Erläuterungen

Hauptgesichtspunkte der Verordnung

Die TK-NSiV 2020 normiert einerseits Informationspflichten von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste bei Sicherheitsvorfällen im Zusammenhang mit elektronischen Kommunikationsnetzen und -diensten, die zu beträchtlichen Auswirkungen auf den Netzbetrieb oder die Dienstebereitstellung geführt haben. Zudem regelt sie das Vorgehen der Regulierungsbehörde bei derartigen Sicherheitsvorfällen. Überdies legt sie Rahmenbedingungen einer Erstattung von Mitteilungen in Bezug auf Sicherheitsvorfälle ohne beträchtliche Auswirkungen auf Netzbetrieb oder Dienstebereitstellung fest.

Andererseits stellt sie Anforderungen an die von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste zur Gewährleistung einer angemessenen Beherrschung der Risiken für elektronische Kommunikationsnetze und -dienste und Aufrechterhaltung des diesbezüglich geeigneten Sicherheitsniveaus zu ergreifenden Mindestsicherheitsmaßnahmen unter besonderer Berücksichtigung der Sicherheit von 5G-Netzen auf. Hinsichtlich der Sicherheit von 5G-Netzen werden einige der Vorgaben aus dem diesbezüglichen EU-Instrumentarium („5G-Toolbox“) umgesetzt.

§ 1. Zweck und Anwendungsbereich

Abs. 1: Abweichend von § 3 Z 6 NISG wird hier der Begriff Sicherheitsvorfall konform zu Art. 2 Z 42 der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (European Electronic Communications Code – EECC) verwendet.

Abs. 3: Für Rundfunknetze und für Übertragungsdienste in Rundfunknetzen besteht eine Zuständigkeit der Kommunikationsbehörde Austria.

§ 2. Begriffsbestimmungen

Z 1: Da der Begriff „Sicherheit von Netzen und Diensten“ bislang nicht in den Begriffsbestimmungen des TKG 2003 enthalten war, wurde eine entsprechende EECC-konforme Definition aufgenommen.

Z 2: Beim böswilligen Angriff wurde die Möglichkeit einer vorsätzlichen Beeinträchtigung der Funktion des angegriffenen Netzes oder Dienstes vorgesehen, um auch DDoS-Attacken erfassen zu können. Eine vorsätzliche Beeinträchtigung umfasst nicht nur Angriffe von außerhalb, sondern auch innerhalb des Unternehmens.

Z 4: Das im Klammerausdruck genannte Beispiel „epidemische Krankheit“ schließt auch eine Pandemie ein.

Z 6: Da eine besondere Gefährdung durch Zusammenschaltungspartner im Vergleich zu Abhängigkeiten von anderen Drittbeziehungen nicht ersichtlich ist, erscheint eine zusätzliche Anführung dieser Gruppe als Beispiel für „Drittversagen“ nicht geboten.

Z 8: „Unverzüglich“ bedeutet ohne schuldhaftes Zögern, wobei die Informationspflichten jedenfalls nicht auf die Geschäftszeiten des Betreibers beschränkt sind. Die Informationspflicht besteht, sobald absehbar ist, dass der Vorfall beträchtliche Auswirkungen hervorrufen wird. Im Zweifel wird von einer Meldepflicht auszugehen sein.

Z 9: In Z 9 wurde eine Definition des Begriffs „5G-Netz“ aufgenommen, die jener in Punkt 2 lit. a der Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 „Cybersicherheit der 5G-Netze“ entspricht. Aus Gründen der Konsistenz mit dieser Empfehlung wurde der Klammerausdruck „4G oder 3G“ entgegen den Forderungen einiger Konsultationsteilnehmer belassen. Die ebenfalls im Konsultationsverfahren geforderte Einschränkung des Begriffs „5G-Netz“ auf „5G-Standalone“ steht nicht im Einklang mit der erwähnten Empfehlung.

