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

Wien, 05.06.2020

Per E-Mail: konsultationen@rtr.at

Betrifft: **Stellungnahme zum Entwurf der TK-NSiV 2020**

Sehr geehrte Damen und Herren,

Huawei Technologies Austria GmbH, als einer der führenden IT-Anbieter, hat den Entwurf der Telekom-Netzsicherheitsverordnung 2020 ("TK-NSiV 2020"), die weitere Anforderungen an eine sichere Telekommunikationsinfrastruktur festlegen soll, mit Interesse geprüft. Um einen raschen und nachhaltigen 5G-Ausbau zu ermöglichen gibt es aus unserer Praktikersicht den einen oder anderen Punkt anzumerken. Auch vor dem Hintergrund, die TK-NSiV 2020 Verordnung in der Praxis anwendbar zu gestalten, nehmen wir im Rahmen des laufenden Konsultationsverfahrens zum vorliegenden Entwurf wie folgt Stellung:

A. VORBEMERKUNG

Einleitend begrüßen wir den Ansatz der Rundfunk und Telekom Regulierungs-GmbH ("RTR"), die Maßnahmenvorschläge der Europäischen Kommission für einen sicheren Betrieb von 5G-Netzen aufzugreifen und auf Grundlage des Telekommunikationsgesetzes ("TKG") in einer Verordnung festzuhalten. Gerade der Ausbau des 5G-Netzes ist ein Meilenstein für die Sicherstellung des digitalen Fortschritts und der Wettbewerbsfähigkeit der Betreiber elektronischer Kommunikationsnetze und Anbieter elektronischer Kommunikationsdienste sowie der österreichischen Wirtschaft bzw der Gesellschaft als solches. Gerade jüngst hat die Corona Krise gezeigt, dass ein hoher Bedarf an mehr Bandbreite zur Ermöglichung höherer Datenvolumen besteht. Der mit den jüngsten, tragischen Entwicklungen einhergegangene Digitalisierungsschub sorgt auch für weitere Nachfrage und wird uns wohl auf Dauer erhalten bleiben.

Damit der Mobilfunkstandard 5G sein Potential auch in Industrie und Gewerbe voll entfalten kann, bedarf es neben der Infrastruktur auch eines entsprechenden Rechtsrahmens. Dieser sollte ausgewogen das Bedürfnis nach Netzsicherheit sowie organisatorischer und wirtschaftlicher Realisierbarkeit der neuen Anforderungen in einer bereits eng verwobenen Infrastruktur und einem bestehenden, langjährigen Vertriebsnetz berücksichtigen. Nur so wird es Netzwerkanbietern und ihren Zulieferern in diversen Branchen ermöglicht, die notwendigen Investitionen zu tätigen und die Netze dauerhaft sicher zu betreiben. Diesen Gedanken folgend kristallisieren sich im Entwurf der TK-NSiV 2020 einige zentrale, wirtschaftlich und wirtschaftspolitisch wesentliche Bestimmungen heraus, die über den Erfolg des Rechtsrahmens und der 5G-Initiative entscheiden. Wird in diesen Punkten eine zu einschränkende oder protektionistische Position eingenommen, wird der aus den dargelegten Gründen so wichtige 5G-Ausbau nachhaltig behindert. Dementsprechend beschränken wir uns in unserer Stellungnahme auf diese Kernbestimmungen:

B. ZUSAMMENFASSUNG

- **Betriebsort der NOC/SOC (§ 6 Abs 3 Z 1 TK-NSiV 2020)**: Die Forderung des zwingenden Betriebs von NOC und SOC in "*eigenen Räumlichkeiten*" des Betreibers berücksichtigt nicht ausreichend die damit einhergehenden, faktischen Probleme und Zwänge sowie die sich daraus etablierte Praxis. So wird gerade zur Sicherstellung ausreichender Expertise beim Betrieb, was wiederum die Netzsicherheit erhöht, für solche kritischen Dienste üblicherweise auf externe Experten zurückgegriffen. Den faktischen und Kostenzwängen folgend ist es gang und gäbe, einen Großteil dieser Dienste auf Dritte auszulagern. Eine Verpflichtung, NOC und SOC in eigenen Räumlichkeiten zu betreiben wäre faktisch kaum, keinesfalls zu wirtschaftlich vertretbaren Kosten zu erfüllen. Zudem findet die Anforderung keine Deckung im EU-Recht und ist damit auch überschießend. Weiters widerspricht die Umsetzung auch dem TKG, das im Gegensatz zum Verordnungsvorschlag eine rein rechtliche Funktionsherrschaft genügen lässt. Schließlich ist die Norm auch aus verfassungsrechtlichen Gründen kritisch.

  Im Ergebnis sollte die Entscheidung, ob und wie externe Dienstleister beim Betrieb von NOC und SOC einbezogen werden, daher ausschließlich beim Betreiber selbst liegen. Er muss sicherstelle, dass gewisse inhaltliche Kriterien erfüllt werden, aber den Betrieb nicht selbst oder in seinen eigenen Räumlichkeiten besorgen.

- **Zugangsbeschränkungen für Dritte (§ 6 Abs 3 Z 5 TK-NSiV 2020)**: Um ein einheitliches Verständnis adäquater technischer Risikomitigierungsmaßnahmen zu gewährleisten und ein Mitwachsen mit der sich ständig ändernden Technologie zu ermöglichen, sollte die Ausgestaltung der Zugangsbeschränkungen in der TK-NSiV 2020 an das Erfordernis der "*Angemessenheit*" und dem "*Stand der Technik*" gekoppelt werden. In der DSGVO wird ein vergleichbarer Ansatz gewählt.

