Zusammenfassung der eingereichten Stellungnahme

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

Eröffnung	27.05.2026
Eingabefrist	17.09.2026
Zuständiges Departement	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK)
Zuständige Bundesstelle	Bundesamt für Kommunikation (BAKOM)
Zuständige Organisation	Telecomrecht
Adresse	Zukunftstrasse 44, 2500, Biel/Bienne
Unterlagen und Informationen	https://fedlex.data.admin.ch/eli/dl/proj/2026/39/cons_1
Kontaktperson	Lukas Füeg (tp-secretariat@bakom.admin.ch) , Michael Strasser (tp-secretariat@bakom.admin.ch)
Telefon	+41 58 46 03286

Kontaktangaben zur Stellungnahme

Name der Person oder Organisation	Piratenpartei Schweiz (PPS)
Zuständige Stelle	Vorstand
Adresse	3000 Bern
Vorname	Renato
Nachname	Sigg
Telefonnummer für Rückfragen	--
Einreichungsdatum	17.09.2026

Rückmeldung zu: Erhöhung der Netzsicherheit und Schutz vor Cyberbedrohungen (Teilrevision der Verordnungen im Fernmeldebereich): Verordnung über Fernmeldedienste (FDV)

Generelle Stellungnahme

Rückmeldung zur Gesamtvorlage	Neutrale Haltung
Begründung	Die Piratenpartei Schweiz begrüsst grundsätzlich das Ziel, die Sicherheit und Resilienz der schweizerischen Fernmeldeinfrastrukturen zu erhöhen. «Secure by Design», «Secure by Default», wirksame Signalisierungs-Firewalls, die Kontrolle kritischer Netzwerkkomponenten und Massnahmen gegen Rufnummernmissbrauch liegen im öffentlichen Interesse. Im Gegensatz zu weiten Teilen der parallel vorgeschlagenen FMG-Revision betrifft diese Vorlage überwiegend tatsächliche technische Netzsicherheit. Kritisch wird sie dort, wo technische Schutzmassnahmen in eine Überwachung der Nutzerinnen und Nutzer übergehen könnten. Art. 96f^bis verlangt eine permanente und systematische Überwachung der Netze in Echtzeit. Der erläuternde Bericht sieht hierzu insbesondere die Erstellung, Sammlung und Auswertung von Logfiles sämtlicher Netzknoten vor (S. 19) sowie eine gemeinsame Datenbank für Schwachstellen, Anomalien und unbefugtes Eindringen (S. 20). Solche Massnahmen müssen strikt auf technische Cybersicherheitszwecke beschränkt bleiben. Wo Personendaten betroffen sind, sind Zweckbindung, Datenminimierung sowie klare Zugriffs- und Löschregeln notwendig. Vor diesem Hintergrund überzeugt auch der Verzicht auf eine vertiefte Datenschutz-Folgenabschätzung nicht. Der erläuternde Bericht hält auf S. 32 lediglich fest, dass eine datenschutzrechtliche Risikovorprüfung erfolgt sei und das Ausmass der vorgesehenen Datenbearbeitung keine weitergehende Datenschutz-Folgenabschätzung erfordere. Technische Einzelheiten dürfen flexibel geregelt werden; wesentliche Grenzen grundrechtsrelevanter Datenbearbeitungen gehören jedoch nicht in weitgehende Delegationen an das BAKOM oder in blosse Verweise auf private Standards.
Anhang	

