

An die
Rundfunk und Telekom Regulierungs-GmbH
Mariahilfer Straße 77-79
1060 Wien

Per E-Mail an:
konsultationen@rtr.at

Wien, am 07.09.2026

Stellungnahme der ISPA zur Novelle der Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020)

Sehr geehrte Damen und Herren,

der Verband der österreichischen Internetanbieter ISPA bedankt sich für die Möglichkeit, zum Entwurf der Novelle der TK-NSiV 2020 Stellung zu nehmen.

Wir unterstützen ausdrücklich das Ziel eines hohen Cybersicherheitsniveaus. Nach unserer Einschätzung muss dieses Ziel jedoch im Lichte der NIS-2-Richtlinie sowie des NISG 2026 erreicht werden. Aus dieser Systematik folgt, dass parallele sektorspezifische Sicherheitsvorgaben weitgehend zurückgenommen und in den NIS2-Rahmen integriert werden sollen. Wir begrüßen ausdrücklich, dass die RTR im laufenden Verfahren bereits die Aufhebung der Schwellenwerte der TK-NSiV 2020 angekündigt hat; die konsequente Fortführung dieses Ansatzes gebietet jedoch auch die Aufhebung des § 6 und damit die **vollständige Aufhebung der TK-NSiV 2020**.

ISPA-Forderungen im Überblick:

- **Vollständige Aufhebung der TK-NSiV mit 1. Oktober 2026**, zeitgleich mit dem Inkrafttreten des NISG 2026.
- **Abschließende Regelung der Cybersicherheit im Telekommunikationssektor** über NIS-2, DVO (EU) 2024/2690, NISG 2026 sowie die dazugehörigen Durchführungsverordnungen.

- **Vermeidung von Doppelregulierung und „Goldplating“** gegenüber der NIS2 sowie der DVO (EU) 2024/2690 und den unionsrechtlich harmonisierten Anforderungen.
- **Adressierung etwaiger telekommunikationsspezifischer Besonderheiten innerhalb des NIS-Rahmens** – sofern sich nach ersten Vollzugserfahrungen tatsächlich Regelungslücken zeigen.
- **Beseitigung bestehender Widersprüche** zwischen § 6 TK-NSiV und dem NISG 2026 bei Nachweismodalitäten, Frequenz, Behördenzuständigkeit und technischen Detailvorgaben.

1. Vorrang einer einheitlichen NIS2-Regulierung

Die NIS-2-Richtlinie zielt darauf ab, die bisherige Zersplitterung der Cybersicherheitsregulierung zu überwinden. Cybersicherheitsanforderungen sollen möglichst einheitlich, kohärent und risikobasiert ausgestaltet werden, um regulatorische Fragmentierung und divergierende nationale Sonderregelungen zu vermeiden. So spricht etwa ErwGr. 22 davon, dass, um eine Fragmentierung der Cybersicherheitsbestimmungen zu vermeiden, die Kommission bei weiterem sektorspezifischem Regelungsbedarf zunächst prüfen soll, ob dieser durch einen Durchführungsrechtsakt nach NIS2 abgedeckt werden kann.

Besonders im Bereich der elektronischen Kommunikationsnetze wurden folglich die bisherigen sektorspezifischen Sicherheitsvorgaben der Art. 40 und 41 des Europäischen Kodex für die elektronische Kommunikation aufgehoben und in das NIS2-Regime überführt, explizit um die einschlägigen Verpflichtungen zu vereinheitlichen und zu straffen (siehe ErwGr. 92). Zusätzliche nationale Sonderregeln bedürfen vor diesem Hintergrund einer eigenständigen sachlichen Rechtfertigung. Auch ErwGr. 95 spricht von einer Harmonisierung der Cybersicherheitsregelungen explizit für Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste.

Der unionsrechtlich vorgesehene Weg besteht daher nicht darin, nationale sektorspezifische Sonderregeln vorsorglich fortzuführen. Vielmehr soll zunächst geprüft werden, ob ein zusätzlicher Regelungsbedarf unionsweit durch einen Durchführungsrechtsakt nach NIS2 abgedeckt werden kann.