- **Multi-Vendor-Strategie (§ 6 Abs 3 Z 7 TK-NSiV 2020)**: Der konkrete Inhalt der Verpflichtung zur *Multi-Vendor-Strategie* ist höchst unklar. Laut EB ist darunter die "*Auswahlmöglichkeit eines Betreibers unter zumindest zwei Lieferanten für Netzinfrastrukturelemente eines 5G-Netzes*" zu verstehen. Auch das eröffnet – bei einer so zentralen und weitreichenden Norm – unzulässiger Weise unterschiedliche Auslegungen:

  > (a) Verpflichtung der Betreiber zur Beauftragung mehrerer Lieferanten für Netzteile der eigenen 5G-Netze ("*multi vendor on operator level*");
  > (b) Vorschreiben des Einsatzes von Netzkomponenten unterschiedlicher Lieferanten für das landesweite 5G-Netz ("*multi vendor on country level*");
  > (c) Verbot des Bezugs technischen Equipments, das nur bei einem einzigen Lieferanten erhältlich ist.

  Eine Auslegung der Verpflichtung im Sinne der Variante (a) und (c) wäre im Lichte der Ziele der Verordnung kontraproduktiv, da es Sicherheitsdefizite schaffen und die konstante Qualität der Waren und Dienstleistungen beeinträchtigen würde. Es ist in der Praxis genau gegenläufig und sogar gegen gebilligten Aufpreis üblich, bei größeren IT Projekten nach Möglichkeit einen Anbieter bzw Generalunternehmer zu engagieren. Nur so werden Schnittstellenthemen, Probleme der fehlenden Interoperabilität und wechselseitigen Schuldzuweisungen bei– durch die Splittung auf mehrere Anbieter wahrscheinlicheren – Auftreten von Projektproblemen vermieden. Eine harte Multi-Vendorenverpflichtung auf Anbieterebene würde daher Sicherheitsrisken erzeugen, die bei der Vergabe in eine Hand gegebenenfalls nicht bestehen. Zudem würden die Verpflichtung, mehrere Anbieter auswählen zu müssen, das verfassungsrechtlich geschützte Eigentumsgrundrecht, insbesondere die daraus ableitbare Privatautonomie, das aus dem Gleichheitssatz resultierende Sachlichkeitsgebot und die Erwerbsausübungsfreiheit externer Dienstleister verletzen.

  Aus all diesen Gründen sollten die Betreiber elektronischer Kommunikationsnetze und Anbieter elektronischer Kommunikationsdienste daher lediglich zur Berücksichtigung der Multi-Vendor-Strategie beim Aufbau und Betrieb von 5G-Netzen verpflichtet werden. Die Entscheidungsgewalt über die Anzahl an Lieferanten sollte damit beim Betreiber selbst liegen. Das sollte sowohl in der TK-NSiV 2020 als auch in den EB festgehalten werden.

Im Detail:

C. ANFORDERUNGEN AN DEN BETRIEB VON NOC/SOC

1. RÄUMLICHKEITEN DER NOC/SOC

In **§ 6 Abs 3 Z 1 TK-NSiV 2020** ist derzeit vorgesehen, dass Network Operation Center ("NOC") und Security Operation Center ("SOC") vom Netzwerkbetreiber "*in eigenen Räumlichkeiten*" vorgehalten werden müssen. Nach den erläuternden Bemerkungen ("EB") müssen diese Leistungen daher in Räumen, die unter der Kontrolle des Betreibers des 5G-Netzes stehen, erbracht werden. Das würde zB selbst angemietee Rechenzentren, nicht aber Räume externer Dienstleister, umfassen. Die Bündelung der NOC/SOC beim Betreiber wird mit der Notwendigkeit des effektiven Monitorings und der Verhinderung von Anomalien und Bedrohungen (zB kompromittierte Endgeräte inkl IoT-Komponenten) begründet. Der gewählte Ansatz läuft freilich auf ein faktisches Verbot des Betriebs von NOC und SOC durch externe Dienstleister hinaus. Dies ist jedoch aus mehreren Gründen sachlich nicht begründet und geradezu kontraproduktiv, was die Aufrechterhaltung und Garantie eines größtmöglichen Sicherheitsniveau betrifft:

1.1. Qualitätsverluste und potentielle Sicherheitsdefizite

Damit NOC und SOC ihre Sicherheitsaufgaben effektiv erfüllen können, müssen sie rund um die Uhr aktiv betrieben werden. Die bloße Installation und passives Laufen lassen von Prozessen ist nicht ausreichend. Vielmehr bedarf es eines aktiven Managements und Überwachung.

Für den sinnvollen Betrieb von NOC und SOC bedarf es zudem eigens geschulter, höchst qualifizierter NOC-/SOC-Ingenieure und Techniker. Sie müssen umfassendes Know-How auf dem Gebiet der IT-Sicherheit und auch spezifische Kenntnisse über die Infrastruktur, Netzteilkomponenten sowie der dazugehörigen Software verfügen. Schließlich zählen zu ihren Hauptaufgaben das aktive Erkennen von Bedrohungsszenarien, das Troubleshooting sowie die Anpassungen und Optimierung des Netzwerkes und ihrer Komponenten. Diese Tätigkeiten erfordern auch ein ad-hoc Eingreifen in die Systeme und damit sehr tiefgehendes technisches Verständnis. Damit ist der Betrieb sowohl des NOC als auch des SOC extrem personalintensiv.

