T-MOBILE AUSTRIA GMBH
A-1030 Wien, Rennweg 97-99

Rundfunk und Telekom Regulierungs – GmbH (RTR-GmbH)

Mariahilferstrasse 77-79

1060 Wien

per E-Mail: konsultationen@rtr.at

Wien, 05.06.2020

Stellungnahme zur Telekom-Netzsicherheitsverordnung 2020

Sehr geehrte Damen und Herren,

die T-Mobile Austria GmbH (Magenta) nimmt mit diesem Schreiben im Rahmen der öffentlichen Konsultation zum Entwurf einer Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR) 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), Stellung.

Sicherheit in all seinen Dimensionen ist Magenta ein essentielles Anliegen und Teil der Unternehmensphilosophie. Gerade die derzeit herrschende Covid-19 Pandemie und deren Auswirkungen demonstrieren eindrucksvoll, wie essentiell stabile und sichere Kommunikationsnetze für das Funktionieren von Gesellschaft und Wirtschaft sind. Magenta ist sich dieser Verantwortung als Betreiberin einer kritischen Infrastruktur bewusst und arbeitet jeden Tag daran, das hohe Sicherheitsniveau unserer Netze und innerhalb unseres Unternehmens aufrecht zu erhalten und zu verbessern. Technologischer Fortschritt und Sicherheit müssen Hand in Hand gehen, um zum Wohle der Gesellschaft und Wirtschaft beizutragen. Daher begrüßen wir den vorgelegten Entwurf der TK-NSiV, der erstmals verbindliche Sicherheitsstandards für 5G einführt und die Meldepflichten präzisiert. Es finden sich darin gute Ansätze und Vorschriften, um bei der Markteinführung und -etablierung von 5G ein hohes Sicherheitsniveau zu gewährleisten. Um die Rechtsicherheit der normunterworfenen Unternehmen zu erhöhen und eine sinnvolle Kosten-Nutzen Relation zu wahren, sind aus Sicht von Magenta jedoch noch substantielle Änderungen notwendig. Im folgenden Abschnitt findet sich der detaillierte Input von Magenta, gegliedert nach den jeweiligen Paragraphen der VO:

Ad § 2 Begriffsbestimmungen:

- Im Entwurf fehlt eine Definition des Begriffs „Dienstekategorie", insbesondere welche Dienstekategorien von der Verordnung geregelt werden sollen. Aus § 3 Abs 1 Z 5 ergibt sich indirekt, dass es zumindest vier Dienstekategorien geben muss. Um die Verständlichkeit der TK-NSiV zu erhöhen, sollte in den Begriffsbestimmungen der in der VO häufig genutzte Ausdruck „Dienstekategorie" aufgenommen werden. Für die Normunterworfenen sollte sich aus der VO eindeutig ablesen können, wie viele Dienstekategorien es gibt und wie diese definiert sind.

  Magenta regt an eine entsprechende Definition aufzunehmen.
- In § 2 Z 7 wird der zentrale Begriff des Sicherheitsvorfalls definiert, der wiederum auf die Sicherheit von Kommunikationsnetzen oder –diensten referenziert. In der Definition des letztgenannten Begriffs wird u.a. darauf abgestellt, ob die „*Integrität oder Vertraulichkeit dieser Netze und Dienste, der gespeicherten, übermittelten oder verarbeiteten Daten*" beeinträchtigt wird. In einer weiten Auslegung dieser Definition könnten auch sogenannte Datenleaks d.h. die nicht autorisierte, wie auch immer geartete, Veröffentlichung von personenbezogenen Daten als Sicherheitsvorfall betrachtet werden. 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. Der Mehrwert einer solchen, für die Betreiber mit höherem Aufwand verbundenen, doppelten Meldepflicht lässt nicht erblicken. Vielmehr sollten Datenleaks ausschließlich der DSGVO unterliegen und im Zuständigkeitsbereich der Datenschutzbehörde verbleiben.

  Magenta regt an die Definition des Sicherheitsvorfalls dahingehend zu ändern und/oder in den EB klarzustellen, dass Datenleaks nicht Gegenstand der TK-NSiV sind.
- Die Definition von „unverzüglich" und die EB dazu geben keine Auskunft darüber, innerhalb welchen Zeitraums eine Meldung zu erfolgen hat. Es wäre wünschenswert einen konkreten zeitlichen Rahmen vorzugeben (z.B.: innerhalb von 24 Stunden) der dem meldepflichtigen Unternehmen Rechtssicherheit geben würde. Aktuell existiert aufgrund eines solchen fehlenden zeitlichen Rahmens ein Graubereich und die für die Einmeldung zuständigen Personen müssen selbst entscheiden bis wann eine Meldung zu erfolgen hat.

