentlichen Punkten nicht gerecht. Er schafft ein Regulierungsmodell, das in seiner heutigen Ausgestaltung weitreichende neue Eingriffs- und Steuerungsmöglichkeiten des Staates vorsieht, ohne deren Voraussetzungen, Grenzen und Auswirkungen auf Gesetzesstufe hinreichend präzise festzulegen und die Dringlichkeit dafür aufzuzeigen.

Besonders kritisch ist, dass zentrale Fragen der Sicherheitsarchitektur, der Datenbearbeitung, der Beschaffung und des Betriebs von Fernmeldeinfrastrukturen weitgehend auf Verordnungsstufe oder in den Vollzug verlagert werden. Damit erhalten Bundesrat und BAKOM sehr grosse Ermessensspielräume in Bereichen, die für die betroffenen Unternehmen erhebliche technische, organisatorische und wirtschaftliche Folgen haben können. Dies schwächt die Rechtssicherheit und erschwert langfristige Investitions- und Beschaffungsentscheide. Es braucht daher auf Gesetzesstufe klare und begründete Rahmenbedingungen und Definitionen.

Cybersicherheit nicht an politische Gegebenheiten knüpfen
Die Artikelreihe 48a-48d braucht eine grundlegende Überarbeitung. Wir fordern, dass die Artikel 48a bis 48d nicht in eine Botschaft einfliessen, bevor bessere Grundlagen vorliegen und die Umsetzung sowie die Folgen der Regulierung klar aufgezeigt sind. Dies setzt insbesondere eine umfassende Regulierungsfolgenabschätzung voraus, die namentlich die Auswirkungen auf Investitionen in die digitale Infrastruktur, die Betriebskosten der Anbieterinnen, die Versorgungssicherheit, den Wettbewerb sowie die Aussenwirtschaft systematisch untersucht. Mindestens aber müssen die durch die Regulierung entstehenden Mehrkosten bei den betroffenen Betreibern korrekt eruiert werden. Der Bundesrat soll diese Bestimmungen nach der Vernehmlassung zurückstellen und die offenen Fragen zuerst vertieft klären, etwa in einem erneuten Aussprachepapier, statt das Geschäft direkt ans Parlament zu überweisen.

Bei den genannten Artikeln sind die umfassenden Delegationen an den Bundesrat und das BAKOM besonders kritisch. Swico beurteilt zudem Eingriffe, die an Herkunfts-, Sitzstaat- oder geopolitische Kriterien anknüpfen, mit grosser Zurückhaltung. Cybersicherheit darf nicht pauschal mit Datenschutzangemessenheit, Unternehmenssitz oder geopolitischer Herkunft gleichgesetzt werden. Entscheidend müssen nachweisbare, technisch begründete Sicherheitsrisiken sowie wirksame organisatorische, vertragliche und technische Schutzmassnahmen sein. Andernfalls drohen Marktverzerrungen, zusätzliche Abhängigkeiten, erhebliche Kostenfolgen und Unsicherheiten für bereits getätigte Investitionen.

Orientierung an internationalen Standards
Aus Sicht von Swico müssen Sicherheitsvorgaben und Definitionen deshalb klar risikobasiert, technologieneutral und verhältnismässig ausgestaltet werden. Die Schweiz sollte sich konsequent an international anerkannten Cybersicherheitsstandards und bewährten Sicherheitsmodellen orientieren, statt nationale Sonderanforderungen oder konkrete Betriebs- und Organisationsmodelle vorzuschreiben. Gerade international tätige Anbieter stützen sich auf globale Sicherheitsorganisationen, standardisierte Prozesse und spezialisierte Security

Operations Center, die einen wesentlichen Beitrag zur Resilienz leisten. Eine Fragmentierung dieser Strukturen kann die Reaktionsfähigkeit bei Sicherheitsvorfällen schwächen und damit dem Ziel der Vorlage zuwiderlaufen.

Keine weiteren Datenbearbeitungsbefugnisse schaffen
Ebenso problematisch sind die vorgeschlagenen Datenbearbeitungsbefugnisse. Die Vorlage eröffnet dem BAKOM und weiteren Stellen weitgehende Möglichkeiten zur Bearbeitung und Weitergabe sensibler Informationen, einschliesslich besonders schützenswerter Personendaten, Profiling sowie Daten juristischer Personen. Umfang, Zweckbindung, Voraussetzungen und Schutzmechanismen werden dabei nicht ausreichend konkretisiert. Dies ist mit Blick auf Geschäftsgeheimnisse, Datensparsamkeit, Transparenz und die informationelle Selbstbestimmung kritisch zu beurteilen.

Swico lehnt die Vorlage in der vorliegenden Form daher ab und fordert eine Überarbeitung. Der Gesetzgeber sollte klare Sicherheitsziele definieren, die Umsetzung aber so ausgestalten, dass sie mit internationalen Standards vereinbar bleibt, die betriebliche Autonomie der Unternehmen respektiert und Innovation sowie Investitionen in sichere digitale Infrastrukturen nicht unnötig erschwert.