Neben den personellen Ressourcen bedarf es für den Betrieb eines NOC und SOC zudem auch einer entsprechenden, sehr kostenintensiven Infrastruktur (Hard- und Software, wie Verwaltungs- und Analysesoftware, Räumlichkeiten etc).

Insgesamt bedeutet die Verpflichtung, dass jeder Betreiber sein eigenes NOC und SOC betreiben muss, daher – wenn man die geforderten Sicherheitsstandards erfüllen möchte – signifikante finanzielle Investition und Belastung, die die Betreiber an die Grenzen ihrer finanziellen Möglichkeiten bringt. Um die Kosten zu senken droht, dass die Netzwerkbetreiber bei den Sicherheitsmaßnahmen oder der Infrastruktur Zugeständnisse machen. Das wäre aber gerade in Hinblick auf dem Telos der Verordnung kontraproduktiv.

Dazu kommt, dass die Betreiber von 5G-Netzen die (notwendigen) hohen Qualitätsanforderungen der Verordnung an NOC und SOC kaum, jedenfalls aber nicht kosteneffizient selbst abdecken können. So bedarf es für den Aufbau und den Betrieb von NOC und SOC – wie schon dargelegt – auch umfassender Kenntnisse über die einzelnen zugelieferten Netzteilkomponenten und ihre Interoperabilität und Wechselwirkungen zu anderen Komponenten und Systemen, die im geforderten Detailgrad für ein sicheres Monitoring meist nur wenige IT-Experten aufweisen. Am Ende des Tages ist das auch der Flaschenhals: Es gibt eine limitierte Anzahl an Personen mit entsprechend tiefem IT Verständnis, die dementsprechend auch hoch bezahlt sind. Es ist zu bezweifeln, dass beim bestehenden globalen Wettbewerb rund um die wenigen echten Experten ausreichende Ressourcen bestehen, sodass jeder 5G-Netzbetreiber genug qualifiziertes und wirtschaftlich leistbares Personal zum eigenen Betrieb von NOC und SOC vorfindet.

Daher lagern Betreiber den Großteil der NOC und SOC in der Praxis regelmäßig auf externe Dienstleister oder auf Dienstleister der Hauptfunktionen aus, die außerhalb der Räumlichkeiten des lokalen Betreibers operieren. Das entspricht auch dem generellen Trend und Status Quo in der IT: Unternehmen betreiben ihre kritischen Systeme nicht mehr selbst, da ihnen selbst die Ressourcen und das notwendige Know-How fehlt und auch am Markt zu wirtschaftlich vertretbaren Kosten nicht zugänglich ist. Für den Betrieb von NOC und SOC haben sich in der Praxis insbesondere folgende Formen der Auslagerung herauskristallisiert und bewährt:

- Virutelle (outsourced) NOC/SOC: Ein externer Dienstleister übernimmt sämtliche Dienste für den Betreiber einer Netzwerkinfrastruktur und greift aus eigenen Räumlichkeiten auf die Infrastruktur des Betreibers zu.
- Hybride NOC/SOC: Dabei handelt es sich um eine Mischung zwischen dem Betrieb mit eigenen Ressourcen und der virtuellen Variante. Einige Leistungen werden sohin vom Betreiber selbst erbracht und komplexere ausgelagert. Das ermöglicht insbesondere auch Klein- und Mittelbetrieben rund um die Uhr für Cybersecurity zu sorgen.
- Übergeordnete NOC/SOC: Eine Leitstelle überwacht, koordiniert und plant die Tätigkeiten der untergeordneten NOC und SOC. Dabei wird die Leitstelle regelmäßig inhouse betrieben und die konkret operative Tätigkeit (die untergeordneten NOC/SOC) an externe Experten vergeben. Dieses Modell findet insbesondere bei großen Konzernen Anwendung.

Die Notwendigkeit der Einbindung externer Experten bzw Auslagerung von Teilen der Services zeigt sich auch am aktuellen Marktangebot. So übernehmen zahlreiche IT-Dienstleister sowie auch die größten Telekommunikationsdienstleister in den ihren eigenen Räumlichkeiten regelmäßig für Dritte NOC- und SOC-Dienste. Dies regelmäßig von dem Gedanken getrieben, dass ein echter Spezialist in dem Bereich Zugang zu besseren Ressourcen und größeres Know-How hat und daher unter Berücksichtigung der Skalierungseffekte bessere Leistungen kostengünstiger am Markt anbieten kann. Der Selbstbetrieb von NOC und SOC Leistungen würde dagegen aufgrund der Markt- und der

wirtschaftlichen Begrenzungen zu einem tendenziell schlechteren Sicherheitsniveau führen.

Ein implizierter Ausschluss des Betriebs von NOC und SOC durch externe Dienstleister würde daher zu einem massiven Sicherheitsverlust bzw gar zur Unmöglichkeit des Betriebs von 5G-Netzen führen.

1.2. Wirtschaftliche Durchführbarkeit und Rentabilität

Weiters stellt – wie oben dargelegt – der Kostenfaktor beim Aufbau und Betrieb von NOC und SOC für viele Marktteilnehmer eine große Hürde dar. Wie bereits aufgezeigt, ist eine voll ausgestattete Infrastruktur sowie qualifiziertes Personal notwendig. Gerade letzteres ist im globalen Wettbewerb kaum zu bekommen. Da Cyberangriffe und Ausfälle rund um die Uhr drohen, müssen die IT-Experten auch in einem 24/7-Schichtbetrieb arbeiten. Das ist gerade im Hochkostenland Österreich ein erheblicher, zusätzlicher Kostenfaktor. Es ist zu erwarten, dass insbesondere Klein- und Mittelbetriebe die notwendigen finanziellen Ressourcen nicht bereitstellen können. Daher werden in der Praxis als Alternative regelmäßig auch aus Kostengründen externe Dienstleister eingesetzt. Wenn diese Möglichkeit gesetzlich genommen wird, wird das zwangsläufig zu einer – ungewünschten – Marktkonzentration zu Gunsten der finanzstarken Anbieter führen.