  Magenta regt an hier klarere zeitliche Vorgaben zu machen, die auch in der Praxis erfüllbar sind.

Ad § 3 Informationspflichten

- In § 3 werden Informationspflichten für Betreiber von elektronischen Kommunikationsnetzen und –diensten normiert für den Fall, dass Sicherheitsvorfälle mit beträchtlichen Auswirkungen auf die Sicherheit auftreten. Eine solche Meldepflicht sollte jedoch nicht nur für die Betreiber von elektronischen Kommunikationsnetzen und – diensten zutreffen, sondern auch sogenannte Over-the-Top Diensteanbieter (OTT), wie Messenger und Chat Apps (z.B.: Whatsapp, Apple Messenger, Face Time, Instagram, Facebook Messages, etc.). Diese OTT Dienste stehen in zunehmender Konkurrenz zu klassischen TK Diensten und

sollten daher den gleichen Regeln unterliegen wie TK Betreiber. In der regulatorischen Praxis unterliegen letztere einer strikteren Regulierung als OTT Dienste, was zu einer unsachlichen Ungleichbehandlung führt. Die TK-NSiV sollte versuchen ein Level Playing Field zu schaffen und der zunehmenden Bedeutung von OTT Diensten, die in Konkurrenz zu TK Diensten stehen, Rechnung tragen.

Magenta regt an auch OTT Dienste im Rahmen der TK-NSiV zu adressieren.

- Die Informationspflichten sollten auf jene Netze eingeschränkt werden, die öffentlich sind und deren Dienste der Allgemeinheit angeboten werden. In Abgrenzung dazu kann es zukünftig Individuallösungen für große Unternehmen oder Institutionen geben, die ein komplexes internes Netzwerk nachfragen, welches ausschließlich von einer bestimmten Personengruppe für interne Zwecke genutzt wird (z.B.: Campus Netzwerk). Ein solches Netzwerk dient nicht zur Versorgung einer breiten Öffentlichkeit mit Kommunikationsdiensten. Ein Campus Netzwerk ist ein Businessprodukt, das jedoch nicht öffentlich angeboten wird und dessen Ausfall nur einen Teilnehmer treffen würde. Es besteht daher keine Notwendigkeit den Ausfall eines solchen Netzwerks der Informationspflicht des § 3 zu unterwerfen, unabhängig von der Anzahl der darin vernetzten Nutzer.

  Magenta regt an in § 3 auf *öffentliche* elektronischen Kommunikationsnetzen oder –dienste abzustellen.

- Der Standard Prozess zur Einmeldung eines Sicherheitsvorfalls sieht die Verwendung des eRTR-Portals vor. Als Alternative dazu ist für den Fall des Ausfalls des eRTR-Portals die Einmeldung per E-Mail vorgesehen. Aus Praktikabilitätsgründen sollte diese Variante auch möglich sein, wenn die Verwendung des eRTR-Portals auf Seiten des Betreibers vorübergehend nicht möglich ist z.B.: wenn in dringenden Fällen kein Mitarbeiter mit eRTR-Portal Zugang verfügbar ist.

  Magenta regt an auch eine Einmeldung via E-Mail als Alternative zur Einmeldung über das eRTR-Portal einzuführen.

- Z 5 definiert die Anzahl der in der jeweiligen Dienstekategorie betroffenen Teilnehmer für verschiedene Dienste. In diesem Zusammenhang sollte klargestellt werden,
  - wie Hybrid-Produkte zu klassifizieren sind. Magenta vertritt dabei die Ansicht, dass es sich bei einem Hybrid-Produkt um einen festen Internetzugang handelt, der auch dieser Dienstekategorie zuzuordnen ist. BEREC vertritt ebenfalls diese Ansicht und empfiehlt den nationalen Regulierungsbehörden Hybrid-Produkte den Regeln für feste Internetzugangsprodukte zu unterwerfen (Rz 141b Draft BEREC Guidelines on the Implementation of the Open Internet Regulation).

