WIRTSCHAFTSKAMMER ÖSTERREICH

Rundfunk- und Telekom
Regulierungs-GmbH
Mariahilferstraße 77-79
1060 Wien
konsultationen@rtr.at

Wiedner Hauptstraße 63 | Postfach 195
1045 Wien
T +43 (0)5 90 900-DW | F +43 (0)5 90 900-243
E rp@wko.at
W http://wko.at

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
	Rp 476.0016/2020/WP/VR Dr. Winfried Pöcherstorfer	4002	5.6.2020

Öffentliche Konsultation der RTR-GmbH zum Entwurf einer Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste im Zusammenhang mit Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G-Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen (Telekom-Netzsicherheitsverordnung 2020 - TK-NSiV 2020) - Stellungnahme

Sehr geehrte Damen und Herren,

die Wirtschaftskammer Österreich bedankt sich für die Übermittlung der Einladung zur Teilnahme an der öffentlichen Konsultation der RTR-GmbH zum Entwurf einer Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste im Zusammenhang mit Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G-Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen (Telekom-Netzsicherheitsverordnung 2020 - TK-NSiV 2020) und nimmt hiezu - unter besonderer Berücksichtigung der seitens des in der Bundesparte Information und Consulting organisierten Fachverbandes der Telekommunikations- und Rundfunkunternehmungen übermittelten Überlegungen - wie folgt Stellung:

I. Allgemeines

Eingangs erlauben wir uns, auf die Stellungnahme des Fachverbandes der Telekommunikations- und Rundfunkunternehmungen vom 14. Februar 2020 zum unmittelbar verwandten Themenkreis an die RTR GmbH zu verweisen, in der eine ausführliche Auseinandersetzung mit der „Befragung der Bieter der 5G Frequenzvergabe 3,4 - 3,8 GHz zur Mitteilung der Europäischen Kommission betreffend die ‚Sichere 5G-Einführung in der EU - Umsetzung des EU-Instrumentariums' (COM(2020) 50) - 5G Toolbox" stattgefunden hat. Auf die darin skizzierte sog 5G-Toolbox nimmt auch die vorliegende Konsultation einer TK-NSiV 2020 Bezug.

Angemessene Regelungen für eine höhere Netzsicherheit sind gerade im Hinblick auf die fortschreitende Digitalisierung wichtig und sinnvoll. Netzsicherheit ist dabei kein neues Thema: Die Branche hat einen hohen Sicherheitsstandard, weil sie schon seit Jahren zahlreiche Maßnahmen

implementiert hat, um diesen zu gewährleisten und den weiteren Entwicklungen anzupassen. So wurde zB von der RTR im Rahmen der „Branchenrisikoanalyse" bereits ein umfangreicher Risikokatalog samt Maßnahmen erarbeitet, den die Unternehmen implementiert haben.

Dabei kommt es darauf an, dass allfällige Maßnahmen in einem so wettbewerbsintensiven Marktumfeld wie in Österreich keine negativen Auswirkungen auf den Wettbewerb haben, sohin mit Bedacht gewählt und mit vergleichbarer Belastung im Sinne der Wettbewerbsneutralität für die Marktteilnehmer einhergehen müssen. Es gilt dabei, Innovationen nicht zu behindern und auf bestehende Netze und deren - im Vergleich der Netzbetreiber untereinander durchaus unterschiedlichen - Architekturen Rücksicht zu nehmen.

II. Zum Vorschlag einer TK-NSiV 2020 im Einzelnen:

§ 1 Zweck und Anwendungsbereich

Da der vorliegende Entwurf auf § 16a Abs 9 TKG fußt, finden sich hier keine überraschenden oder neuen Ausführungen, die über das hinausgehen, was bislang grundsätzlich als Regelungszweck von §§ 16 und 16a TKG angesehen wurde.

Aufgrund der Etablierung von Diensten, die Kommunikationsdienste vermehrt funktional substituieren, aber bislang nicht erfasst sind, sollte der Anwendungsbereich einschließlich der folgenden Meldepflichten nicht nur die Betreiber von elektronischen Kommunikationsnetzen und -diensten treffen, sondern auch sog Over the Top-Diensteanbieter (OTT), wie zB Whatsapp oä. Diese OTT-Dienste stehen zunehmend in Konkurrenz zu klassischen Telekommunikationsdiensten und sollten daher den gleichen Regeln unterliegen. In der regulatorischen Praxis unterliegen letztere einer strikteren Regulierung als OTT-Dienste, was zu einer unsachlichen Ungleichbehandlung führt. Die TK-NSiV sollte daher auch im Hinblick auf den EECC versuchen, gleiche Rahmenbedingungen zu schaffen.