Eine Aufnahme zusätzlicher Begriffsbestimmungen erschien nicht notwendig. Bei einigen Begriffen ist dies nicht sinnvoll, da sie Bestandteil bestehender Legaldefinitionen aus der RL 2018/1972/EU sind („Ereignis“ vgl. Art 2 Z 42, „bestimmtes Vertrauensniveau“ vgl. Art. 2 Z 21).

Der Begriff „Dienstekategorie“ ist selbsterklärend und wird nur in § 3 verwendet. Der Begriff „unverzüglich“ bedarf im gegebenen Kontext keiner Ergänzung.

§ 3. Informationspflichten

Die gewünschte ausdrückliche Ausdehnung der Meldepflicht auf OTT-Anbieter soll mit Umsetzung der entsprechenden Vorschriften der RL 2018/1972/EU in nationales Recht erfolgen. Eine Einschränkung der Meldepflicht auf öffentliche Kommunikationsnetze oder ein Ausnehmen von M2M-Diensten würde die Teilnehmer nicht öffentlicher Kommunikationsnetze und die Nutzer von M2M-Applikationen aus dem Schutzbereich der Netzsicherheitsvorschriften ausnehmen, wofür eine entsprechende Rechtfertigung nicht ersichtlich ist.

Zur Kritik an einer allfälligen doppelten Meldepflicht an Datenschutzbehörde und RTR-GmbH vor dem Hintergrund der Begriffsdefinition in § 2 . 1, nach welcher „Sicherheit von Netzen und Diensten“ auch die Vertraulichkeit der gespeicherten, übermittelten oder verarbeiteten Daten einschließt, wird klargestellt, dass die Meldung einer Verletzung des Schutzes personenbezogener Daten nach Art. 2 Abs. 2 VO 2013/611/EU ausschließlich an die Datenschutzbehörde zu richten ist. Falls der Betroffene feststellt, dass die Datenschutzverletzung auf Mängel in Bezug auf die Sicherheit von Kommunikationsnetzen und –diensten zurückzuführen ist, wird bei Vorliegen beträchtlicher Auswirkungen iSd § 3 Abs. 2 (bei Überschreiten der Schwellwerte) auch eine Meldung an die Regulierungsbehörde erforderlich sein.

Die im Konsultationsverfahren angeregte Möglichkeit der Bezugnahme auf einen zuvor betreffend denselben Sicherheitsvorfall übermittelten Warnhinweis erleichtert die Zuordnung und dient zur Information, dass der Einmelder seiner Pflicht zur unverzüglichen Bekanntgabe des Sicherheitsvorfalls genügt hat.

Abs. 1: Die von den Betreibern öffentlicher Kommunikationsnetze oder Anbietern öffentlicher Kommunikationsdienste zu übermittelnden Informationen ergeben sich aus dem von den Mitgliedstaaten der Europäischen Union unter Mitwirkung der ENISA verabschiedeten Dokument „Technical Guideline on Reporting Incidents“, Version 2.1, Oktober 2014. Das Dokument liegt bei der Regulierungsbehörde zur Einsichtnahme auf und ist auf deren Website unter http://www.rtr.at/de/tk/Netzsicherheit/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf allgemein zugänglich.

Abs. 1 Z 1: Ist der exakte Beginnzeitpunkt des Vorfalls nicht feststellbar, kann auch der Zeitpunkt angegeben werden, an dem der Betroffene erstmals vom Vorfall Kenntnis erlangt hat. Den Anregungen zur Aufnahme einer Maximalfrist von 24 Stunden für die Erstmeldung und drei Arbeitstagen für die Folgemeldung wurde nicht nachgekommen, da beides den Anreiz zu einer raschestmöglichen Meldung verringert.

Abs. 1 Z 3: vgl. hierzu ENISA-Guideline „Threats and Assets“, https://www.rtr.at/de/tk/Netzsicherheit/Article_13a_ENISA_Technical_Guideline_On_Threats_And_Assets.pdf , Version 1.2, August 2015.

