

REGIERUNGSRAT

Regierungsgebäude, 5001 Aarau
Telefon zentral 062 835 12 40
regierungsrat@ag.ch
www.ag.ch/regierungsrat

Per E-Mail

Bundesamt für Kommunikation

tp-secretariat@bakom.admin.ch

26. August 2026

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

Sehr geehrte Damen und Herren

Mit Schreiben vom 27. Mai 2026 wurden die Kantonsregierungen zur Vernehmlassung zur Erhöhung der Netzsicherheit und Schutz vor Cyberbedrohungen (Teilrevision der Verordnungen im Fernmeldebereich [FDV]) eingeladen.

Der Regierungsrat des Kantons Aargau dankt Ihnen für die Gelegenheit, dazu Stellung nehmen zu können. Er unterstützt die vorgesehene Umsetzung im Grundsatz, hat jedoch die folgenden Bemerkungen dazu:

Rolle des Bundesamts für Kommunikation (BAKOM)

Der Regierungsrat regt an, dass die Vorlage an einzelnen zentralen Stellen, an denen die Formulierung "[...] das BAKOM kann [...]" verwendet wird, hinreichend verbindlich ausgestaltet wird. Dies betrifft insbesondere Bestimmungen, wonach das BAKOM Anlagen näher bestimmen, Vorschriften erlassen oder aufsichtsrechtliche Massnahmen anordnen kann. Solche Kann-Formulierungen schaffen zwar den erforderlichen Handlungsspielraum, begründen jedoch keine Pflicht zum Tätigwerden.

Gerade im Bereich kritischer Infrastrukturen und bei erheblichen Risiken für die Betriebs- und Versorgungssicherheit sowie für die staatliche Handlungsfähigkeit sollte geprüft werden, ob in besonders sicherheitsrelevanten Bereichen eine verbindlichere Regelung zweckmässig wäre. Eine klarere Festlegung, unter welchen Voraussetzungen das BAKOM tätig werden soll oder muss, könnte die Rechtssicherheit und die Nachvollziehbarkeit im Vollzug zusätzlich stärken. Der Regierungsrat regt daher an, die einschlägigen Bestimmungen unter diesem Gesichtspunkt nochmals zu überprüfen. Insbesondere in sicherheitsrelevanten Kernbereichen ist zu prüfen, ob eine präzisere Umschreibung der Voraussetzungen für ein Tätigwerden des BAKOM angezeigt ist.

Miterfassung von ausgelagerten Strukturen

Aus Sicht des Regierungsrats könnte die ausdrückliche Verwendung der Bezeichnung "Full Mobile Virtual Operator (Full MVNO)" dazu führen, dass andere relevante Betreiber technischer Infrastruktur von den neuen Sicherheitsvorgaben nicht direkt erfasst werden. Dazu zählen je nach Ausgestaltung insbesondere:

- Mobile Virtual Network Enabler (MVNE): Betrieb technischer Plattformen und netznaher Infrastruktur;

- Light MVNO / Service Provider MVNO: je nach Modell insbesondere Provisioning-Prozesse oder Teile des SIM-Managements;
- Mobile Virtual Network Aggregator (MVNA): häufig in Kombination mit MVNE-Funktionen.

Auch wenn mit den "Mobilfunkkonzessionärinnen" (MNO) und den "Full MVNO" alle für Endkunden relevanten Anbieter abgedeckt werden können, folgt daraus nicht zwingend, dass diese Akteure auch die gesamte sicherheitsrelevante technische Infrastruktur selbst betreiben. Dies zeigt sich beispielhaft am vorgeschlagenen Art. 96f FDV. Gerade sicherheitskritische Fernmeldeanlagen oder Teile davon können jedoch von Subunternehmern oder anderen beigezogenen Dritten betrieben werden, etwa von einem MVNE. Ausgelagerte Strukturen sollten daher in den entsprechenden Bestimmungen ausdrücklich oder funktional miterfasst werden, um Unschärfen bei der Adressierung und Verantwortungszuordnung zu vermeiden.

Verifizierte Herkunft von Mobilfunkverbindungen

Im Interesse einer sicheren und vertrauenswürdigen Signalisierung im Mobilfunk regt der Regierungsrat folgende Ergänzung der Vorlage an:

Als Endkundenanbieter gilt derjenige Anbieter, der den Vertrag mit dem Endkunden abschliesst. Bei neuen oder weiterentwickelten Mobilfunkstandards ist eine eindeutige Identifikation des originierenden Endkundenanbieters dem terminierenden Endkundenanbieter bei der Signalisierung zu übermitteln. Die MNO sowie die Full MVNO wirken direkt oder über ihre Zulieferer, soweit technisch und international möglich, darauf hin. Die eindeutige Identifikation ist mittels kryptographischer Verfahren, die dem Stand der Technik entsprechen, vor Fälschung zu schützen. Das BAKOM legt die Anforderungen an eine vertrauenswürdige Zertifikatsstruktur fest, insbesondere hinsichtlich Ausstellung, Verwaltung, Sperrung und Anerkennung kryptographischer Zertifikate sowie der Validierung der übermittelten Anbieteridentifikation.

Fehlt die Identifikation des originierenden Endkundenanbieters oder kann sie nicht erfolgreich validiert werden, so darf die Herkunft der Verbindung gegenüber dem terminierenden Endkundenanbieter sowie dessen Endkunden nicht als verifiziert ausgewiesen werden. Die technischen und organisatorischen Voraussetzungen sind so auszugestalten, dass terminierende Endkundenanbieter ihren Endkunden auf freiwilliger Basis Dienstleistungen zur Kennzeichnung, Filterung oder Blockierung bestimmter originierender Endkundenanbieter sowie nicht verifizierter Verbindungen anbieten können.

Der Regierungsrat dankt Ihnen für die Berücksichtigung seiner Vernehmlassung.

Freundliche Grüsse

Im Namen des Regierungsrats

Stephan Attiger
Landammann

Joana Filippi
Staatsschreiberin