1.3. Widerspruch zu den EU-Zielen

Der nationale Regelungsvorschlag steht weiters auch im Widerspruch zu den Empfehlungen auf EU-Ebene:

Laut Europäischer Kommission sollen Mitgliedstaaten bei Festlegung der Maßnahmen zur Bewältigung der Sicherheitsrisiken die Cybersicherheit durch Anbietervielfalt fördern (ErwGr 25 der Empfehlung 2019/534 der Kommission vom 26.03.2019 zu "*Cybersicherheit der 5G-Netze*"). Durch den faktischen Ausschluss externer Dienstleister vom Betrieb der NOC und SOC wird dieses gemeinsame Ziel der Förderung der Wettbewerbsfähigkeit der Marktteilnehmer im österreichischen 5G-Sektor aber bewusst vereitelt – sowohl auf Anbieterseite von NOC und SOC Diensten, aber auch auf Telekommunikationsseite durch die Limitierung des Marktes auf die finanzkräftigen Anbieter.

Eine Rechtfertigung hierfür besteht auch für den konkreten 5G-Markt nicht: So enthält selbst der Katalog der NIS Cooperation Group über "*Cybersecurity of 5G networks, EU Toolbox of risk mitigating measures*" keine Empfehlung zum Betrieb der NOC und SOC "*in eigenen Räumlichkeiten*". Vielmehr wird darin lediglich vorgeschlagen, dass NOC und SOC innerhalb der EU betrieben werden sollen. Damit ist aber über die (Un)Zulässigkeit einer Auslagerung noch nichts gesagt.

Die vorgeschlagene Norm findet damit auch keine Deckung im EU-Recht und den Empfehlungen der EU-Organe und ist daher ein gold-plating, dass negative Konsequenzen

im Sinne der Beschränkung des Wettbewerbs auf mehreren Ebenen, aber auch die Qualität der Sicherheitsleistungen hat.

1.4. Verfassungsrechtliche Bedenken

Schließlich ist die Regelung auch aus verfassungsrechtlicher Sicht kritisch:

Nach dem aus dem Gleichheitssatz abgeleiteten Sachlichkeitsgebot (Art 7 B-VG; Art 2 StGG) muss eine Norm nämlich zur Zielerreichung geeignet sein. Das ist bei der vorgeschlagenen Regelung des § 6 Abs 3 Z 1 TK-NSiV 2020, wie bereits Pkt 1.1 bis 1.3 aufgezeigt, aber gerade nicht Fall. Die Bestimmung verhindert aus unserer Sicht daher die Erreichung des angestrebten Zwecks einer möglichst hohen Netzsicherheit. Damit ist die geforderte Mittel-Zweck-Relation nicht gegeben und liegt eine Verletzung des Sachlichkeitsgebotes vor.

Weiters greift § 6 Abs 3 Z 1 TK-NSiV 2020 auch rechtswidrig in das Grundrecht auf Erwerbsausübungsfreiheit nach Art 6 StGG ein. So werden Netzbetreiber wie auch externe Dienstleister, die die Sicherheitsleistungen professioneller und wirtschaftlich ökonomischer anbieten könnten, in unnötiger und damit unverhältnismäßiger Weise in ihrer Erwerbstätigkeit beschränkt.

Letztlich ist die Beschränkung auf "*in eigenen Räumlichkeiten*" auch unklar und verstößt daher gegen das Legalitätsprinzip gemäß Art 18 B-VG. Demnach müssen Normen ausreichend determiniert sein. Je eingriffsintensiver eine Norm, desto höher muss auch ihr Bestimmtheitsgrad sein. Durch den *de facto* Marktausschluss externer Anbieter ist die Eingriffsintensivität unbestritten gegeben. Dennoch bleibt der Verordnungsgeber vage, wenn er vom Betrieb "*in eigenen Räumlichkeiten*" spricht. Diese Beschreibung lässt schließlich auch Raum für Interpretation. Rechtsanwender könnten die Norm auch so auslegen, dass externe Dienstleister lediglich von der Verfügungsgewalt über die Räumlichkeiten ausgeschlossen sind, nicht aber vom Betrieb selbst. Erst aus den EB erschließt sich aber erst die verfassungswidrige Absicht des Verordnungsgebers.

Zudem ist die von der RTR vorgeschlagene Vorgangsweise unwirtschaftlich und widerspricht der oben angeführten Empfehlung der EU-Kommission. Diese ist zwar für den nationalen Gesetz- und Verordnungsgeber nicht zwingend, aber für ein konsistentes europaweites Rechtsverständnis, wie dies auch in den EB selbst betont wird, dennoch ratsam. Langfristig wird schließlich ein europaweiter und künftig auch ein transeuropäischer Netzausbau angepeilt.