    Magenta regt an in den EB die richtige Einordnung von Hybrid Diensten festzuhalten.
  - dass M2M Dienste nicht in eine der im Entwurf genannten Dienstekategorien fallen. M2M Dienste werden u.a. in beweglichen Gegenständen genutzt, die in der gesamten Welt vertrieben werden und nicht auf einen nationalen Gebrauch eingeschränkt sind. Ein gutes Beispiel dafür sind M2M Automobil Anwendungen. Diese Dienste werden in Fahrzeugen großer Automobilhersteller genutzt, welche weltweit vertrieben werden. Ein Ausfall eines solchen Dienstes hat daher auch nur

überschaubare nationale Auswirkungen und sollte daher nicht unter die Informationspflicht des § 3 fallen.

Magenta regt daher an, M2M Dienste von der Informationspflicht auszunehmen.

- Die Schwellwerte des Abs 2 lassen sich nicht eindeutig erfassen, da die Formulierung der einzelnen Tatbestände uneinheitlich und unklar formuliert ist. Während Z 1 und Z 7 nur auf die Anzahl der betroffenen Teilnehmer der jeweiligen Dienstekategorie abstellt, wird in Z 2 bis 6 auch auf die Gesamtzahl der Nutzer des Dienstes im Bundesgebiet referenziert. Diese Zahlen sind naturgemäß nur der Regulierungsbehörde bekannt und können vom Leser nicht nachvollzogen werden. Im Gegensatz dazu wird in den EB zu Abs 2 auf jene Teilnehmer verwiesen, die dem Anbieter des betroffenen Kommunikationsdienstes zuzurechnen sind. Daraus lässt sich nicht ableiten, ob nun die Gesamtzahl der Nutzer im Bundesgebiet als Maßzahl für die Schwellwerte gilt oder die Anzahl an Teilnehmer des jeweiligen Anbieters.

  Auch der Umstand, dass in Z 2 bis 6 jeweils zwei Schwellwerte genannt sind, nämlich eine prozentuelle und eine absolute, führt nicht zur mehr Klarheit. Wenn Erstere auf die Gesamtzahl der Nutzer im Bundesgebiet abstellt, handelt es sich ebenfalls um eine relativ robuste absolute Zahl. Im Ergebnis wären dann zwei Schwellwerte je Ziffer in der VO genannt, was Verwirrung stiften könnte.

  Gem. Abs 4 und den EB dazu sind die Schwellwerte des Abs 2 auf der Webseite der Regulierungsbehörde zu veröffentlichen, wie dies bereits heute der Fall ist. Aus Sicht von Magenta sollte diese Praxis beibehalten werden und die missverständliche Formulierung des Abs 2 nicht dazu führen, dass davon abgewichen wird. Relevant für eine Informationsverpflichtung kann dabei immer nur die Anzahl der betroffenen Teilnehmer iSd § 3 Z 19 TKG 2003 sein, da der Betreiber nur über diese Gruppe Auskunft geben kann.

  Magenta regt an die bisherige Praxis der Veröffentlichung der Schwellwerte auf der RTR Webseite fortzusetzen und dies in Abs 2 zu verankern.

- Eine Information der Öffentlichkeit über einen Sicherheitsvorfall durch die Regulierungsbehörde gem. Abs 3 sollte nur in einem absoluten Ausnahmefall erfolgen. Hierbei sollte eine strenge Verhältnismäßigkeitsprüfung durchgeführt werden.

  Magenta regt an in den EB zu Abs 3 festzuhalten, dass die Information der Öffentlichkeit durch die Regulierungsbehörde einer strengen Verhältnismäßigkeitsprüfung zu unterziehen ist.

Ad § 4 Warnhinweis

- Magenta begrüßt die Möglichkeit eines (freiwilligen) Warnhinweises, da dieser dem Anbieter die Chance gibt, die Regulierungsbehörde über einen etwaigen Sicherheitsvorfall zu informieren ohne, dass dem Betreiber das Ausmaß und die Tragweite des Vorfalls bereits vollständig bekannt ist. Auf diese Art und Weise kann die Regulierungsbehörde frühzeitig informiert werden.