§ 2 Begriffsbestimmungen

Hier regen wir einige Adaptionen zu den verwendeten Begriffen an.

Es erschließt sich nicht, was unter einem „bestimmten Vertrauensniveau" in **§ 2 Z 1** zu verstehen ist. Der Begriff ist jedoch zentral, weil auf diesem Vertrauensniveau Ereignissen entgegengewirkt werden soll, sohin es der generelle Maßstab ist, an dem sich allfällige Maßnahmen messen lassen müssen.

Zu **§ 2 Z 5** sollte noch klärend ausgeführt werden, wie Hybridprodukte eingeordnet werden, nämlich als Festnetzprodukte. Dazu sollten noch ausdrücklich M2M-Produkte ausgenommen werden, da hier Dienste in Produkte integriert werden, die großteils außerhalb des Anwendungsbereichs dieser Verordnung vertrieben werden.

Unter die Definition des Sicherheitsvorfalls in **§ 2 Z 7** könnten auch sog Datenleaks (also die nicht autorisierte, wie auch immer geartete, Veröffentlichung von personenbezogenen Daten) fallen. Dies hätte zur Folge, dass neben einer Meldung bei der Datenschutzbehörde auch die Vorschriften der TK-NSiV einschlägig wären, was eine Doppelstruktur beim Thema Datenschutz schaffen würde.

Wir gehen davon aus, dass Datenleaks ausschließlich der DSGVO unterliegen und im Zuständigkeitsbereich der Datenschutzbehörde verbleiben, weshalb eine Klarstellung in den Erläuterungen hilfreich wäre.

Die Definition von „unverzüglich" in **§ 2 Z 8** halten wir für verzichtbar. Es gibt die allgemein anerkannte (juristische) Definition, dass ein Handeln dann unverzüglich ist, wenn es ohne schuldhaftes Zögern erfolgt. Insofern ist deren Anführung in einer Verordnung nicht erforderlich, wenn auch unschädlich. Von hoher Relevanz ist vielmehr die konkrete Verknüpfung des Begriffes mit Handlungsverpflichtungen der Betreiber. Dazu unten mehr.

Die Definition eines 5G-Netzes in **§ 2 Z 9** geht aus unserer Sicht zu weit. Einerseits zählt die aktuelle Formulierung annähernd alle Netzbestandteile dem „5G-Netz" hinzu, sobald eine 5G-Funktion vom Betreiber angeboten wird. Andererseits suggeriert die Formulierung 5G-Standalone (5G-SA) Netze, da in der Praxis die diskutierten Charakteristika wie „niedrige Latenzzeit" oder „ultra-hohe Zuverlässigkeit" nur bei 5G-SA erzielbar sind. 5G-SA wird in Österreich von den meisten Betreibern erst in den nächsten Jahren ausgerollt und aktuell noch nicht angeboten. Die Definition „5G-Netz" sollte auf 5G-SA eingeschränkt werden.

§ 3 Informationspflichten

Wir regen an, in **Absatz 1** das Wort „öffentlichen" vor „elektronischen Kommunikationsnetzen oder -diensten" einzufügen. Damit sind interne Netzwerke ausgenommen, die ausschließlich von einer bestimmten Personengruppe für interne Zwecke genutzt werden (zB Campus-Netzwerke). Solche Netzwerke sind von außen nicht zugänglich und können über das öffentliche Netz nicht erreicht werden, sodass hier kein Regelungsbedarf im Sinne von § 16a TKG besteht.

Wir begrüßen die Aufteilung in eine Erst- und eine Folgemeldung. Dies trägt der Situation beim Betreiber anlässlich eines Sicherheitsvorfalls Rechnung, wenn es gilt, personelle Kapazitäten primär zur Behebung eines Vorfalls einzusetzen und nicht mit weitergehenden Meldeverpflichtungen zu überlasten. Gerade im Hinblick auf kleinere Unternehmen ist das sehr wichtig.