1.5. Widerspruch zum TKG

Für die Qualifikation als Dienste- und Netzbetreiber iSv § 3 Z 3 und Z 4 TKG ist der Begriff der (rechtlichen) Funktionsherrschaft ein zentrales Tatbestandsmerkmal:

Für Bereitsteller von Kommunikationsdiensten reicht es nach dem klaren Gesetzeswortlaut jedenfalls aus, wenn die rechtliche Kontrolle über die notwendigen Funktionen des

angebotenen Produktes ausgeübt werden können. Eigentum ist nach herrschender Lehre und Rechtsprechung jedenfalls nicht erforderlich (VwGH 2002/03/0320). Die rechtliche Funktionsherrschaft kann auf vertraglicher Grundlage mit dem Eigentümer technischer Infrastrukturen oder Erbringer von Vorleistungsdiensten beruhen. Auf die faktisch-technische oder wirtschaftliche Kontrolle wird dabei aber nicht abgestellt.

Art 16a TKG ermächtigt die RTR mit Verordnung nähere Bestimmungen zur Umsetzung der §§ 16 und 16a TKG festzulegen. Ein Eingriff in zentrale Tatbestandsmerkmale der gesetzlich normierten Betreiberbegriffe ist davon jedenfalls nicht erfasst. Damit steht § 6 Abs 3 Z 1 TK-NSiV 2020 auch im Widerspruch zum TKG und geht über die Verordnungsermächtigung der RTR zum Erlass von ausführenden Bestimmungen hinaus.

1.6. Fazit

Aus all diesen Gründen sollte die Entscheidung, ob und wie externe Dienstleister beim Betrieb von NOC und SOC einbezogen werden, ausschließlich beim Betreiber selbst liegen. Eine starre Regelung ist nicht nur aus verfassungsrechtlicher Sicht kritisch, sondern auch aus Sicherheitsgründen kontraproduktiv. Es wird daher angeregt, § 6 Abs 3 Z 1 TK-NSiV 2020 wie folgt anzupassen:

> "*Betrieb von Network Operation Center (NOC) sowie Security Operation Center (SOC) ~~in eigenen Räumlichkeiten~~ innerhalb der Europäischen Union;*"

Die Beschreibung der "*eigenen Räumlichkeiten*" in den EB ist entsprechend zu löschen.

2. ZUGANGSBESCHRÄNKUNGEN FÜR DRITTE

§ 6 Abs 3 Z 5 TK-NSiV 2020 bestimmt allgemein, dass Zugänge durch Dritte beschränkt und überwacht werden müssen. Diese Regelung ist zu begrüßen und ergibt sich bereits aus zahlreichen relevanten Cybersicherheitsmaterien, wie zB aus Art 32 DSGVO und der gelebten IT-Sicherheitspraxis. Um ein einheitliches Verständnis adäquater technischer Risikomitigierungsmaßnahmen zu gewährleisten, sollte die Ausgestaltung der Zugangsbeschränkungen an das Erfordernis der "*Angemessenheit*" und dem "*Stand der Technik*" gekoppelt werden (vgl auch gesetzliche Diktion in Art 32 Abs 1 DSGVO bzw § 17 Abs 1 NISG).

Demnach regen wir an, die Bestimmung wie folgt anzupassen, *in eventu* zumindest in den EB sinngemäß zu berücksichtigen:

> "*Einschränkung des Zugriffs auf befähigtes und qualifiziertes Personal, das einer Sicherheitsüberprüfung unterzogen wurde; ein Zugang durch Dritte ist entsprechend dem Stand der Technik im angemessenen Umfang zu beschränken und zu überwachen;*"

D. MULTI-VENDOR-STRATEGIE

1. AUSWAHL VON MINDENSTENS ZWEI LIEFERANTEN

§ 6 Abs 3 Z 7 TK-NSiV 2020 bestimmt, dass Betreiber von 5G-Netzen die Einhaltung der Multi-Vendor-Strategie nachweisen müssen. Laut EB ist unter der "*Multi-Vendor-Strategie*" die "*Auswahlmöglichkeit eines Betreibers unter zumindest zwei Lieferanten für Netzinfrastrukturelemente eines 5G-Netzes*" zu verstehen. Dadurch sollen Abhängigkeiten von einem einzigen Lieferanten bzw Abhängigkeiten von Lieferanten mit hohen Risikoprofil vermieden oder beschränkt werden.

Der konkrete Inhalt der Verpflichtung zur Multi-Vendor-Strategie ist höchst unklar. Zudem würde eine Auslegung im Sinne der EB zur Verfassungswidrigkeit der Norm führen:

1.1. Unklarer Inhalt

§ 6 Abs 3 Z 7 TK-NSiV 2020 schreibt Betreibern von 5G-Netzten eine "*Multi-Vendor-Strategie*" vor, definiert diese jedoch nicht. Auch im TKG bzw in der gesamten österreichischen Rechtsordnung fehlt ein entsprechendes Begriffsverständnis. So ergibt auch eine Suche im Rechtsinformationssystem des Bundeskanzleramts (www.ris.bka.gv.at) nach "*Multi-Vendor-Strategie*" in den unterschiedlichen Schreibvarianten keinen einzigen Treffer. Dieser Begriff ist dem österreichischen Recht sohin schlichtweg fremd. Auch aus dem allgemeinen Sprachgebrauch – selbst unter Berücksichtigung der Branchenkenntnisse und –entwicklungen – lässt sich der konkrete Inhalt des Begriffs und der daran gekoppelten Verpflichtung nicht klar entnehmen. Wie folgende zwei Auslegungsmöglichkeiten zeigen, ist der Begriff zu unbestimmt und sind die daraus resultierenden Rechte und Pflichten für den Rechtsanwender unvorhersehbar:

a) So lässt sich daraus ableiten, dass Betreiber zur Beauftragung mehrerer Lieferanten bei Ausstattung der eigenen 5G-Netze verpflichtet werden sollen ("*multi vendor on operator level*").
b) Die "*Multi-Vendor-Strategie*" kann jedoch auch als allgemeine österreichische Zielsetzung verstanden werden, dass das landesweite 5G-Netz aus Netzteilen mehrerer Lieferanten bestehen soll ("*multi vendor on country level*").
c) Die Regelung kann schließlich auch als Verbot des Bezugs technischen Equipments, das nur bei einem einzigen Lieferanten erhältlich ist, verstanden werden.