Das doppelte Goldplating wird deutlich, wenn die unionsrechtliche Ausgangslage und die nationale Umsetzung gemeinsam betrachtet werden: Die EU-Durchführungsverordnung (2024/2690) gilt originär nicht für Telekommunikationsunternehmen. Österreich erstreckt ihre Anforderungen durch die nunmehr konsultierte Risikomanagementmaßnahmen-Verordnung (RMMV) gemäß § 32 Abs. 5 NISG 2026 sowie durch die Verordnung über die Erheblichkeit von Cybersicherheitsvorfällen (ECV) gemäß § 35 Abs. 3 NISG 2026 nunmehr auch auf Telekommunikationsanbieter und -betreiber. Dies

bildet das **erste zusätzliche nationale Regelungsniveau** nach dem NISG 2026.

Daneben hält Österreich mit der TK-NSiV 2020 ein weiteres eigenständiges sektorspezifisches Regelungsniveau mit zusätzlichen Nachweis-, Melde- und technischen Detailanforderungen aufrecht. Dieses bildet das **zweite zusätzliche nationale Regelungsniveau**. Damit entsteht **doppeltes Goldplating**: Telekommunikationsunternehmen werden einerseits national den Anforderungen der **EU-Durchführungsverordnung** mittels RMMV und ECV unterworfen, obwohl die EU-Durchführungsverordnung originär nicht für sie gilt, und andererseits zusätzlich mit der TK-NSiV 2020 konfrontiert. Diese Kumulation widerspricht dem Ziel der NIS2, die einschlägigen Verpflichtungen zu vereinheitlichen und regulatorische Fragmentierung zu vermeiden.

Eine solche Entwicklung soll durch den Vorschlag der Kommission COM (2026) 13 vom 20. Jänner 2026 ausdrücklich untersagt werden. Danach wären zusätzliche nationale technische oder methodologische Sicherheitsanforderungen verboten, sobald die Kommission den betreffenden Sektor mittels Durchführungsrechtsakt harmonisiert. Dadurch sollen nationales Goldplating, divergierende Anforderungen und zusätzliche Belastungen für grenzüberschreitend tätige Unternehmen verhindert werden.

Auch der österreichische Gesetzgeber verfolgt mit dem NISG 2026 und dem nunmehr gefassten § 44 TKG 2021 einen subsidiären Ansatz. Betreiber und Anbieter haben Cybersicherheitsmaßnahmen primär „nach Maßgabe anderer Rechtsvorschriften“, insbesondere des NISG 2026 samt seinen Verordnungen, zu treffen. Nur wenn diese Rechtsvorschriften nicht ausreichen, dürfen durch Verordnung nähere technische und organisatorische Sicherheitsmaßnahmen festgelegt werden. Sektorspezifische Regelungen im TKG sind daher **subsidiär** und nur dann gerechtfertigt, wenn konkrete telekommunikationsspezifische Risiken im NIS-Rahmen nicht hinreichend erfasst sind.

Richtig geht die zuständige NIS-Behörde in Wahrnehmung ihrer Verordnungskompetenzen gemäß NISG 2026 vor: In den Erläuterungen zur Risikomanagementmaßnahmen-Verordnung (RMMV) gemäß § 32 Abs. 5 NISG 2026 sowie zur Verordnung über die Erheblichkeit von Cybersicherheitsvorfällen (ECV) gemäß § 35 Abs. 3 NISG 2026 wird festgehalten, dass „von sektorspezifischen Anforderungen initial abgesehen werden soll, da dies mangels konkreter Erfahrungswerte aus dem Vollzug des NISG 2026 nicht treffsicher abgebildet werden kann.“ Folglich verfolgt selbst die zuständige Behörde den Ansatz, zunächst Erfahrungen aus dem Vollzug des NISG 2026 zu sammeln und erst auf dieser Grundlage festzustellen, ob es neben dem NISG 2026 und den sektorübergreifenden Verordnungen überhaupt noch weiterer sektorspezifischer Maßnahmen bedarf.

Dieser Ansatz steht in unmittelbarem Widerspruch zur Fortgeltung der TK-NSiV 2020. Die zuständige Behörde will zunächst Vollzugserfahrungen mit dem NISG 2026 und den sektorübergreifenden Verordnungen sammeln und erst danach beurteilen, ob zusätzlicher sektorspezifischer Regelungsbedarf besteht. Der Fortbestand der TK-NSiV würde diese Prüfung vorwegnehmen, obwohl die dafür maßgeblichen Erfahrungswerte noch gar nicht vorliegen.