Problematisch ist die Formulierung „unverzüglich ab Kenntnis des Vorfalls". Dies deshalb, weil Betreiber regelmäßig das Interesse haben, Warnhinweise (§ 4) an die Behörde zu übermitteln und dann abwarten zu können, ob im weiteren Verlauf der Entwicklung eines Vorfalls es überhaupt zu Überschreitungen der Schwellenwerte (gemäß der Matrix aus Zahl der Betroffenen und Dauer) kommt oder der Notruf betroffen ist. Daher sollte klarstellend eine Änderung des Textes dahingehend erfolgen, dass eine Kenntnis eines meldepflichtigen Vorfalls erst ab Überschreitung der Schwellenwerte besteht.

Dabei sollte auch klargestellt werden, dass mit einem Warnhinweis nach § 4 automatisch dem Kriterium der Unverzüglichkeit einer nachgelagerten Meldung nach Absatz 2 genüge getan ist.

Für kleine und mittelgroße Unternehmen stellt ein unverzügliches Melden außerhalb der Geschäftszeiten generell ein großes Problem dar. Daher sollte weiters für diese Unternehmen das Melden auf die Zeiten des technischen Supports beschränkt sein können oder allenfalls für eine unverzügliche Meldung eine Meldefrist von 24 Stunden in den Erläuterungen festgehalten werden.

Erst- und Folgemeldungen sind nach dem Entwurf über das Meldeportal der Regulierungsbehörde einzubringen. Hier halten wir eine Schnittstelle für automatisierte Meldungen für sinnvoller. Meldungen könnten darüber direkt aus den Incident-Reporting-Systemen der Betreiber erfolgen, ohne

dass hier in einer kritischen Situation auch noch manuelle Schritte erforderlich wären. Wir regen hier daher die Implementierung einer solchen Schnittstelle als Zusatzoption an.

Die Folgemeldung soll binnen 24 Stunden ab Wiederherstellung der betroffenen Dienste erfolgen. Diese Frist ist für eine aussagekräftige und in diesem Sinne für den Regulator sinnvoll verwertbare Meldung deutlich zu kurz. Die Folgemeldung sollte doch weitergehende, qualifizierte Einschätzungen des Vorfalls ermöglichen. Folglich sollten im Idealfall die zu machenden Ausführungen mit angemessener Ausführlichkeit und Tiefe in der Analyse des Vorfalls erfolgen - dafür sind 24 Stunden zu kurz angesetzt. Drei normale Werktage wäre hier ein sinnvoller Zeitraum bis zur Folgemeldung.

In **Absatz 2** sind Schwellenwerte für beträchtliche Auswirkungen definiert. Diese erleichtern grundsätzlich die Implementierung in die Meldesysteme der Betreiber. Allerdings wird hier eine eigene Matrix aufgestellt, statt sich an den NIS-Bestimmungen zu orientieren.

Erschwerend ist, dass hier neben absoluten Zahlen auf einen Prozentwert von Nutzern einer Dienstekategorie im Bundesgebiet abgestellt wird. Dieser Quotient lässt sich für den einzelnen Betreiber nicht ermitteln. Leider wird dazu in den Erläuterungen ausgeführt, dass unter den betroffenen Teilnehmern der jeweiligen Dienstekategorie nur jene Teilnehmer zu verstehen sind, „die dem Anbieter des betroffenen Kommunikationsdienstes zuzurechnen sind." Das führt dazu, dass kleinere Anbieter sehr viel schneller den prozentualen Schwellenwert erreichen können, was wohl von der TK-NSiV 2020 generell nicht intendiert ist. Daher sollte in den Erläuterungen der Satz gestrichen und auf die Dienstkategorie im Bundesgebiet abgestellt werden.

Im Ergebnis ist es am einfachsten, wenn es weiter klare Zahlenveröffentlichungen der Behörde mit absoluten Zahlen gibt, wie sie die RTR bislang schon veröffentlicht hat, und von relativen Zahlen Abstand genommen wird.

Wir begrüßen in **Absatz 3**, dass es den Betreibern überlassen ist, über welche Kanäle sie die Öffentlichkeit informieren. Bei der Beurteilung der Frage, ob die Bekanntgabe des Vorfalls im öffentlichen Interesse liegt, ist aufgrund der Implikationen für den Betreiber ein sehr strenger Maßstab anzulegen. Eine solche Veröffentlichung muss unbedingt der Ausnahmefall bleiben.