Abs. 1 Z 5: Die Anzahl der in der jeweiligen Dienstekategorie betroffenen Teilnehmer beinhaltet bei Mobiltelefonie und mobilen Internetzugängen neben aktivierten SIM-Karten auch eSIMs. Bei Erbringung von Diensten auf einer SIM-Karte oder eSIM, die zu mehr als einer Dienstekategorie gehören (Mobiltelefonie, mobiler Internetzugang), ist die Anzahl der betroffenen SIM-Karten einschließlich eSIMs jeweils in den Dienstekategorien lit. b und d anzugeben. Bei Erbringung von Diensten über einen Festnetzanschluss, die sowohl zur Dienstekategorie Festnetztelefonie als auch zur Dienstekategorie fester Internetzugang gehören, ist die Anzahl jeweils in den Dienstekategorien lit. a und c anzugeben. Bei der Erbringung von Internetzugangsdiensten über eine Kombination aus festem und mobilem Internetzugang (sog. „Hybridprodukte“) ist die Anzahl abhängig von der beeinträchtigten Kategorie jeweils in den Dienstekategorien lit. c und d anzugeben.

Abs. 1 Z 5 lit. b und d: Falls die exakte Anzahl nicht ermittelbar ist, kann diese anhand des auf Erfahrungswerten basierenden Mittelwerts der Nutzer der betroffenen Funkzellen abgeschätzt werden.

Abs. 2: Unter den betroffenen Teilnehmern der jeweiligen Dienstekategorie sind nur jene Teilnehmer zu verstehen, die dem Anbieter des betroffenen Kommunikationsdienstes zuzurechnen sind.

Abs. 4: Bei der Ermittlung der Gesamtzahlen der Nutzer eines Dienstes im Bundesgebiet kann sich der Betreiber an den von der Regulierungsbehörde unter https://www.rtr.at/de/tk/MitteilungVorflle veröffentlichten Daten orientieren.

§ 4. Warnhinweis

Die Bestimmungen in Bezug auf Warnhinweis und Folgemitteilungen in Bezug auf Risiken oder Vorfälle, die nicht der Meldepflicht nach § 3 Abs. 1 unterliegen, sind den §§ 19 Abs. 3, 23 NISG nachgebildet und enthalten diesbezügliche Rahmenbedingungen. Der im Konsultationsverfahren geäußerten Forderung nach Streichung der zusammengefassten Weiterleitung des Warnhinweises und der Folgemitteilungen durch das zuständige Computer-Notfallteam an den Bundesminister für Inneres wurde nachgekommen; diesbezüglich wird jedoch klargestellt, dass eine derartige Weiterleitung nach § 23 Abs. 2 iVm Abs. 3 NISG ohnehin zu erfolgen hat.

§ 5. Mindestsicherheitsmaßnahmen

Abs. 1: Die Bereiche, die Betreiber öffentlicher Kommunikationsnetze oder Anbieter öffentlicher Kommunikationsdienste durch Sicherheitsmaßnahmen abdecken müssen, ergeben sich aus dem von den Mitgliedstaaten der Europäischen Union unter Mitwirkung der ENISA verabschiedeten Dokument „Technical Guideline on Security Measures“, Version 2.0, Oktober 2014. Das Dokument liegt bei der Regulierungsbehörde zur Einsichtnahme auf und ist auch auf deren Website unter
https://www.rtr.at/de/tk/Netzsicherheit/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf allgemein zugänglich. Zu den Sicherheitsmaßnahmen zählt auch die Festlegung einer Information Security Policy. Darunter ist eine von der Führung einer Organisation approbierte Richtlinie zu verstehen, die den Ansatz der Organisation zur Erreichung von Informationssicherheitszielen darlegt. Eine Information Security Policy sollte Anforderungen adressieren, die sich aus der Geschäftsstrategie, Gesetzen und Vereinbarungen sowie gegenwärtigen und zu erwartenden Bedrohungen für die Informationssicherheit ergeben. Die Information Security Policy sollte folgende Angaben enthalten:

a) Definition der Informationssicherheit, Ziele und Grundsätze, von denen man sich bei allen Tätigkeiten betreffend Informationssicherheit leiten lässt;

b) Zuweisung von allgemeinen und spezifischen Verantwortlichkeiten für das Informationssicherheitsmanagement an definierte Rollen;

c) Prozesse zur Behandlung von Abweichungen und Ausnahmen.