Zudem beruht die TK-NSiV 2020 auf § 16a Abs. 9 TKG 2003 und steht damit für einen Sicherheitsrahmen, der durch die unionsrechtliche und nationale Neuausrichtung des Cybersicherheitsrechts überholt ist. Die vollständige Aufhebung der TK-NSiV 2020 ist daher folgerichtig: Die NIS2-Regulierung, das NISG 2026 und die dazugehörigen Verordnungen erfassen den Telekommunikationssektor bereits; die TK-NSiV fügt dem lediglich eine weitere parallele Regelungsebene hinzu.

Die vollständige Aufhebung der TK-NSiV 2020 entspricht somit sowohl der unionsrechtlichen Zielsetzung einer einheitlichen Cybersicherheitsregulierung als auch dem Ansatz der zuständigen NIS-Behörde. Sollte sich nach den ersten Vollzugserfahrungen tatsächlich eine Regelungslücke zeigen, kann diese im vorgesehenen unionsrechtlichen und nationalen Verfahren gezielt und treffsicher adressiert werden.

2. § 6 TK-NSiV 2020 im Verhältnis zu NIS2

Die Begründung für eine Fortgeltung des § 6 TK-NSiV mit dem Hinweis auf dessen Umsetzung im Hinblick auf die 5G-Toolbox überzeugt im heutigen Rechtsrahmen nicht mehr.

Hinzu kommt, dass die in der 5G-Toolbox enthaltenen Maßnahmen selbst keinen verbindlichen Unionsrechtsakt darstellen und daher für sich genommen die Aufrechterhaltung zusätzlicher nationaler Sicherheitsverpflichtungen nicht rechtfertigen kann. Die wesentlichen Inhalte der 5G-Toolbox sind mittlerweile in die NIS-2-Systematik eingeflossen, insbesondere in die Vorgaben zum Risikomanagement, zu Lieferketten und Zugriffsschutz, zu Entwicklung und Wartung, zum Schwachstellenmanagement und zur Business Continuity sowie in die Nachweis- und Auditpflichten. **Dies gilt insbesondere auch für die unionsweit koordinierten Risikobewertungen kritischer Lieferketten.** Vor diesem Hintergrund bedarf es einer eigenständigen sachlichen Rechtfertigung dafür, weshalb § 6 TK-NSiV über den bereits bestehenden NIS-2-Rahmen hinausgehende Anforderungen erforderlich macht.

Eine solche Rechtfertigung ist nur dann gegeben, wenn § 6 TK-NSiV ein spezifisches, durch den bestehenden NIS-2-Rahmen nicht hinreichend erfasstes Risiko adressiert. Fehlt es hieran, lässt

sich eine eigenständige Fortgeltung der Bestimmung unter dem Maßstab des § 44 TKG sachlich nicht rechtfertigen.

Die konkreten Überschneidungen und Widersprüche zeigen sich vor allem in vier Punkten:

- **Nachweis des Informationssicherheitsmanagements (§ 6 Abs. 1 TK-NSiV):**

§ 6 Abs. 1 TK-NSiV verlangt alle drei Jahre die automatische Vorlage eines ISO-27001-Reports an die RTR. Das NISG 2026 sieht demgegenüber vor, dass ein solcher Nachweis auf Anfrage der Cybersicherheitsbehörde vorzulegen ist und nicht älter als zwei Jahre sein darf. Es bestehen somit Widersprüche in Modus (automatisch vs. auf Anforderung), Frequenz und Behördenzuständigkeit (RTR vs. Cybersicherheitsbehörde) – mit entsprechendem Mehraufwand für Unternehmen und Behörden.