§ 4 Warnhinweis

Wir begrüßen die Möglichkeit für die Betreiber, freiwillige Meldungen zu übermitteln. Dies ist insbesondere in der Ausgestaltung sinnvoll, wenn im Fall einer später festgestellten Meldepflicht nach § 3 ein Warnhinweis nach § 4 um die Punkte für eine Folgemeldung ergänzt werden kann und die Meldung nach § 4 als Erstmeldung nach § 3 gilt und ein schuldhaftes Zögern ausschließt. In diesem Sinne sollte daher eine Klarstellung im Text oder in den Erläuterungen erfolgen. Im Ergebnis würde die Behörde frühzeitig von potentiellen Vorfällen erfahren, sohin wäre dem Zweck von § 3 genüge getan und die Betreiber wären hinsichtlich des Erfordernisses einer unverzüglichen Meldung auf der sicheren Seite.

In Bezug auf die Möglichkeit der Behörde, den Warnhinweis mit Einwilligung des Einmelders an den Bundesminister für Inneres weiterzuleiten, darf der Einwilligungsvorbehalt nicht umgangen werden können. Daher ist der letzte Satz in Absatz 2 zu streichen.

§ 5 Mindestsicherheitsmaßnahmen

Dieser Absatz fasst im Grunde lediglich zusammen, was bislang bereits unter der Maßgabe von § 16a Abs 1 bis 3 TKG gemäß dessen allgemeiner Auslegung praktiziert wurde - insbesondere die Orientierung an den „Technical Guidelines on Minimum Security Measures" der ENISA entspricht der aktuellen Praxis.

Hier regen wir an, dass die RTR (bzw TKK) als Behörde, der die Unternehmen regulatorisch unterworfen sind, allfällige Zu- und Ausarbeitungen für und von Information Security Policies - die im Ergebnis die relevante Behördenmeinung für die Anwendung der Bestimmung widerspiegeln - dem Fachverband Telekom-Rundfunk (der gesetzlichen Interessensvertretung aller betroffenen Unternehmen) in transparenter Weise zugänglich macht und deren Weiterverbreitung gestattet.

Wir regen weiters an, die Wortentlehnung „Information Security Policy" aus dem Englischen durch den Ausdruck Informationssicherheitsrichtlinie(n) zu ersetzen. Systematisch ist anzumerken, dass eine „Information Security Policy" bereits ausdrücklich in Absatz 1 gefordert wird und ihre Anführung unter Ziffer 1 unklar ist bzw keinen Sinn ergibt.

Hinsichtlich der Angaben zum Personal sollten allgemeine Informationen genügen und keine personenbezogenen Daten angegeben werden müssen.

Schließlich ist klarzustellen, dass die Erfüllung der Mindestsicherheitsmaßnahmen keiner Auditierungspflicht unterliegt. Hier genügt es, wenn Betreiber am Maßstab der in den Erläuterungen genannten „Technical Guideline on Security Measures" der ENISA in einem Selbstaudit die Erfüllung überprüfen.

§ 6 Sicherheitsanforderungen an 5G-Netze

Grundsätzlich können wir nicht nachvollziehen, wieso in den Erläuterungen im Zusammenhang mit 5G-Netzen pauschal von einem erhöhten Risiko durch den Betrieb von 5G-Netzen die Rede ist. Hier werden womöglich Risiko und Bedeutung von 5G verwechselt. Leider bleibt auch die Mitteilung der Kommission vom 29. Jänner 2020 hierzu recht diffus, wenn sie die vorgeschlagenen Maßnahmen pauschal mit Cybersicherheit begründet, aber im Ergebnis erkennbar auf nichteuropäische Lieferanten von Netzwerkausrüstung zielt. Dazu verweisen wir auf die Äußerungen des Fachverbandes der Telekommunikations- und Rundfunkunternehmungen in der ausführlichen Stellungnahme vom 14. Februar 2020.

Kritisch sehen wir das Abstellen auf eine bestimmte Teilnehmerzahl, ab der das Bestehen eines Informationssicherheitsmanagementsystems nachzuweisen ist. Das bloße Abstellen auf die Anzahl der Teilnehmer greift zB in den Fällen zu kurz, wo ein einzelner Teilnehmer iSv § 3 Z 19 TKG zahlreiche Anwendungen steuert. Besser wäre es, auf die Anzahl der Anwendungen oder auf Netzabschlusspunkte abzustellen. Alternativ könnte man die Sicherheitsanforderungen ganz allgemein an Mobilfunkdiensteanbieter richten und Ausnahmen für kleine Anbieter schaffen.