Detaillierte Stellungnahme

Titel	Art. 96fbis Sicherheitsmassnahmen
Antwortoption	Ablehnung
Anpassungen / Gegenvorschlag	~~1 Die Mobilfunkkonzessionärinnen und die Full-MVNO müssen die notwendigen technischen, betrieblichen und organisatorischen Massnahmen treffen, um die Sicherheit von Fernmeldeinfrastrukturen zu gewährleisten und Cyberbedrohungen zu verhindern.~~ ~~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.~~ ~~3 Sie müssen in Echtzeit eine permanente und systematische Überwachung ihrer Netze zur Erkennung von Schwachstellen, Anomalien und Eindringlingen durchführen.~~ ~~4 Sie müssen sich über erkannte Schwachstellen, Anomalien und Eindringlinge austauschen und sich auf die aktuell beste fachliche Praxis einigen. Im Falle eines Cyberangriffs müssen sie sich gegenseitig über den Zustand ihrer Netze informieren. Sie müssen zusammenarbeiten, um die Folgen zu mindern und die Bedrohung zu beseitigen.~~ ~~5 Sie müssen ein SMS-Umleitungssystem verwenden, das sicherstellt, dass diese Nachrichten in jedem Fall über die Schweiz geleitet werden.~~ ~~6 Sie müssen Signalisierungsnachrichten mithilfe von Filterinstrumenten und nach Methoden filtern, die den international anerkannten Empfehlungen und Normen entsprechen. Das BAKOM kann die anerkannten Empfehlungen und Normen näher bestimmen~~Streichung von Absatz 3 in der vorliegenden Form und Neufassung mit klarer Beschränkung auf technische Cybersicherheitszwecke. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt
Begründung	Absatz 3 verlangt eine permanente und systematische Überwachung der Netze in Echtzeit zur Erkennung von Schwachstellen, Anomalien und Eindringlingen. Der erläuternde Bericht konkretisiert diese Pflicht auf S. 19: Die Überwachung soll sämtliche Teile der Netze erfassen, namentlich Zugangs-, Kern-, Transport-, Signalisierungs- und Interkonnektionsnetze. Dazu sollen Logfiles sämtlicher Netzknoten kontinuierlich erstellt, gesammelt und ausgewertet werden. Anomalien sollen unter anderem durch die Korrelation mehrerer Ereignisse sowie durch Abweichungen vom normalen Systemverhalten erkannt werden. Damit handelt es sich nicht bloss um punktuelle technische Sicherheitskontrollen, sondern um eine sehr umfassende und dauerhafte Auswertungsinfrastruktur. Absatz 3 selbst enthält jedoch keine nähere Begrenzung der dabei bearbeiteten Datenarten, keine Vorgaben zur Aufbewahrungsdauer und keine spezifischen Regeln zu Zugriffsberechtigungen. Gerade bei einer permanenten Auswertung sämtlicher Netzknoten müssen diese Grenzen klar definiert sein. Die Überwachung ist ausdrücklich auf technische Sicherheitszustände, Schwachstellen, Anomalien und Angriffsindikatoren zu beschränken. Kommunikationsinhalte sowie eine allgemeine Analyse von Verkehrsdaten oder des Kommunikationsverhaltens der Kundinnen und Kunden dürfen davon nicht erfasst werden. Dies ist umso wichtiger, als der erläuternde Bericht ebenfalls festhält, dass eine durch diese Überwachung erkannte Gefahr, welche unmittelbar die Sicherheit von Bevölkerung, Unternehmen, Wirtschaft oder Staat bedroht, unverzüglich den Polizeibehörden und den zuständigen Bundesbehörden gemeldet werden soll (S. 19). Die Anbieterinnen sollen anschliessend aktiv mit diesen Behörden zusammenarbeiten, um die Risiken zu minimieren und die Bedrohung zu beseitigen. Technische Netzsicherheit darf nicht zur Hintertür für eine permanente Überwachung der Kommunikation werden.
Anhang	

Rückmeldung zu: Erhöhung der Netzsicherheit und Schutz vor Cyberbedrohungen (Teilrevision der Verordnungen im Fernmeldebereich): Verordnung über Fernmeldeanlagen (FAV)

Generelle Stellungnahme

Rückmeldung zur Gesamtvorlage	Keine Rückmeldung
Begründung	--
Anhang	

Rückmeldung zu: Erhöhung der Netzsicherheit und Schutz vor Cyberbedrohungen (Teilrevision der Verordnungen im Fernmeldebereich): Verordnung des BAKOM über Fernmeldeanlagen (VFAV)

Generelle Stellungnahme

Rückmeldung zur Gesamtvorlage	Keine Rückmeldung
Begründung	--
Anhang	

Rückmeldung zu: Erhöhung der Netzsicherheit und Schutz vor Cyberbedrohungen (Teilrevision der Verordnungen im Fernmeldebereich): Verordnung über die Adressierungselemente im Fernmeldebereich (AEFV)

Generelle Stellungnahme

Rückmeldung zur Gesamtvorlage	Keine Rückmeldung
Begründung	--
Anhang	

Detaillierte Stellungnahme

Titel	Art. 47g Global Titles
Antwortoption	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	~~1 Fernmeldedienstanbieterinnen, denen Adressierungselemente des Numm~~ Zustimmung zum Vermietungs~~plans E.164 zugeteilt wurden, dürfen von diesen Elementen abgeleitete Global Titles erstellen, sofern sie diese in Signalisierungs- und Interkonnektionsnetzen verwenden.~~ ~~2 Sie dürfen die von ihnen erstellten Global Titles nicht an Dritte vermieten. Das BAKOM kann Ausnahmen bewilligen.~~ ~~3 Das BAKOM erlässt die notwendigen technischen und administrativen Vorschrift~~verbot nach Absatz 2; Voraussetzungen für Ausnahmen direkt in der Verordnung festlegen. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt
Begründung	Das Vermietungsverbot ist zu begrüssen. Der erläuternde Bericht zeigt auf S. 27, dass missbräuchlich verwendete Global Titles unter anderem das Abfangen von SMS und Einmalcodes sowie die unrechtmässige Standortverfolgung von Mobilfunkkundinnen und -kunden ermöglichen können. Art. 47g ist damit ein gutes Beispiel dafür, dass technische Netzsicherheit und Grundrechtsschutz keine Gegensätze sind. Die Beschränkung des Zugangs zu sensiblen Signalisierungsressourcen schützt unmittelbar die Vertraulichkeit der Kommunikation, die Privatsphäre und die digitale Integrität der Nutzerinnen und Nutzer. Zu offen bleibt die Ausnahmebestimmung: Während Absatz 2 lediglich festhält, dass das BAKOM Ausnahmen bewilligen kann, nennt der Bericht hierfür konkrete Voraussetzungen wie einen dokumentierten Einzelfall, gewährleistete Sicherheitsmassnahmen und fehlende Alternativen. Diese Schranken sollten direkt in der Verordnung festgehalten werden.
Anhang	