- **Konformitätserklärung (§ 6 Abs. 2 TK-NSiV):**

§ 6 Abs. 2 TK-NSiV sieht den Nachweis der Einhaltung bestimmter, im Jahr 2020 festgelegter 3GPP- und ENISA-Standards vor. Diese Verpflichtung wird durch die NIS-2-Regelungen funktional abgedeckt. Während § 6 Abs. 2 TK-NSiV auf einen statischen Katalog technischer Standards abstellt, verfolgt NIS-2 einen umfassenden und risikobasierten Sicherheitsansatz, der laufend am Stand der Technik ausgerichtet wird. Die mit § 6 Abs. 2 TK-NSiV verfolgten Schutzziele werden dadurch vollumfänglich erfasst. Die Bestimmung kann daher entfallen, ohne dass dadurch das Sicherheitsniveau verringert wird.

- **Spezifische technische Vorgaben (§ 6 Abs. 3 Z 1–7 TK-NSiV):**

Die in § 6 Abs. 3 TK-NSiV festgelegten Anforderungen – etwa zu Multi-Edge-Computing, Basisstationen, 5G-Sicherheitsüberprüfungen oder Multi-Vendor-Strategien – finden inhaltlich bereits in der DVO, dem NISG 2026 und der RMMV Berücksichtigung. Der risikobasierte Ansatz des NISG 2026 gewährleistet daher, dass die damit verfolgten Schutzziele auch ohne die dauerhafte Festlegung technologiespezifischer Einzelvorgaben erreicht werden können. So wird etwa die mit der Multi-Vendor-Strategie bezweckte Risikoreduzierung bereits durch die Anforderungen an die Sicherheit der Lieferkette nach dem NISG 2026 erfasst. Einer eigenständigen und dauerhaften Vorgabe einer bestimmten technischen Strategie bedarf es insoweit nicht.

- **Liste sicherheitsrelevanter Komponenten (§ 6 Abs. 4 TK-NSiV):**

Die in § 6 Abs. 4 TK-NSiV normierte Pflicht zur regelmäßigen Übermittlung von Hersteller- und Komponentenlisten dient der behördlichen Bewertung von Lieferketten- und

Komponentenrisiken. Genau dieses Ziel wird durch die Anforderungen an das Lieferkettenrisikomanagement und die behördlichen Nachweis- und Auskunftspflichten des NISG 2026 vollständig erfasst. Die Bestimmung ist damit eine entbehrliche Doppelregulierung. Insgesamt entsteht so das Bild einer zusätzlichen nationalen Sonderordnung, die keinen eigenständigen Mehrwert bietet, wohl aber die Komplexität erhöht, Mehrfachberichterstattung erzeugt und die klare Zuordnung von Zuständigkeiten erschwert.

3. Schlussfolgerung

Die TK-NSiV 2020 ist in ihrer Gesamtheit durch die unionsrechtliche und nationale Neuausrichtung des Cybersicherheitsrechts überholt. Die Cybersicherheitsanforderungen für den Telekommunikationssektor werden durch die NIS-2-Richtlinie, das NISG 2026 und die dazugehörigen nationalen Durchführungsverordnungen bereits in einem einheitlichen und risikobasierten Rahmen geregelt. **Die parallele Fortgeltung der TK-NSiV 2020 neben den sektorübergreifenden nationalen Durchführungsverordnungen schafft ein nationales Goldplating, das dem gesetzgeberischen Willen der EU widerspricht und gerade jene regulatorische Fragmentierung verstärkt, die durch NIS2 bereits überwunden wurde.** Auch die zuständige NIS-Behörde will zunächst Vollzugserfahrungen mit dem NISG 2026 sammeln und erst auf dieser Grundlage beurteilen, ob überhaupt weiterer sektorspezifischer Regelungsbedarf besteht. Der Fortbestand der TK-NSiV würde diese Prüfung vorwegnehmen, obwohl die maßgeblichen Erfahrungswerte noch nicht vorliegen.

Die ISPA fordert daher die vollständige Aufhebung der TK-NSiV 2020 zum 1. Oktober 2026, zeitgleich mit dem Inkrafttreten des NISG 2026.

Damit wird der Schutz der Telekommunikationsnetze und -dienste nicht reduziert, sondern abschließend, kohärent und europarechtskonform im Rahmen der NIS2-Regulierung, dem NISG 2026 sowie in den dazugehörigen Verordnungen sichergestellt.

Für Rückfragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen



Mag. Stefan Ebenberger
Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von rund 220 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.