Auf einer darunter befindlichen Ebene sollte die Information Security Policy durch themenspezifische Policies unterstützt werden, die die Umsetzung von Sicherheitsmaßnahmen konkretisieren und typischerweise so strukturiert sind, dass sie die Bedürfnisse bestimmter Zielgruppen innerhalb der Organisation adressieren oder bestimmte Themen abdecken (vgl. ISO/IEC 27002:2013, 5.1.1).

Soweit im Konsultationsverfahren die Notwendigkeit einer Gewährleistung der Versorgungssicherheit in Bezug auf Software besonders hervorgehoben wurde, wird darauf hingewiesen, dass dieses Thema von § 5 Abs. 1 Z 3 (Versorgungssicherheit allgemein) und Z 4 (Änderungsmanagement, das auch SW-Patches umfasst) abgedeckt wird.

Die gewünschte maximale Umsetzungsfrist (sechs Monate bzw ein Jahr) nach Inkrafttreten dieser Verordnung zur Erfüllung der Mindestsicherheitsmaßnahmen wurde nicht aufgenommen. Hinsichtlich der Verpflichtung zum Ergreifen dieser Mindestsicherheitsmaßnahmen erfolgt keine Änderung an dem seit vielen Jahren geltenden Rechtszustand. Musterkonzepte zur Erstellung von Dokumenten, in denen derartige Mindestsicherheitsmaßnahmen festgehalten werden können, sind kostenfrei verfügbar (vgl. etwa https://www.ispa.at/wissenspool/vorlagen/ispa-mustersicherheitskonzept.html)

§ 6. Sicherheitsanforderungen an 5G-Netze

§ 6 setzt die Empfehlung (EU) 2019/534 der Europäischen Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze um und enthält hinsichtlich der von Betreibern öffentlicher Kommunikationsnetze oder Anbietern öffentlicher Kommunikationsdienste zu ergreifenden Sicherheitsmaßnahmen ergänzende Bestimmungen, die unter Berücksichtigung der diesbezüglich auf EU-Ebene nach Durchführung einer entsprechenden Risikoabschätzung zusammengefassten Empfehlungen („EU-Instrumentarium“, vgl. das Dokument CG 01/2020 der NIS Cooperation Group „Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures“, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures) sowie die Mitteilung der Europäischen Kommission COM(2020)50 vom

29.01.2020 an das Parlament, den Rat, den Wirtschafts- und Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: „Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums“) sicherstellen sollen, dass erhöhten Sicherheitsrisiken, die mit dem Betrieb von 5G-Netzen verbunden sind, angemessen begegnet werden kann.

Die von einzelnen Konsultationsteilnehmern geforderte Ausweitung der Anforderungen an 5G-Netze auf Open-Access-Netze, Netze von Zusammenschaltungspartnern sowie Internet-Exchange-Knoten und andere Akteure mit Nutzungsrechten an 5G-Frequenzen, die Infrastruktur im Slicing-Betrieb oder mit Multi Access Edge Computing nutzen möchten, ist tlw problematisch – so unterliegen etwa Internet Exchange-Knoten dem NISG und fallen mangels Erbringung von Telekommunikationsdiensten nicht in den Anwendungsbereich des TKG bzw dieser Verordnung – und angesichts der geringeren Teilnehmerzahlen auch nicht geboten.