Es herrscht daher offensichtlich Unklarheit über den Inhalt des Begriffs der "*Multi-Vendor Strategie*". Dabei kommt dem zentrale Bedeutung zu. Eine so wichtige Bestimmung muss der Verordnungsgeber aber selbst erklären und kann den Erklärungsinhalt nicht bloß am Rande in den EB anstreifen.

Unabhängig davon konterkarieren folgende Auslegungsvarianten das Ziel einer hohen Netzsicherheit und verleiten im Ergebnis auch zu einer verfassungswidrigen Anwendung:

1.2. Verpflichtung zum Einsatz mehrerer Lieferanten im 5G-Netz des Betreibers

1.2.1. Qualitätsverluste und potentielle Sicherheitsdefizite

Die implizierte Verpflichtung des Einsatzes mehrerer Lieferanten im 5G-Netz des Betreibers ("*multi vendor on operator level*") ist dazu geeignet, Sicherheitsdefizite zu schaffen und eine konstante Qualität der Waren und Dienstleistungen zu beeinträchtigen. Wie allgemein die Erfahrungen aus IT-Projekten zeigen, liegt die wahre Kunst darin, einzeln für sich funktionierende Elemente zu einem großen Ganzen zusammen zu führen. Tatsächlich ist die Marktbestrebung, nach Möglichkeit nur mit einem Anbieter oder zumindest – unter Akzeptanz eines Entgeltaufschlages – mit einem Generalunternehmer zu kontrahieren, der seinerseits das Koordinations- und Schnittstellenthema als sein Risiko übernimmt. Dem steht der Verordnungsansatz gegenüber, der nun den Betreiber von hoch technischen Telekommunikationsnetzen dazu zwingen möchte, bewusst einen "*Fleckerlteppich*" zu beauftragen. Statt nur einem Anbieter sollen mehrere Komponenten angeschafft werden. Damit werden aber unnötige Gefahren und Risiken begründet:

Dem angestrebten Ziel der größeren Unabhängigkeit von den Anbietern steht der hohe Preis der Schaffung von Problemen der Kompatibilität und Interoperabilität der Systeme und Netzteile gegenüber. Neben dem faktischen Thema schließen diverse Anbieter in ihren Geschäftsbedingungen regelmäßig jegliche Gewährleistung für Probleme aus den Bereichen anderer Anbieter bzw von selbst geschaffenen Schnittstellen aus. In der Praxis führt eine solche Zersplitterung der Anbieter im Problemfall regelmäßig zu einem "*Fingerpointing*" und im Kreis schicken des Auftraggebers zwischen den unterschiedlichen Anbietern. Im Zweifel war jedenfalls der andere, aber nicht der konkret angesprochene Auftragnehmer Schuld. Durch die erhöhte Projektkomplexität durch mehrere Anbieter steigt aber auch die faktische Eintrittswahrscheinlichkeit von Problemen. Damit wird das Thema noch intensiviert.

Selbst wenn die Projektphase überstanden ist, bestehen auch im laufenden Betrieb Nachteile: So wird auch das Netzwerk- und Incidentmanagement komplexer. Kommt es zu einem Incident ist es schwieriger möglich, ihn zu lokalisieren und dann vor allem auch zu beheben. Die Anforderungen an die IT-Experten, der nun Detailwissen für unterschiedliche Anbieter braucht, steigt dadurch noch weiter. Gerade im Zusammenspiel mit der oben kritisch erörterten Verpflichtung des Betriebs des NOC und SOC in den Räumlichkeiten des Netzwerkbetreibers kommt es damit zu einer weiteren Verschärfung der Situation. Weiters bestehen kaum Möglichkeiten, zu einem einheitlichen, herstellerübergreifenden Monitoring. Damit wird aber auch die Zielrichtung der Verordnung für ein entsprechendes Sicherheitsniveau im Betrieb zu sorgen, untergraben. So ist ja gerade die laufende Analyse des Netzwerks zur Verhinderung von Cyberangriffen, Ausfällen und Sicherheitsfehlern- zu Recht – eines der Hauptanliegen der Verordnung.

Dementsprechend werden in der Praxis – dem Ansatz der Verordnung entgegenlaufend - üblicherweise möglichst viele Leistungen aus einer Hand bezogen. Damit kann auch der Betreiber die Einhaltung der gesetzlich vorgeschriebenen Sicherheitsanforderungen sowie

die Verfügbarkeit der notwendigen Funktionen und Leistungen bestmöglich sicherstellen. Der gegenteilige Ansatz der Verordnung verkennt die praktischen, tatsächlichen Probleme bei IT-Projekten und untergräbt durch seine starre Verpflichtung die Sicherstellung der geforderten IT-Sicherheitsqualität. Richtigerweise muss es dem Betreiber überlassen sein, in Kenntnis des Marktumfeldes unter Berücksichtigung sämtlicher Faktoren, die für einen oder mehrere Zulieferer im konkreten Fall sprechen, eine ausgewogene Entscheidung zu treffen.