  Als Anreiz für den Betreiber von dieser Möglichkeit Gebrauch zu machen, sollte in den EB zu § 4 ausgeführt werden, dass die Abgabe eines Warnhinweises ein schuldhaftes Verzögern einer Informationspflicht gem. § 3 zumindest für eine bestimmte Zeitspanne (z.B.: 12 Stunden) ausschließt. Denn die

Regulierungsbehörde wurde mittels des Warnhinweises informiert, bevor die Schwellwerte des § 3 Abs 2 überschritten wurden. Eine Folgemeldung nach Überschreiten des Schwellwerts ist eine Konkretisierung des Warnhinweises, was aufgrund der bereits erfolgten ersten Meldung ein schuldhaftes Zögern ausschließt. Sowohl die Regulierungsbehörde als auch die Anbieter würden von so einem Vorgehen in der Praxis profitieren. Die Behörde würde sehr früh von potentiellen Sicherheitsvorfällen erfahren und die Anbieter müssten nicht im bereits geschilderten Graubereich der unverzüglichen Meldung agieren (siehe Ausführungen zum Begriff „unverzüglich" in den Begriffsbestimmungen).

Magenta regt an in den EB klarzustellen, dass die Abgabe eines Warnhinweises einem schuldhaften Zögern, das potentiell strafbewährt ist, zumindest für eine bestimmte Zeitspanne, entgegensteht.

- Es sollte die Möglichkeit geben, den Warnhinweis für die Weiterleitung an das zuständige Computer-Notfallteam mit einer bestimmten Vertraulichkeitsstufe zu klassifizieren. Dies könnte mit Hilfe eines sog. Traffic Light Protokolls gemacht werden. Dadurch könnte der Anbieter festlegen, wie vertraulich die von ihm übermittelten Informationen sind und mit welchen Personenkreis das zuständige Computer-Notfallteam diese teilen darf. Dies stellt eine bisher bereits im Kreise der mit Sicherheitsthemen beauftragten Personen übliche Praxis dar, die auch für den Warnhinweis angedacht werden sollte.

  Magenta regt an die Möglichkeit zu schaffen, den Warnhinweis mit Hilfe eines Traffic Light Protokolls oder eines ähnlich gelagerten Instruments, klassifizieren zu können.

- Im Entwurf der TK-NSiV ist vorgesehen, dass das zuständige Computer-Notfallteam den Warnhinweis und die Mitteilungen zusammengefasst an den Bundesminister für Inneres (BMI) weiterleiten kann. In diesem Zusammenhang ist unklar, wie solch eine Zusammenfassung auszusehen hat, die weitergeleitet werden kann. Dies steht außerdem im Widerspruch zur ebenfalls im Entwurf verankerten Möglichkeit, dass der Übermittler des Warnhinweises einer Weiterleitung an den BMI zustimmen muss. Diese Zustimmung vor Weitergabe an den BMI ist aus unserer Sicht essentiell, da nur so sichergestellt ist, dass das betroffene Unternehmen einen Anreiz hat die Möglichkeit den Warnhinweises zu nutzen und nicht durch eine nicht vom Unternehmen autorisierte Weiterleitung an das BMI abgeschreckt wird.

  Magenta regt an den Satz „*Das zuständige Computer Notfallteam kann den Warnhinweis und die Mitteilungen zusammengefasst an den Bundesminister für Inneres weiterleiten.*" ersatzlos zu streichen.

Ad § 5 Mindestsicherheitsmaßnahmen

- Gem. Abs 1 Z 2 dieser Bestimmung muss die Information Security Policy auch Angaben über die Sicherheit im Hinblick auf Personal beinhalten. Magenta geht davon aus, dass diese Informationen generischer Natur sein können und keine personenbezogenen Daten beinhalten müssen, da dies nicht für die Überprüfung der Einhaltung dieser Bestimmung notwendig ist. Abzustellen ist vielmehr auf Prozesse und Vorkehrungen um die in Z 2 geforderten Anforderungen zu erfüllen.

  Magenta regt an, dass in den EB festgehalten wird, dass keine personenbezogenen Daten für die Einhaltung dieser Bestimmung inkludiert werden müssen.

- Die Regulierungsbehörde kann gem. Abs 2 Unterlagen zur Beurteilung der Einhaltung der Mindestsicherheitsmaßnahmen anfordern. Aus dieser Bestimmung ist jedoch nicht ersichtlich, ab wann eine solche Anforderung gestellt werden kann. Da Anbieter die entsprechenden Unterlagen vorbereiten und sich einen Überblick verschaffen müssen, sollte nach Inkrafttreten der TK-NSiV ein bestimmter Zeitraum liegen.