2 Stellungnahme zu ausgewählten Bestimmungen in der Teilrevision Fernmeldegesetzes

2.1 Sperrung von Telefonnummern und Domain-Namen

Neu sollen in Art. 6b auch Telefonnummern und Domain-Namen zweiter Ebene blockiert werden können, wenn ein begründeter Verdacht auf mutmasslichen Betrug nach Art. 146 Strafgesetzbuch besteht. Durch eine rasche Blockierung für fünf Tage (die durch Staatsanwaltschaften oder Gerichte verlängert werden kann) sollen Kundinnen und Kunden vor Betrug geschützt werden.

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

Die Branche unterstützt somit die Schaffung eines raschen und wirksamen Mechanismus zur Unterbrechung betrügerischer Aktivitäten und stellt sich daher nicht grundsätzlich gegen eine Ausweitung der Blockierungspflicht bei Domain-Namen. Damit die vorgesehenen Massnahmen wirksam, verhältnismässig und rechtsstaatlich umgesetzt werden können, ist die verfahrensrechtliche Ausgestaltung von Artikel 6b jedoch zu präzisieren.

Die Sperrung von Telefonnummern und die Blockierung von Domain-Namen muss von der zuständigen Behörde, d.h. dem Fedpol, zwingend angeordnet werden, nachdem das Fedpol den begründeten Verdacht abgeklärt hat. Ein Hinweis allein reicht nicht aus, und es ist auch nicht die Aufgabe einer Fernmeldedienstanbieterin oder einer Registerbetreiberin abzuklären, ob ein Verdacht vorliegt und ob dieser ausreichend begründet ist. In diesem Zusammenhang ist zu erwähnen, dass der Begriff der Registerbetreiberin eindeutig zu definieren ist. Unseres Erachtens dürfen darunter nur die Registry fallen. Registrare sind unbedingt davon auszuschliessen.

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

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

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

Forderung zu Art. 6b

Angesichts der offenen politischen Debatte im Parlament zur Motion Götte beantragen wir vorerst nur formale und prozedurale Anpassungen in Art. 6b. Insbesondere soll in Bezug auf die Domain-Namen (im Titel und in Abs. 2) konsequent der Begriff Blockierung verwendet werden. Es muss klar geregelt werden, dass es sich hierbei nicht um eine Netzsperre auf Ebene der Provider handelt. Zudem sollen – allenfalls in Rücksprache mit der zuständigen Registry – Schnittstellen, Abläufe und die Information der betroffenen Personen und Unternehmen praxistauglich geregelt werden. Wichtig ist, dass es am Fedpol, bzw. der zuständigen Behörde liegt, den begründeten Verdacht und die Verhältnismässigkeit zu prüfen. Die Behörde ordnet die Massnahme verbindlich an und trägt dafür die Verantwortung. Registrare sind von den Prüf- und Blockierungspflichten auszunehmen.

2.2 Bearbeitung und Bekanntgabe von Daten juristischer Personen

Der neue Art. 13c erweitert die behördlichen Datenbearbeitungsbefugnisse erheblich, indem die Regelungen von Art. 13a und 13b ausdrücklich auch auf juristische Personen ausgedehnt und damit die Bearbeitung von Berufs-, Geschäfts- und Fabrikationsgeheimnissen ermöglicht werden.

Die Bestimmung schafft die Grundlage für den Zugriff auf sensible Unternehmensinformationen, ohne die Voraussetzungen und Schranken ausreichend zu konkretisieren. Dadurch droht eine Schwächung des Schutzes von Geschäftsgeheimnissen und eine erhebliche Rechtsunsicherheit für die betroffenen Unternehmen. Swico fordert deshalb eine klare Definition der Daten, die bearbeitet und bekanntgegeben werden müssen sowie präzisere gesetzliche Vorgaben zum Schutz vertraulicher Unternehmensdaten.

2.3 Datenbearbeitung sowie Amts- und Rechtshilfe.

Die mit Art. 30a verfolgte Stossrichtung lehnt Swico in der vorliegenden Form ab. Die vorgeschlagene Bestimmung geht weit über eine notwendige Informationsgrundlage hinaus. Der Artikel schafft eine gesetzliche Grundlage für Profiling durch das BAKOM, nötigenfalls auch ohne Wissen der betroffenen Personen, und erlaubt dabei die Bearbeitung besonders

schützenswerter Personendaten. Gleichzeitig eröffnet die Bestimmung die Möglichkeit, die daraus gewonnenen Informationen an weitere Behörden sowie an anerkannte private und öffentliche Stellen im Bereich der Cybersicherheit weiterzugeben.

Wir erachten es als kritisch, dass die wesentlichen Fragen zur Bearbeitung besonders schützenswerter Personendaten und zur Durchführung von Profiling dem Bundesrat zur Regelung auf Verordnungsstufe übertragen werden. Damit erhält die Exekutive einen sehr grossen Handlungsspielraum, während die konkreten Voraussetzungen und Schranken der Datenbearbeitung nicht durch den Gesetzgeber selbst festgelegt werden. Dies schafft Rechtsunsicherheit und erschwert die demokratische Kontrolle in einem sensiblen Eingriffsbereich.