1.2.2. Haftungsfragen bei mehreren Lieferanten

Beim Einsatz mehrerer Lieferanten im 5G-Netz des Betreibers stellt sich rechtlich zudem das Problem, dass eine vertragliche Haftung oder Gewährleistung für die Kompatibilität und Interoperabilität der unterschiedlichen Netzteilkomponenten erfahrungsgemäß nicht übernommen wird. Das erschwert im – durch den Einsatz mehrerer Anbieter wahrscheinlicheren Konfliktfall – die Durchsetzung rechtlicher Ansprüche und schließlich die ordnungsgemäße Implementierung und Betrieb eines sensiblen 5G-Netzes. Auch aus diesem Grund greifen in der Praxis daher Betreiber vermehrt zu einem einzigen Lieferanten, der für die gesamte IT-Infrastruktur verantwortlich ist. Allein dadurch kann auch aus rechtlicher Sicht ein hoher Sicherheitsstandard verlässlich gewährleistet werden.

1.2.3. Wirtschaftliche Aspekte

Der Einsatz mehrerer Dienstleister im eigenen 5G-Netz stellt für viele Betreiber auch einen zusätzlichen Kostenfaktor dar, der insbesondere Klein- und Mittelbetriebe übermäßig belastet. Eine zwangsweise Umsetzung einer Multi-Vendor-Strategie führt neben den aufgezeigten Risiken der Kompatibilität der unterschiedlichen Netzelemente auch zu einem potentiellen Ausschluss neuer Marktteilnehmer, sowohl Betreiber von 5G-Netzen als auch IT-Dienstleister und Lieferanten, in dem wachsenden und zunehmend bedeutsameren 5G-Sektor. Das widerspricht klar dem festgelegten Ziel der Kommission, die Anbietervielfalt zu fördern (ErwGr 25 der Empfehlung 2019/534 der Kommission vom 26. März 2019 zu "*Cybersicherheit der 5G-Netze*").

Damit eine Interoperabilität vollständig hergestellt werden kann, müssten die unterschiedlichen Anbieter sich wechselseitig diverse technische Parameter bis hin zu Zugang zu (Steuerungs)Software offen legen. Das kann jedoch zu einem Abfluss von Betriebs- und Geschäftsgeheimnisse des jeweiligen Anbieters führen. Es ist das eine, ob ein Anbieter freiwillig am Markt Teilkomponenten anbietet und daher zwangsläufig gewisse Spezifikationen offenlegen muss, oder ob man ihn durch eine Verordnung zu einer Zusammenarbeit zwingt – da er den Auftrag alleine nicht bekommen kann. Mit einer solchen Verpflichtung würde in das Eigentumsrecht und in die Erwerbsfreiheit der betroffenen Anbieter eingegriffen. Auf der anderen Seite müsste aber auch der Betreiber seine Systemkonfiguration mehreren potentiellen Anbietern statt nur einem gegenüber offenlegen, was wiederum ein erhöhtes Risikopotential in sich birgt. Der konkrete Aufbau komplexer Systeme und Netzwerke wird in der Praxis aber bewusst geheim gehalten, weil sonst Dritten ein Angriff leichter möglich wird. Bei Kenntnis der Komponenten und Planung

kann ein Zugriff auf das System besser geplant und umgesetzt werden. Dementsprechend werden System- und Netzwerkarchitekturen in kritischen (Infrastruktur)Bereichen als Geschäftsgeheimnis gehütet. Muss der Betreiber nun zwangsweise zumindest zwei Anbieter nutzen, wird das Risiko, dass seine gehütete Systemarchitektur publik wird, bereits verdoppelt.

Weiters kann das laut EB verfolgte Ziel der Vermeidung von Abhängigkeiten selbst durch ein verpflichtendes, weites Zuliefernetz nicht erreicht werden. Wie die aktuelle Covid-19-Krise zeigt, sind beinahe alle Lieferanten selbst von dritten Zulieferern abhängig. Das trifft umso mehr auf technologieaffine Waren in einem so engen Geschäftsfeld, wie Hard- und Software für 5G-Netze, zu. Die Multi-Vendoren-Verpflichtung begründet also nicht nur massive sicherheitstechnische Risiken, sondern ist darüber hinaus auch nicht geeignet, um das beschriebene wirtschaftliche Interesse zu erreichen.

1.2.4. Überschießende Implementierung der Empfehlungen auf EU-Ebene

Die Guideline der NIS Cooperation Group über "*Cybersecurity of 5G networks, EU Toolbox of risk mitigating measures*" enthält lediglich den Vorschlag, die Anbietervielfalt durch eine angemessene Multi-Vendor-Strategie zu berücksichtigen (vgl Maßnahme "*SM03*" im Anhang ./1 der Guideline). Damit ist aber noch keine Aussage über eine Verpflichtung zum Einsatz mehrerer Lieferanten getroffen. Wie die NIS Cooperation Group in ihrem Risikomitigierungsplan (vgl "*Risk 4*" im Anhang ./1 der Guideline) selbst einräumt, hängt die Effektivität der Maßnahme von ihrer konkreten Ausgestaltung ab. Zudem sind bei der Umsetzung der Überlegungen ins nationale Recht stets folgende Faktoren zu berücksichtigen: (i) damit einhergehende Ressourcen bzw Kosten, (ii) sektor-spezifische wirtschaftliche Auswirkungen (insbesondere auf Betreiber und ihre Dienstleister) und (iii) etwaige weitere wirtschaftliche und soziale Konsequenzen.