  Magenta regt an, dass eine erstmalige Anforderung durch die Regulierungsbehörde 12 Monate nach Inkrafttreten der TK-NSiV erfolgen kann.

Ad § 6 Sicherheitsanforderungen an 5G Netze

- Wie in der Einleitung der Stellungnahme bereits ausgeführt, ist die Sicherheit und Stabilität aller Netze ein essentielles Anliegen von Magenta. Umso mehr gilt dies für das neue 5G Netz. Aus unserer Sicht sollte der Fokus der TK-NSiV im Allgemeinen und des § 6 im Speziellen auf der faktischen Durchsetzung, Einhaltung und Wahrung von hohen Sicherheitsstandards liegen und nicht auf der Art und Weise wie eine solche bescheinigt oder nachgewiesen werden kann. Wichtig ist die tatsächliche Einhaltung der Sicherheitsstandards und nicht so sehr die Form der Dokumentation und der Nachweis derselbigen. Die materiellen Aspekte von § 6 sollten daher mehr im Vordergrund stehen als die formellen, da dies die Implementierungskosten für die Betreiber erhöht, ohne einen sicherheitsrelevanten Mehrwert zu bieten.
  Magenta regt an § 6 entsprechend umzugestalten.
- Im Entwurf der VO werden Betreiber von 5G Netzen, die mehr als 100 000 Teilnehmer in allen von ihnen betriebenen Mobilfunknetzen aufweisen, als Adressat für die Sicherheitsanforderungen normiert. Aus Sicht von Magenta droht dadurch der Sinn und Zweck der TK-NSiV unterlaufen zu werden, denn es sind durchaus Szenarien denkbar, in denen kleinere Anbieter 5G Anwendungen auf den Markt bringen, die von wenigen Teilnehmern massenhaft eingesetzt werden. Ein anschauliches Beispiel wäre dafür eine größere Stadt als Kunde eines Anbieters, der ausschließlich ein 5G Netz betreibt. Die Stadt zählt nur als ein Teilnehmer iSd § 3 Z 19 TKG 2003, wenn diese jedoch einen Teil ihrer Infrastruktur (z.B.: Strassenlaternen, Verkehrsampeln) über 5G steuert, wäre dies im Falle eines Ausfalls als kritisch zu betrachten. Das bloße Abstellen auf die Anzahl der Teilnehmer greift also zu kurz. Besser wäre es auf die quantitative Anzahl der Anwendungen oder auf Netzabschlusspunkte abzustellen, um das potentielle Ausfallsrisiko besser erfassen zu können. Alternativ könnten die Sicherheitsanforderungen ganz allgemein an Mobilfunkdiensteanbieter gerichtet werden und Ausnahmen für besonders kleine Anbieter geschaffen werden.

  Magenta regt an den Adressatenkreis des § 6 deutlich zu erweitern, um die Zielsetzung der TK-NSiV abzusichern.
- Betreiber werden zur Vorlage von Auditberichten verpflichtet, welche das Bestehen eines Informationssicherheitsmanagementsystems gemäß einer anerkannten Norm nachweisen. Hinsichtlich dieser Verpflichtung bestehen für den Normunterworfenen einige Unklarheiten:

- Es ist nicht klar, auf welche Bereiche des Unternehmens sich die Auditierung beziehen muss. Es macht einen großen Unterschied, ob nur bestimmte Bereiche eines Unternehmens oder das gesamte Unternehmen auditiert werden müssen.
- Wer kommt als Autor eines solchen Auditberichts in Frage? Kann dieser auch im Rahmen eines Self-Assessment erstellt werden?
- In den EB werden bestimmte Normen genannt, welche als anerkannt im Sinne der Bestimmung in Frage kommen. Können darüber hinaus noch andere Normen einschlägig sein?
- Eine Auditierung auf Basis der in den EB genannte Norm ISO 27 001 würde für Magenta substantielle Kosten in der Höhe von mehreren € 100.000 und einigen Mannjahren Arbeitszeit verursachen und der Prozess wäre auch schwer innerhalb der vorgesehenen Frist bis zum 31. Dezember 2021 abzuschließen. Durch den Umstand, dass die VO „nur" die Vorlage eines Auditberichts, anstatt einer Zertifizierung vorsieht, reduzieren sich die Kosten und der Aufwand für Magenta nicht. Dies stellt keine Erleichterung für uns dar.
- Für Magenta als Tochterunternehmen eines großen Konzerns könnte auch eine Gruppenzertifizierung in Frage kommen. Wäre eine solche Zertifizierung samt Auditbericht ausreichend, um die Anforderungen der VO zu erfüllen?