Darüber hinaus erscheint fraglich, ob die vorgesehenen Datenbearbeitungsbefugnisse mit dem Grundsatz der Datensparsamkeit (Art. 6 DSG) vereinbar sind. Die Bearbeitung biometrischer Daten und die Durchführung von Profiling ohne Wissen der betroffenen Personen stellen erhebliche Eingriffe in die informationelle Selbstbestimmung dar und sollten nur unter klar definierten, eng begrenzten Voraussetzungen zulässig sein. Gerade im Bereich der Cybersicherheit ist Vertrauen zwischen Staat, Wirtschaft und Bevölkerung von zentraler Bedeutung. Dieses Vertrauen setzt voraus, dass Umfang und Grenzen staatlicher Datenbearbeitung transparent, verhältnismässig und gesetzlich klar geregelt sind.

2.4 Schutz der Fernmeldeinfrastrukturen vor Cyberbedrohungen

Art. 48a verpflichtet Fernmeldedienstanbieterinnen, technische, operative und administrative Massnahmen zum Schutz ihrer Infrastrukturen vor Cyberbedrohungen und Manipulationen zu ergreifen. Gleichzeitig erhält das BAKOM den Auftrag, Risiken für die Resilienz von Fernmeldeinfrastrukturen zu überwachen, zu bewerten und dafür von den Anbietern die notwendigen Auskünfte, einschliesslich Verkehrsdaten, einzufordern. Der Bundesrat wird zudem ermächtigt, die konkreten Anforderungen an die Cybersicherheit und Resilienz auf Verordnungsstufe weiter zu präzisieren.

Swico schlägt eine Anpassung des Art. 48a vor. Das Anliegen, den Schutz der Fernmeldeinfrastrukturen vor Cyberbedrohungen zu verbessern, ist berechtigt. Jedoch kritisieren wir, dass der Regulierungsgegenstand in Art. 48a mit Cybersicherheit und Resilienz vermischt wird. Cybersicherheit und Resilienz sind konzeptionell zu trennen und in Art. 48a ist klar auf Cybersicherheit zu fokussieren. Zudem geht der Artikel über die Festlegung allgemeiner Sicherheitsziele hinaus und schafft eine weitreichende Grundlage für staatliche Eingriffe in den Betrieb von Fernmeldeinfrastrukturen.

Als kritisch erachten wir die bundesrätliche Kompetenz, zentrale Aspekte der Sicherheitsarchitektur und des Netzbetriebs auf Verordnungsstufe zu regeln. Damit werden wesentliche Anforderungen, welche erhebliche technische, organisatorische und wirtschaftliche Auswirkungen auf die betroffenen Unternehmen haben können, weitgehend der Exekutive überlassen. Staatliche Regulierung im Bereich der Cybersicherheit ist nur dort angezeigt, wo Schutzlücken bestehen. Dem BAKOM die Aufgabe zu übertragen, Risikofaktoren zu überwachen, zu ermitteln und zu bewerten, schafft Doppelspurigkeiten, erhöht das Risiko von Mehrfachregulierung und führt zu unnötigem administrativem Zusatzaufwand. Der Schutz vor Cyberbedrohungen findet in einem hochdynamischen Umfeld statt. Schwachstellen und Sicherheitslücken werden rasch ausgenutzt und müssen ebenso rasch behoben werden. Art. 48a ist deshalb zu präzisieren. So dürfen unseres Erachtens die neuen BAKOM-Kompetenzen die etablierte Zusammenarbeit mit den zuständigen Sicherheitsbehörden, insbesondere dem BACS, weder überschneiden noch gefährden.

Eine wirksame und legitime staatliche Cybersicherheitsregulierung nach Art. 48a Abs. 1 in Verbindung mit Abs. 4 VE-FMG sollte sich an den international etablierten Cybersicherheitsstandards orientieren. Internationale Referenzrahmen verfolgen grundsätzlich einen risikobasierten und technologieneutralen Ansatz. Sie definieren Sicherheitsziele und Resilienzerwartungen, überlassen die konkrete Ausgestaltung der Sicherheitsmassnahmen jedoch weitgehend den betroffenen Unternehmen. Art. 48a schafft hingegen die Grundlage für detaillierte regulatorische Vorgaben zu Betrieb, Redundanzen, Meldeprozessen oder Sicherheitsmassnahmen. Die Vorgaben sind auf IKT-Mindeststandards nach aktuellem Stand der Technik und international anerkannten Best Practices zu beschränken, statt einzelne Hersteller, Technologien oder Beschaffungsmodelle vorzugeben. So bleibt ein hohes Sicherheitsniveau gewahrt, ohne Innovations- und Investitionsfähigkeit zu beeinträchtigen.

Da die vorgesehenen Sicherheitsmassnahmen in die Rechte der betroffenen Unternehmen eingreifen können und konkrete Betriebs- oder Organisationsmodelle vorgeben können, sollte im Gesetz ausdrücklich festgehalten werden, dass der Bundesrat die technische Machbarkeit und die wirtschaftliche Zumutbarkeit zu berücksichtigen hat. Eine unverhältnismässige Kostenbelastung ist dringend zu verhindern.