Problematisch ist eine Auditierung auf Basis der in den EB genannte Norm ISO 27 001. Dies würde bei vielen Betreibern enorm hohe Kosten mit sich bringen und einen großen Personaleinsatz erfordern, der kaum zu leisten ist, gerade auch im Hinblick auf die zeitlichen Vorgaben. Es sollte daher dringend den betroffenen Unternehmen überlassen sein, welche Normen für den Auditbericht zugrunde gelegt werden. Die Erstellung des Auditberichts sollte so einfach wie möglich zu gestalten sein, um die Kosten-Nutzen Relation und die Verhältnismäßigkeit zu wahren.

Der in **Absatz 2** vorgegebenen Zeitrahmen für die Vorlage von Konformitätserklärungen erstmalig bis zum 30. Juni 2021 ist zu knapp bemessen. Außerdem sind im Anhang 1 zu viele Standards aufgelistet. Die Beurteilung der Konformität mit all diesen Standards ist sehr aufwändig und verursacht hohe Kosten - bei den Betreibern wie auch bei der überprüfenden Behörde. Bei der Verpflichtung zur Konformität mit Standards muss immer bedacht werden, dass sich diese weiterentwickeln und neue hinzu oder an ihre Stelle treten können. Auch solche alternativen Standards zu befolgen muss anerkannt werden. Und umgekehrt darf es keine Pflicht geben, nachfolgende Novellierungen von Standards berücksichtigen zu müssen.

Es ist außerdem nicht klar, auf welche Bereiche eines Unternehmens sich die Auditierung bezieht. Hier sind sinnvolle Eingrenzungen vonnöten. Besonders wichtig ist, hier allfällige Nachweisepflichten zunächst einmal ausschließlich auf 5G-Ausrüstung zu beziehen, weil für ältere Komponenten von den Lieferanten oft keine Informationen dazu geliefert werden können. Daher sollten auch alle Standards aus dem Anhang gestrichen werden, die nicht ausschließlich 5G adressieren.

Wie bereits in der Stellungnahme des Fachverbandes vom 14. Februar 2020 angemerkt, sehen wir darüber hinaus generell einen sinnvollen Regulierungsansatz darin, Hersteller und Lieferanten zur Konformität mit den angeführten Standards zu verpflichten und ihnen andernfalls den Marktzutritt zu versagen. Eine Konformitätsverpflichtung mit Standards auf die Betreiber als Nutzer nachzuverlagern, träfe die falschen Adressaten. Die Netzbetreiber müssen sich darauf verlassen können, dass Netzwerkausrüstung, die am Markt erhältlich ist, die Standards erfüllt.

Zu den in **Absatz 3** genannten zusätzlichen Anforderungen:

In Ziffer 1 zu NOC/ SOC sollte das Wort „eigenen" gestrichen werden. Es muss Netzbetreibern in ihrer unternehmerischen Freiheit möglich sein, hier auf externe Anbieter zu setzen (erst Recht gilt dies für kleinere Betreiber, die ohne Outsourcing womöglich nicht arbeiten können). Außerdem muss es möglich sein, NOC und SOC hinsichtlich Auslagerung getrennt zu behandeln. Schließlich kann eine solche Trennung durchaus positiv unter Aspekten der Netzsicherheit gesehen werden, wenn allfällige Angriffspunkte getrennt loziert werden.

Ziffer 4: Multi-access Edge Computing (MEC): Solche Lösungen kommen nur für Großkunden in Frage. Gemeinsam mit dem Kunden wird das erforderliche Sicherheits-Level gemäß den festgestellten Risiken festgelegt. Zu beachten ist, dass mit MEC ausschließlich Lösungen gemeint sind, die 5G-SA erfordern und heute noch nicht realisierbar sind. Sie dürfen nicht mit Campus-Lösungen verwechselt werden. Ein Eingriff wird strikt abgelehnt, da bei solchen Lösungen immer ein hohes angepasstes Schutzniveau vorgesehen wird.

Zur Multi-Vendor-Strategie in Ziffer 7 haben wir uns bereits in der Stellungnahme vom 14. Februar 2020 erschöpfend geäußert. Wiederholend und unterstreichend sei gesagt, dass wir jedweden regulatorischen Eingriff in die Planung und Umsetzung der Architektur von Kommunikationsnetzen im Hinblick auf Lieferanten und Hersteller von Komponenten ablehnen. Dies wäre ein nicht zu rechtfertigender Eingriff in die unternehmerische Freiheit.