Magenta regt an den betroffenen Unternehmen mehr Freiheitsgrade betreffend der für den Auditbericht anzuwendenden Norm zu geben und die Erstellung des Auditberichts so einfach wie möglich zu gestalten, um die Kosten-Nutzen Relation und die Verhältnismäßigkeit zu wahren.

- Betreiber von 5G Netzen müssen eine Konformitätserklärung über die Einhaltung der in Anhang 1 angeführten Standards abgeben. Aus Sicht von Magenta ist ebenjene Liste zu umfangreich und zu unspezifisch. Anstatt eine lange Aufzählung von Standards vorzusehen, sollten von der Regulierungsbehörde konkrete Sicherheitsvorgaben gemacht bzw. die Liste auf die wesentlichen Standards gekürzt werden. Anhang 1 ist in seiner derzeitigen Form überschießend. In der VO wird dessen Inhalt auch nicht begründet oder einer Verhältnismäßigkeitsüberprüfung unterzogen.

  Abgesehen davon sollte aus der VO hervorgehen, dass nur jene Version der Standards für die betroffenen Unternehmen gilt, welche zum Zeitpunkt des Inkrafttretens der VO bereits veröffentlicht sind. Spätere Novellierungen von Standards können nicht berücksichtigt werden, da dies ein laufendes Monitoring auf Seiten der Betreiber voraussetzen würde, was entsprechend kostenintensiv wäre.

  Magenta regt daher an die Anhang 1 Liste deutlich zu kürzen und/oder konkrete Vorgaben aus den gelisteten Standards zu entnehmen, um den Umsetzungsaufwand zu reduzieren.
- Desweiteren werden in Abs 3 mehrere Sicherheitsvorgaben gemacht, aus welchen die spezifische Verpflichtung nicht eindeutig ersichtlich ist. Z 1 nennt dazu den Betrieb von NOC und SOC in eigenen Räumlichkeiten innerhalb der Europäischen Union. Aus dem Wortlaut der Verpflichtung und den EB lässt sich nicht schließen, ob damit gemeint ist, dass NOC und SOC sich in einer Betriebsstätte des Betreibers befinden müssen oder ob NOC und SOC in separaten Räumlichkeiten innerhalb der Betriebsstätte

betrieben werden müssen. Zweiteres ergibt aus unserer Sicht keinen Sinn, da sich die Aufgaben teilweise überschneiden und eine räumliche Nähe der verantwortlichen Personen die Arbeit erleichtert. Ebenso lässt sich keine sachliche Begründung erblicken zu fordern, dass nur eigene Räumlichkeiten geeignet wären, um NOC und SOC zu betreiben, solange diese in der Europäischen Union liegen. Es muss weiterhin in der unternehmerischen Gestaltungsfreiheit liegen den Betrieb von NOC und/oder SOC outsourcen zu können.
Magenta regt daher an das Wort „*eigenen*" in § 6 Abs 3 Z 1 ersatzlos zu streichen.

- Der Normgehalt der in Z 7 formulierten Anforderung der Existenz einer Multi-Vendor Strategie ist unklar. Auch ein Studium der EB trägt wenig zur Klärung bei, so wird diesbezüglich auf die „*Auswahlmöglichkeit eines Betreibers unter zumindest zwei Lieferanten für Netzinfrastrukturelemente eines 5G-Netzes gemäß § 2 Z 9*" verwiesen.

  In unserem Verständnis dieser Anforderung wäre es ausreichend, wenn ein Betreiber einen zweiten Lieferanten benennen könnte, der als Alternative bereitstünde für den Fall, dass der aktuell gewählte Lieferant ausfällt. Es sollte in der VO klargestellt werden, dass darüber hinaus keine Verpflichtungen aus dieser Bestimmung bestehen. Sollte es aus technischen Gründen (z.B.: Kompatibilität, Netzsicherheit) nicht möglich sein, einen anderen Lieferanten zu wählen, sollte dies als Begründung ausreichen, um die Anforderung zu erfüllen. Wir gehen auch davon aus, dass sich die Multi-Vendor Strategie auf das gesamte 5G Netz bezieht und nicht auf einzelne Komponenten. Ein pauschaler Nachweis eines alternativen Lieferanten sollte der Anforderung daher entsprechen.