Art. 48a

[1] Die Anbieterinnen von Fernmeldediensten müssen dem Risiko angemessene technische, operative und administrative Massnahmen ergreifen [...]

[4] Der Bundesrat präzisiert die Massnahmen nach Absatz 1. Er kann zum Schutz vor Gefahren, zur Vermeidung von Schäden und zur Minimierung von Risiken Bestimmungen über die Sicherheit von Informationen sowie von Fernmeldeinfrastrukturen und -diensten erlassen. Er orientiert sich dabei auf international anerkannte Standards und berücksichtigt technische Machbarkeit und die wirtschaftliche Zumutbarkeit. ~~insbesondere bezüglich:~~

~~a. Verfügbarkeit;~~
~~b. Betrieb;~~
~~c. Sicherstellung von redundanten Infrastrukturen;~~
~~d. Meldung von Störungen;~~
~~e. Nachvollziehbarkeit von Vorgängen;~~
~~f. Umleitung oder Verhinderung von Verbindungen sowie Unterdrückung von Informationen nach Absatz 1.~~

2.5 Sicherheit von Fernmeldeinfrastrukturen

Art. 48b verlangt, dass kritische Komponenten der Fernmeldeinfrastruktur von verschiedenen Herstellerinnen stammen und mindestens eine Herstellerin muss ihren Sitz in einem Staat mit angemessenem Datenschutzniveau haben. Der Bundesrat soll Kategorien, Anteile und Mindestquoten festlegen können. Das BAKOM kann bei begründetem Sicherheitsrisiko neu die Inbetriebnahme bestimmter Bestandteile verbieten, eine Liste verbotener Bestandteile veröffentlichen und deren Ausserbetriebnahme oder Entfernung verfügen.

Die in Art. 48b vorgesehene Ausgestaltung geht aus Sicht von Swico zu weit und lehnt den Artikel in dieser Form ab. In Art. 48b Abs. 1 fordert nun der Bundesrat, dass nur Fernmeldeinfrastrukturen verwendet werden, welche die Vertraulichkeit, Integrität und Verfügbarkeit von Fernmeldediensten gewährleisten. Diese Regulierung trägt der heutigen Cybersicherheitspraxis im Fernmeldebereich nicht Rechnung. Fernmeldeinfrastrukturen im Mobilfunk- und im Festnetzbereich bestehen aus unzähligen Komponenten und werden von den Netzbetreiberinnen nach eigenen Vorgaben konzipiert, konfiguriert und betrieben. Cybersicherheit entsteht nicht durch die Auswahl der Geräte, sondern in erster Linie durch die Netzbetreiberin im

Betrieb unter Verwendung internationaler Standards, etablierter Frameworks oder der GSMA Knowledge Base.

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

Falsche Einschränkungen und Verknüpfungen

Die staatlich verordnete Multi-Vendor-Strategie in der jetzigen Form ist nicht zielführend. Die Mitglieder von Swico verfolgen dort eine Multi-Vendor-Strategie, wo sie technisch, kommerziell und bezüglich der Sicherheit sinnvoll ist. Eine staatlich vorgeschriebene Mehrlieferantenstrategie, die sich an Anteilen und Mindestprozentsätzen orientiert, wäre nicht nur mit erheblichen Kosten verbunden, sondern würde weder die Sicherheit erhöhen noch die Abhängigkeit von einzelnen Lieferanten verringern. Durch den Einsatz von Komponenten verschiedener Hersteller erhöhen sich nämlich auch die Anzahl der Schnittstellen und die Komplexität des Gesamtsystems. Dadurch steigen nicht nur der Betriebsaufwand und die Fehleranfälligkeit. Auch die Zahl potenzieller Schwachstellen und damit das Risiko von Cyberangriffen nimmt zu. Es ist auch eine Fehleinschätzung anzunehmen, dass sich das Abhängigkeitsrisiko durch eine Mehrlieferantenstrategie reduzieren lässt. Der Ausfall eines einzelnen Herstellers kann die Infrastruktur auch dann beeinträchtigen, wenn mehrere Lieferanten eingesetzt werden. Bei einer Single-Vendor-Strategie besteht die Abhängigkeit von einem Hersteller, bei einer Multi-Vendor-Strategie von mehreren Herstellern.

Die Einschränkung nach Herkunftsland und die Verknüpfung von Cybersicherheit mit Datenschutzanforderungen erscheinen sachlich fragwürdig. Datenschutz und Cybersicherheit verfolgen unterschiedliche Schutzziele. Ein angemessenes Datenschutzniveau eines Staates erlaubt für sich allein keine Aussage über das Cybersicherheitsrisiko von Produkten oder Dienstleistungen einer Herstellerin. Mit diesem Ansatz wird verkannt, dass die Sicherheit moderner digitaler Infrastrukturen in erster Linie durch technische, organisatorische und vertragliche Schutzmassnahmen gewährleistet wird. Herkunft oder Hauptsitz eines Unternehmens sind nicht zwingend ausschlaggebend für die Sicherheit der bearbeiteten Daten oder eingesetzten Systeme. Lokale Datenhaltung, Verschlüsselung, Zugangskontrollen und spezialisierte Sicherheitsarchitekturen können wirksameren Schutz bieten als formale Anforderungen an den Sitzstaat einer Anbieterin. Darüber hinaus anerkennt die Schweiz lediglich 44 Staaten als Länder mit einem gleichwertigen Datenschutzniveau. Swico fordert daher, die Einschränkung nach Herkunftsland und die Verknüpfung mit Datenschutzanforderungen zu streichen oder anzupassen.