Diese Überlegungen wurden im aktuellen Regelungsvorschlag nicht ausreichend berücksichtigt. Wie bereits ausgeführt, ist eine harte Verpflichtung zur Multi-Vendor-Strategie, wie dies der aktuelle Wortlaut des § 6 Abs 3 Z 7 TK-NSiV 2020 impliziert, keine geeignete oder angemessene Maßnahme zur Stärkung der Netzsicherheit bzw Unabhängigkeit der Betreiber. Im Gegenteil, werden damit Klein- und Mittelbetriebe ohne Möglichkeit zur Zielerreichung übermäßig belastet und der Markt auf Betreiberseite abgeschottet. Die weiter drohenden Konsequenzen sind nicht erläutert und abgewogen. Die starre Verpflichtung wird daher dem Telos der Guideline nicht genüge.

1.2.5. Eingriff in verfassungsrechtlich gewährleistete Rechte

Schließlich greift die starre Bestimmung durch die in den EB nahegelegte Umsetzung massiv in verfassungsgesetzlich gewährleistete Rechte ein:

Einerseits wird dadurch die Vertragsabschlussfreiheit des Betreibers, aber auch externer Dienstleister und IKT-Lieferanten beschränkt und damit in die Privatautonomie eingegriffen. Das begründet einen Eingriff in das Eigentumsgrundrecht des Art 5 StGG, der

sich aufgrund der Auslegungsmöglichkeiten der nicht definierten Multi Vendor-Strategie intensiviert. Damit wird den Rechtsunterworfenen zusätzlich zur massiven Beschränkung ihrer Grundrechte noch eine wesentliche Unsicherheit aufgebürdet.

Weiters ist die Regelung unsachlich. Wie bereits in Pkt 1.2.1 ff näher ausgeführt, ist die suggerierte Vorgehensweise nicht zur Zielerreichung geeignet. Neben Qualitätsverlusten, potentiellen Sicherheitsdefiziten und der aufgezeigten komplexen Haftungsthemen ist die Maßnahme überdies wirtschaftlich für viele, insbesondere neue Marktteilnehmern übermäßig belastend. Zudem ist die Regelung nicht zielführend, weil selbst die Lieferanten wiederum von dritten Zulieferern abhängig sind und damit durch eine Multi Vendor-Strategie die Versorgungssicherheit und Unabhängigkeit der Betreiber von 5G-Netzen nur scheinbar steigert. Auch aus EU-rechtlicher Sicht ist die in der Verordnung implementierte Multi-Vendor-Strategie überschießend und unverhältnismäßig.

Aus all diesen Gründen verletzt § 6 Abs 3 Z 7 TK-NSiV 2020 (i) das Eigentumsgrundrecht, insbesondere die daraus ableitbare Privatautonomie, (ii) das aus dem Gleichheitssatz resultierende Sachlichkeitsgebot und (iii) beschneidet die Erwerbsausübungsfreiheit der externen Dienstleister in unverhältnismäßiger Weise.

1.3. Auswahl von Netzkomponenten, die mehrere Lieferanten anbieten

Die obigen Ausführungen zur ersten Auslegungsvariante gelten auch sinngemäß für das Verständnis einer Verpflichtung zur Auswahl technischer Komponenten, die mehrere Lieferanten anbieten:

Eine derartige Anwendung der Multi Vendor-Strategie würde ebenso zu einem massiven Qualitäts- und Sicherheitsverlust führen: So wären Betreiber von 5G-Netzen unter Umständen gezwungen, auf bereits veraltete Technologien zurückzugreifen. Neue, innovative Lösungen eines Vorreiters, die gerade den Sicherheitsstandard in einem zunehmend wachsenden Sektor treiben und zur Gewährleistung eines über den sonstigen Branchen stehenden Niveaus sorgen, müssten bewusst ausgeschlossen werden.

Weiters würde eine derartige Praxis (i) das Eigentumsgrundrecht, insbesondere die daraus ableitbare Privatautonomie, (ii) das aus dem Gleichheitssatz resultierende Sachlichkeitsgebot und (iii) die Erwerbsausübungsfreiheit externer Dienstleister, die als erstes neue Produkte auf den Markt bringen, verletzen.

1.4. Fazit

Die Betreiber elektronischer Kommunikationsnetze und Anbieter elektronischer Kommunikationsdienste sollten daher lediglich zur Berücksichtigung der Vor- und Nachteile einer Multi-Vendor-Strategie beim Aufbau und Betrieb von Netzen verpflichtet werden. Die Entscheidungsgewalt über die Anzahl an Lieferanten sollte schlussendlich beim Betreiber selbst liegen, der für die Einhaltung der Sicherheitsvorgaben auch verantwortlich ist. Bei einer reinen Ermessensentscheidung des Betreibers bedarf es sodann auch keiner

Definition der "*Multi Vendor-Strategie*". Demnach schlagen wir vor, § 6 Abs 3 Z 7 TK-NSiV 2020 wie folgt anzupassen:

> "*nach Möglichkeit Berücksichtigung einer Multi-Vendor-Strategie beim Aufbau und Betrieb von Netzwerken, die die technischen Beschränkungen und Interoperabilitätsanforderungen verschiedener Teile eines Netzes dabei einbeziehen~~berücksichtigt~~.*"

* * * * *

Wir ersuchen um entsprechende Berücksichtigung dieser Stellungnahme.

Beste Grüße,

Huawei Technologies Austria GmbH