Außerdem würde eine Verpflichtung, ein Netz auf Basis mehrerer Hersteller aufzubauen dazu führen, dass die Netzbetreiber keinen ausreichenden Support im Falle von technischen Problemen erhielten, weil kein Lieferant oder Hersteller bereit oder in der Lage ist, im Zusammenspiel seiner Komponenten mit denen Dritter eine Gewähr für die Interoperabilität zu übernehmen. Gerade neue, in der Regel kleinere Mobilfunkanbieter am Markt sind daher auf Lösungen aus einer Hand angewiesen, die ihnen eine Sicherheit für das funktionierende Zusammenspiel aller Komponenten gibt und im Fall der Fälle in der Lage ist, Support über die Einsatzdauer sicherzustellen.

Eine Verpflichtung, Produkte eines zweiten Lieferanten in das Netz zu integrieren, könnte unter Umständen auch zum Einbau veralteter Technik führen, nämlich dann, wenn ein Betreiber den für seine Anwendungen besten Anbieter ausgewählt hat und nun ergänzend weniger leistungsfähige und womöglich weniger sichere Komponenten betreiben müsste.

Alles in allem lesen wir daher den Passus „die die technischen Beschränkungen und Interoperabilitätsanforderungen verschiedener Teile eines 5G-Netzes berücksichtigt" so, dass im Falle mangelnden Supports oder sonstiger netzadministrativer oder sicherheitsrelevanter Erschwernisse im Umkehrschluss die idealtypische Multi-Vendor-Strategie dispensiert erfüllt ist.

Wir schlagen weiters vor, dass dieser Strategie auch in der Form nachgegangen werden kann, dass sich ein Netzbetreiber über einen zweiten Anbieter informiert für den Fall, dass sein Standardlieferant ausfällt, er also stets über Informationen verfügt, an wen er sich dann wenden kann, um den Netzbetrieb sicherzustellen.

In diesem Sinne regen wir außerdem eine erläuternde Klarstellung an, dass auch eine gründliche Auseinandersetzung mit den am Markt erhältlichen Komponenten und Services vor einem konkreten Investitionsschritt die Kriterien einer Multi-Vendor-Strategie erfüllt.

Überdies sollte überlegt werden, ob (damit eventuell intendierte) Ausgrenzungen außereuropäischer Anbieter in einem globalen Wirtschaftssystem nicht eher Schaden anrichten als Nutzen zu stiften. Kurzfristig und konkret heißt das, dass Restriktionen im Hinblick auf Anbieter/ Hersteller zu Preiserhöhungen bei den übrigen, nicht betroffenen Anbietern zu Lasten der Netzbetreiber führen können.

Im Ergebnis darf das „Tool" Multi-Vendor-Strategie weder zum verpflichtenden Einsatz von zwei oder mehr Lieferanten/ Herstellern von Netzwerkkomponenten, noch zu einem Eingriff in die Lieferantenbeziehung oder sonst wie in die technische Umsetzung beim Netzbetreiber führen.

Zu den in **Absatz 4** geforderten Hardwarelisten sei angemerkt, dass nicht allein deren Erstellung sehr aufwändig und kostenintensiv ist, sondern außerdem mit deren Erhebung und Übermittlung Sicherheitsrisiken einhergehen, die die Kernfunktionen eines Netzbetreibers betreffen. Weiters wäre nach einer einmaligen Erhebung in Zukunft eine Meldung von Änderungen von Komponenten ausreichend und weniger belastend. Dabei sollte die Auflistung in Anhang 2 als beispielhaft benannt werden, da nicht alle Netzbetreiber über diese Komponenten verfügen. Außerdem sollten auch hier nur reine 5G-Komponenten erfasst sein.

III. Kosten

Schließlich ist das Thema der Kosten für die Maßnahmen nach der TK-NSiV 2020 wichtig. Ihr Vollzug liegt im öffentlichen Interesse. Daher sollten die Kosten des regulatorischen Vollzugs auch zur Gänze von der öffentlichen Hand getragen werden. Im RTR Budget 2021 sollte dies bereits berücksichtigt und der Beitrag des Bundesanteils entsprechend erhöht werden. Andernfalls würden die Betreiber für Kosten aufkommen, die durch den Vollzug von öffentlichen Interessen verursacht wurden.

Wir ersuchen um Berücksichtigung unserer Überlegungen und verbleiben

mit freundlichen Grüßen

Dr. Rosemarie Schön
Abteilungsleiterin