Ebenso ist zu berücksichtigen, dass ein Sicherheitsrisiko regelmässig nicht isoliert als Eigenschaft eines einzelnen Netzbestandteils beurteilt werden kann. Das tatsächliche Risiko hängt vielmehr von dessen konkreter Funktion und Einbindung in die Gesamtarchitektur, der Konfiguration und dem Betrieb des Netzes sowie von den implementierten technischen und organisatorischen Schutzmassnahmen ab. Eine abstrakte komponentenbezogene Risikobeurteilung kann daher zu sachlich nicht gerechtfertigten Verboten führen, obwohl ein identifizierbares Risiko durch geeignete Sicherheitsmassnahmen wirksam reduziert oder ausgeschlossen werden könnte. Vor einem Verbot sollten deshalb stets die konkrete Einsatzumgebung und mögliche risikomindernde Massnahmen berücksichtigt werden.

Klare Definition kritischer Bestandteile

Unklar bleibt auch hier, was mit «kritischen Bestandteilen der Fernmeldeinfrastruktur» gemeint ist. Das sorgt für grosse Unsicherheit. Statt auf Stufe Gesetz für Klarheit und damit

Verlässlichkeit zu sorgen, überträgt Absatz 2 diese weitreichende Definitionskompetenzen dem Bundesrat (Kategorien, Anteile, Mindestprozentsätze). Das entbehrt angesichts des umfangreichen Eingriffs in die Wirtschaftsfreiheit jeglicher Verhältnismässigkeit.

Von besonderer Bedeutung ist eine präzise und technologieneutrale Definition der «kritischen Bestandteile». Die Bestimmung darf nicht dazu führen, dass ganze Technologie- oder Produktkategorien allein aufgrund ihrer Funktion oder Position im Netz pauschal als kritisch qualifiziert werden. Entscheidend sollte vielmehr sein, ob der konkrete Bestandteil aufgrund seiner technischen Funktion tatsächlich einen wesentlichen Einfluss auf die Verfügbarkeit, Integrität oder Sicherheit des Netzes hat. Eine zu breite Definition würde den Anwendungsbereich von Art. 48b erheblich ausweiten und könnte unverhältnismässige Auswirkungen auf Beschaffung, Wettbewerb und bestehende Netzarchitekturen haben.

Kritische Kompetenzerweiterung des BAKOM
Die weitreichenden Kompetenzdelegationen des BAKOM lehnen wir konsequent ab. Die Möglichkeit, aufgrund eines «begründeten Sicherheitsrisikos» Bestandteile zu verbieten oder deren Ausserbetriebnahme beziehungsweise Entfernung anzuordnen, schafft erhebliche Rechts- und Investitionsunsicherheiten. Die vorgesehene Ausweitung der BAKOM-Kompetenzen ist aus unserer Sicht nicht hinreichend klar abgegrenzt. Es fehlt eine präzise gesetzliche Festlegung der Voraussetzungen, Grenzen und Verhältnismässigkeit dieser neuen Eingriffsbefugnisse. Gleichzeitig sind die Kriterien für die Risikobeurteilung noch die Verfahren zur Einbeziehung der betroffenen Unternehmen auf Gesetzesstufe nicht ausreichend geklärt. Dadurch entstehen grosse Ermessensspielräume, die langfristige Investitionen in kritische Infrastrukturen erschweren können.

Eingriffe dieser Tragweite sollten nur auf der Grundlage einer transparenten und nachvollziehbaren technischen Risikobeurteilung zulässig sein. Die betroffenen Anbieterinnen und Herstellerinnen sollten vorgängig angehört werden und Gelegenheit erhalten, zum festgestellten Risiko sowie zu möglichen risikomindernden Massnahmen Stellung zu nehmen. Ein Verbot, eine Ausserbetriebnahme oder eine Entfernung sollte nur angeordnet werden dürfen, wenn weniger einschneidende Massnahmen zur Beherrschung eines konkret nachgewiesenen Sicherheitsrisikos nicht ausreichen. Damit würde das Verhältnismässigkeitsprinzip, die Rechtssicherheit und der Schutz bereits getätigter Investitionen besser gewährleistet.

Swico fordert deshalb, Art. 48b zu streichen.

~~***Art. 48b Sicherheit von Fernmeldeinfrastrukturen***~~

2.6 Massnahmen betreffend Fernmeldeinfrastrukturen bei geopolitischen Risiken

Der Bundesrat erhält mit Art. 48c VE-FMG die Kompetenz, den Erwerb, die Inbetriebnahme und den Betrieb von Bestandteilen von Fernmeldeinfrastrukturen zu verbieten, die von Herstellerinnen stammen, die für die Schweiz ein geopolitisches Risiko darstellen. Zudem kann der Bundesrat die Anbieterinnen verpflichten, solche Bestandteile aus ihrer Infrastruktur zu entfernen.