  Ein weitergehender Norminhalt, wie etwa die Verpflichtung mehr als nur einen Lieferanten für das 5G Netz zu haben, wäre ein massiver Eingriff in die unternehmerische Freiheit und in ein bereits existierendes Netz. Magenta ist der erster Anbieter in Österreich der 5G kommerziell angeboten hat und verfügt dementsprechend bereits über ein aktives 5G Netz. Ein regulatorischer ex post Eingriff würde zu substantiellen Mehrkosten führen und entbehrt jeglicher sachlicher Rechtfertigung. Wir vertreten die Ansicht, dass aktuell kein Grund für eine regulatorische Intervention hinsichtlich einer verpflichtenden Multi-Vendor Strategie existiert.

  Magenta regt an in der VO klarzustellen, dass die Multi-Vendor Strategie nicht zum verpflichtenden Einsatz von zwei Lieferanten für das 5G Netz führt.

- Die Sicherheitsanforderungen des Abs 4 verpflichten Anbieter zu halbjährlichen, sehr umfassenden Datenlieferungen betreffend der Funktionen und Hersteller von sicherheitsrelevanten Komponenten. In Anhang 2 findet sich eine Liste an einzumeldenden Komponenten, wobei diese sehr allgemein beschrieben sind. Ebenso ermächtigt der VO Entwurf die Regulierungsbehörde Angaben zu weiteren Komponenten einzufordern. Nicht nur die allgemein gehaltene Beschreibung der Komponenten in Anhang 2, auch diese Öffnungsklausel sind nicht geeignet um normunterworfenen Unternehmen Rechtsicherheit und Auskunft über die konkrete Einmeldeverpflichtung zu geben. Das gewählte Intervall von 6 Monaten ist zu kurz und erzeugt hohe Aufwände auf Seiten der Betreiber, welche halbjährlich die komplette Liste an Komponenten überprüfen und gegebenenfalls aktualisieren und ergänzen müssten.

Der sehr offene Umfang an einzumeldenden Funktionen der Komponenten ist unseres Erachtens überschießend, ebenso wie das im Entwurf vorgesehene Intervall. Da sich die Komponenten eines 5G Netzes nicht alle paar Monate ändern, kann kein Mehrwert aus einer halbjährlichen Einmeldung gewonnen werden. Anhang 2 stellt eine Zusammenstellung aus logischen Funktionen und physischen Netzwerkkomponenten dar, was die Unklarheit betreffend der konkreten Meldeverpflichtung noch erhöht. Stattdessen sollte eine deutlich reduzierte Liste an spezifizierten, sicherheitsrelevanten Komponenten in Anhang 2 angeführt werden, welche im ersten Jahr nach Inkrafttreten der VO eingemeldet werden muss. Von der Einmeldeverpflichtung sollte jeweils nur der Hersteller umfasst sein. Dieser reduzierte Anhang 2 und das vorgeschriebene Format sollten abermals konsultiert werden, da für die Beurteilung der Sinnhaftigkeit und des Umfangs der Verpflichtung auch das Einmeldeformat relevant ist.

Nach erstmaliger Einmeldung sollte diese Liste einmal im Jahr durch den Anbieter auf ihre Aktualität hin überprüft und gegebenenfalls ergänzt oder überarbeitet werden. Dies würde den Aufwand erheblich reduzieren, ohne den Zweck der TK-NSiV zu gefährden.

Magenta regt an Abs 4 und Anhang 2 dahingehend zu ändern und die reduzierte Anhang 2 Liste samt Einmeldeformat abermals zu konsultieren.

- Die TK-NSiV und ihr Vollzug liegen 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 Bundes entsprechend erhöht werden. Andernfalls würden die Betreiber für Kosten aufkommen, die durch den Vollzug von öffentlichen Interessen verursacht wurden.

  Magenta regt an die Kosten für den Vollzug der TK-NSiV im RTR Budget 2021 entsprechend vorzusehen.

Für Rückfragen stehen wir jederzeit zur Verfügung und verbleiben mit freundlichen Grüßen,

Mag. Anja Tretbar-Bustorf

VP Corporate Affairs
T - Mobile Austria GmbH