Die vorgeschlagene Ausgestaltung von Art. 48c VE-FMG beurteilt Swico als kritisch und wir fordern den Artikel ersatzlos zu streichen. Für den akuten Ausnahmefall verfügt der Bundesrat bereits über das verfassungsrechtliche Notrecht (Art. 184 Abs. 3 und Art. 185 Abs. 3 BV). Dieses ist an enge Voraussetzungen gebunden, zeitlich befristet und innert Frist durch das Parlament in ordentliches Recht zu überführen; andernfalls fällt die Notverordnung dahin. Für die ausserordentlichen und schwer vorhersehbaren geopolitischen Konstellationen, die Art. 48c adressieren will, besteht damit bereits eine tragfähige und rechtsstaatlich abgesicherte Grundlage.

Ein dauerhaftes Sonderregime im Fernmelderecht ist weder erforderlich noch angezeigt. Wollte man dennoch ein dauerhaftes Instrument schaffen, gehörte dieses ins ordentliche

Gesetzgebungsverfahren, mit präzisen Tatbeständen, klaren Verhältnismässigkeitsschranken, wirksamem Rechtsschutz und angemessenen Entschädigungen. Genau dies leistet Art. 48c nicht. Er überträgt dem Bundesrat eine unbefristete, inhaltlich offene Verbotskompetenz und ermöglicht dauerhafte Eingriffe am Parlament vorbei, während das Notrecht den Bundesrat innert Frist zurück ans Parlament zwingt. Die Norm ist damit nicht nur überflüssig, sondern rechtsstaatlich schlechter ausgestaltet als das bestehende Notrecht.

Zudem verschiebt die Bestimmung in dieser Form die Sicherheitsbeurteilung von einer technischen hin zu einer geopolitischen und politischen Betrachtung. Die unbestimmten Rechtsbegriffe für die Krisenintervention sind zu schwammig und kaum justiziabel. Der Bundesrat erhält damit weitreichende Kompetenzen, die politisch motiviert eingesetzt werden könnten. Eine risikobasierte Bewertung auf Basis nachgewiesener Sicherheitsmängel findet nicht statt. Faktisch handelt es sich erneut um einen pauschalen Ausschluss nach Herkunft. Dies ist mit Blick auf das Legalitätsprinzip äusserst problematisch und führt zu erheblichen Rechts- und Investitionsunsicherheiten.

Aus Sicht von Swico ist eine klare Abgrenzung zwischen technischen Sicherheitsrisiken und geopolitischen Risikobeurteilungen erforderlich. Soweit von bestimmten Komponenten konkrete Risiken für die Sicherheit oder Resilienz der Fernmeldeinfrastruktur ausgehen, bestehen mit Art. 48a und 48b bereits Instrumente, die unmittelbar an solche Risiken anknüpfen. Eine zusätzliche Eingriffskompetenz auf Grundlage geopolitischer Kriterien müsste daher besonders klar definiert, objektiv nachvollziehbar und verhältnismässig ausgestaltet werden.

Begriffe wie «geopolitisches Risiko», «Kontrolle» oder «Einfluss» eröffnen in der vorgesehenen Form einen erheblichen Interpretationsspielraum. Für die betroffenen Unternehmen muss auf Gesetzesstufe vorhersehbar sein, unter welchen Voraussetzungen Eingriffe in Beschaffung, Betrieb oder bestehende Infrastruktur zulässig sind. Herkunft oder Eigentümerstruktur einer Herstellerin sollten dabei für sich allein nicht ausschlaggebend sein. Massgeblich sollten objektiv überprüfbare Risiken für die Sicherheit und Resilienz der schweizerischen Fernmeldeinfrastruktur sein.

Zudem besteht die Gefahr, dass politische oder geopolitische Entwicklungen unmittelbar zu Eingriffen in bestehende Netzinfrastrukturen führen. Ein verpflichtender Austausch bereits installierter Komponenten kann erhebliche finanzielle Belastungen verursachen und die Versorgungssicherheit beeinträchtigen. Gerade bei komplexen Mobilfunk- und Kernnetzinfrastrukturen erfordern Austauschmassnahmen technische Planung, Beschaffung, Integration, Tests und Migration. Entsprechende Massnahmen müssen daher auch hinsichtlich ihrer operativen Auswirkungen und Umsetzbarkeit beurteilt werden.

Aus Gründen einer kohärenten Regulierung sollte zudem geprüft werden, wie sich Art. 48c in den übergeordneten regulatorischen Rahmen für kritische Infrastrukturen einfügt. Geopolitische Risiken vergleichbarer Tragweite sollten nach möglichst einheitlichen, sektorübergreifenden und nachvollziehbaren Grundsätzen beurteilt werden. Aus Sicht von Swico sollte Art. 48c daher in der vorliegenden Form gestrichen werden.

Sollte an einer entsprechenden Regelung festgehalten werden, müsste diese wesentlich präzisiert und auf klar definierte Eingriffsvoraussetzungen beschränkt werden. Eingriffe sollten nur als ultima ratio zulässig sein. Zudem soll die Bestimmung auf klar definierte und nachweisbare Sicherheitsrisiken beschränkt, die Entscheidungskriterien für ein Eingreifen präzisiert werden und die Verhältnismässigkeit sowie die wirtschaftlichen Auswirkungen für die

betroffenen Unternehmen deutlich stärker berücksichtigt werden. Insbesondere ist sicherzustellen, dass Fernmeldedienstanbieterinnen nicht mit unverhältnismässigen Kosten belastet werden und bestehende Investitionen einen angemessenen Bestandesschutz geniessen.

Der Eingriff in die Wirtschaftsfreiheit wäre so erheblich, dass solch weitreichende Massnahmen zwingend der Genehmigung durch die Bundesversammlung bedürften. Die Fernmeldenetzbetreiber sind vorgängig anzuhören, und der Eingriff ist so gering wie möglich zu halten. Für die Umsetzung sind ausreichende Fristen von mehreren Jahren vorzusehen.

Swico fordert Art. 48c ersatzlos zu streichen.

~~**Art. 48c Massnahmen betreffend Fernmeldeinfrastrukturen bei geopolitischen Risiken**~~
~~1~~ ...
~~2~~ ...
~~3~~ ...

2.7 Bearbeitung von Daten und Zusammenarbeit

Art. 48d erteilt dem BAKOM die Befugnis, Profiling durchzuführen, besonders schützenswerte Personendaten – einschliesslich biometrischer Daten sowie Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen – zu bearbeiten und diese Daten weiterzugeben. Gleichzeitig werden die wesentlichen Fragen zur Durchführung dieser Profilings und zur Bearbeitung der Daten dem Bundesrat zur Regelung auf Verordnungsstufe übertragen.

Die in Art. 48d vorgesehenen Befugnisse gehen deutlich über eine notwendige Grundlage für die Zusammenarbeit hinaus. Swico befürchtet ein erhebliches Risiko einer Ausweitung staatlicher Eingriffsbefugnisse ohne ausreichend klare gesetzliche Begrenzung. Gleichzeitig bleibt unklar, weshalb das BAKOM für die Aufgaben nach Art. 48a und Art. 48b überhaupt Personendaten nutzen muss. Umfang und Voraussetzungen der Datenbearbeitung, Profiling und Datenflüsse zwischen Behörden und weiteren Stellen werden auf Gesetzesstufe nicht genügend präzisiert. Dies schafft Rechtsunsicherheit und eröffnet der Exekutive einen grossen Ermessensspielraum.

Besonders kritisch ist Art. 48d im Zusammenspiel mit den Artikeln 48a und 48b. Während diese Bestimmungen weitreichende Vorgaben zur Sicherheit von Fernmeldeinfrastrukturen und potenzielle Eingriffe in Beschaffungs-, Betriebs- und Sicherheitsentscheidungen ermöglichen, schafft Art. 48d die notwendige Datengrundlage für solche Interventionen. Damit entsteht ein regulatorisches System, das zunehmend in die betriebliche Autonomie der Unternehmen eingreifen kann. Stellungnahme zu ausgewählten Bestimmungen in den Verordnungen.

Artikel 48d ist darum zu streichen.

~~Art. 48d Bearbeitung von Daten und Zusammenarbeit~~
~~1~~ ...
~~2~~ ...
~~3~~ ...
~~4~~ ...

3 Stellungnahme zu ausgewählten Bestimmungen Teilrevision der Verordnungen im Fernmeldebereich

3.1 Konformitätserklärungen (Art. 2 VE-FAV und Art. 28b VE-VFAV))

Gemäss Art. 28b (Grundsätze) des Entwurfes der Verordnung über Fernmeldeanlagen (VE-FAV) darf eine kritische Netzwerkanlage nur in Verkehr gebracht oder betrieben werden, wenn sie spezifische Sicherheitsanforderungen erfüllt. Das BAKOM kann dazu eine Liste erstellen und die Anforderungen festlegen. Dies jeweils unter Berücksichtigung anerkannter internationaler Normen und Praxis. Gemäss Art. 28c (Konformitätserklärung und technische Unterlagen) VE-FAV muss der Hersteller die Konformität über das Verfahren nach Art. 13 Abs. 1 Bst. b oder ein als gleichwertig anerkanntes ausländisches Verfahren nachweisen. Die Analyse und Bewertung der Sicherheitsrisiken muss auf international beschriebenen und anerkannten Methoden beruhen.

Die Liste der kritischen Bestandteile ist zu weit gefasst. Sie ist auf die tatsächlich sicherheitskritischen zentralen Komponenten (Core Network) zu beschränken. Eine pauschale Einstufung peripherer Netzbereiche wie des Radio Access Network (RAN) als kritisch ist sachlich nicht gerechtfertigt und unverhältnismässig. Zudem darf die Definition in Anhang 8 VFAV nicht über die übergeordnete Umschreibung in Art. 2 Abs. 1 Bst. c^{bis} FAV hinausgehen. Eine Ausweitung durch das Bundesamt wäre mit Blick auf Verhältnismässigkeit und Legalitätsprinzip nicht haltbar.

Die in der VE-FAV vorgesehenen Zertifizierungsstandards erachtet Swico als unklar. Die Bewertungsmethode soll sich gemäss erläuterndem Bericht an international, insbesondere europäisch, anerkannten Methoden orientieren. Swico schlägt vor, Technologieneutralität ausdrücklich zu verankern und lediglich die international etablierte Zertifizierungsstandards anzuerkennen. Bei der Festlegung der anerkannten Bewertungsmethoden und Standards sollte auf etablierte internationale Standards und Standardisierungsorganisationen abgestellt werden. Zudem soll das BAKOM bei der Festlegung von Standards oder der Erstellung der Liste die Expertise und Einschätzung der Branche einholen. Dies schafft Rechtssicherheit. Viele EU-Standards wie EUCC, EU5G oder CRA befinden sich noch in Entwicklung und eignen sich deshalb nicht als alleinige Referenz.

3.2 Betrieb sicherheitskritischer Fernmeldeanlagen (Art. 96 Abs. 2 VE-FDV)

Gemäss Entwurf von Art. 96f der Verordnung über Fernmeldedienste (VE-FDV) müssen Anbieterinnen Network Operations Center (NOC) und Security Operations Center (SOC) ausschliesslich in der Schweiz betreiben. Viele Unternehmen nutzen heute globale SOC und international integrierte Sicherheitsorganisationen, die rund um die Uhr betrieben werden und durch Grösse und Spezialisierung häufig ein höheres Sicherheitsniveau gewährleisten als nationale Insellösungen. Eine Regulierung, die lokale Lösungen bevorzugt oder bestimmte Organisationsformen vorgibt, könnte die Reaktionsfähigkeit bei Sicherheitsvorfällen schwächen. International, insbesondere in NIS2, steht ein risikobasierter Ansatz im Vordergrund: Die EU verlangt wirksame Sicherheitsmassnahmen, schreibt aber grundsätzlich weder den Standort eines SOC noch die Struktur der Sicherheitsorganisation vor. Vielmehr stehen Wirksamkeit, Auditierbarkeit und Risikomanagement im Vordergrund.

Der ausnahmslose Betrieb von Netzbetriebs- und Sicherheitszentren in der Schweiz greift zu weit. Anbieterinnen sowie neuen Technologien (etwa satellitenbasierter Mobilfunk) muss es möglich bleiben, zumindest unterstützende Aufgaben im Bereich NOC und SOC im Ausland zu betreiben, sofern sie nachweislich dieselben Sicherheitsanforderungen wie in der Schweiz

einhalten. Entscheidend ist das erreichte Sicherheitsniveau, nicht der geografische Standort. Möglich bleiben müssen namentlich unterstützende Hersteller- und Supportleistungen aus dem Ausland (etwa 3rd-Level-Support und Wartung), auch im Normalbetrieb, sofern das Sicherheitsniveau gewahrt bleibt.

Art. 96f Betrieb sicherheitskritischer Fernmeldeanlagen

[1] Die Mobilfunkkonzessionärinnen und die Full MVNO müssen sicherstellen, dass die von ihnen betriebenen sicherheitskritischen Fernmeldeanlagen dem Stand der Technik entsprechen. Das BAKOM kann die betroffenen Anlagen festlegen.
~~[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.~~

3.3 Keine pauschale Aktivierung aller Sicherheitsoptionen (FDV Art. 96fbis Abs. 2)

«Secure by Design» und «Secure by Default» werden im Grundsatz unterstützt. Die Aktivierung von Sicherheitsfunktionen muss aber risikobasiert und im Einzelfall erfolgen, da eine pauschale Aktivierung sämtlicher standardisierter Optionen die Netzstabilität beeinträchtigen kann. Eine Pflicht zur Umsetzung aller Empfehlungen ist deshalb abzulehnen. Das Wort «alle» ist zu streichen.

3.4 Keine anbieterübergreifende Schwachstellen-Datenbank (Art. 96fbis Abs. 4 VE-FDV)

Die verstärkte Kooperation bei Cyberangriffen wird unterstützt. Die im erläuternden Bericht vorgesehene gemeinsame Datenbank zu Schwachstellen, Anomalien und Eindringversuchen ist jedoch abzulehnen. Sie würde sicherheitsrelevante Informationen gebündelt angreifbar machen und damit die Netzsicherheit schwächen. Federführung und Koordination der Zusammenarbeit sind beim BACS anzusiedeln.

3.5 Ausländische Konformitätsbewertungen anerkennen (Art. 28c VE-FAV)

Gleichwertige ausländische Verfahren und international anerkannte Zertifizierungen sind anzuerkennen, um Doppelprüfungen und unnötige Handelshemmnisse zu vermeiden.

Wir bedanken uns für die Berücksichtigung unserer Anliegen und stehen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Swico

Dr. Jon Fanzun
CEO

Annika Bos
Public Affairs Manager