Abs. 1: Da die von den Betreibern zu ergreifenden Sicherheitsmaßnahmen ein Sicherheitsniveau gewährleisten müssen, das zur Beherrschung der Risiken geeignet ist, und die Risiken von der Eintrittswahrscheinlichkeit und den potenziellen Auswirkungen eines Sicherheitsvorfalls abhängen, ist es gerechtfertigt, das Ausmaß des Risikos unter Berücksichtigung der Anzahl der Teilnehmer zu bewerten. Da vergleichbare Vorschriften wie zB § 10 Abs. 1 Z 2 lit. a Netz- und Informationssicherheitssystemverordnung („NISV“), BGBl. II Nr. II 215/2019, eine Zahl von 88.000 Teilnehmern bei Kommunikationsdiensten im Bereich des Betriebs von DNS-Diensten als wesentlichen Diensten im Sektor „Digitale Infrastruktur“ heranziehen, ist es gerechtfertigt, auch zur Bewertung des erhöhten Risikos durch den Betrieb von 5G-Netzen in einer zukunftsgerichteten Betrachtung unter Berücksichtigung der Entwicklung der Teilnehmerzahlen bis zum ersten Nachweiszeitpunkt von einem entsprechend höheren Wert auszugehen.

Um dem erhöhten Risiko zu begegnen, sind ein funktionierendes Informationssicherheitsmanagement sowie allgemeine und telekommunikationsspezifische Informationssicherheitsmaßnahmen erforderlich. Das funktionierende Informationssicherheitsmanagement kann durch Vorlage eines Auditberichts über die Einhaltung der Anforderungen gemäß „ÖVE/ÖNORM EN ISO/IEC 27 001:2017, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27 001:2013 + Cor 1:2014 + Cor 2:2015)“ nachgewiesen werden. Die Festlegung und Umsetzung allgemeiner Informationssicherheitsmaßnahmen kann durch eine Anwendbarkeitserklärung iSv. ISO 27 001, Abschnitt 6.1.3, lit. d, dokumentiert werden. Die Festlegung und Umsetzung telekommunikationsspezifischer Informationssicherheitsmaßnahmen kann durch eine analoge Erklärung zur Festlegung und Umsetzung der in „ÖVE/ÖNORM EN ISO/IEC 27 011:2020, Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen auf Grundlage von ISO/IEC 27002 für Telekommunikationsorganisationen“ angeführten Sicherheitsmaßnahmen dokumentiert werden.

Anstelle der vorerwähnten Normen können auch von der Regulierungsbehörde als gleichwertig angesehene Standards wie zB die Standards 200-1, 200-2, 200-3 des deutschen. Bundesamts für Sicherheit in der Informationstechnik iVm. ITU-T-Empfehlung X.1051 angewandt werden. Soweit im Konsultationsverfahren auf die Möglichkeit von Selbstaudits verwiesen wurde, wird nun klargestellt, dass zur Erstellung von Auditberichten diesbezüglich akkreditierte Prüfstellen oder qualifizierte Stellen gemäß § 3 Z 11 NISG herangezogen werden müssen. Der für den erstmaligen Nachweis genannte Zeitpunkt soll jenen Betreibern, die die Normen derzeit nicht erfüllen, ermöglichen, die diesbezüglichen Voraussetzungen für eine Zertifizierung zu schaffen und den Zertifizierungsprozess zu durchlaufen. Die Dreijahresfrist für die Wiedervorlage entspricht üblichen Auditzyklen.

Abs. 2: Betreiber von 5G-Netzen mit mehr als 100 000 Teilnehmern haben aufgrund des EU-Instrumentariums überdies auch die in den im Anhang angeführten relevanten 3GPP- und ETSI-Technologiestandards (vgl. https://www.3gpp.org/DynaReport/33-series.htm) vorgesehenen Sicherheitsmaßnahmen zu ergreifen sowie von der ENISA definierte „Virtualization Good Practises“ zu beachten und durch eine Konformitätserklärung des Betreibers zu dokumentieren. Sämtliche der in Anhang 1 angeführten Dokumente sind öffentlich zugänglich. Der Anforderung des EU-Instrumentariums, in angemessener Weise auch eine Umsetzung optionaler Teile der 3GPP-Technologiestandards sicherzustellen, wird dadurch Rechnung getragen, dass der Betreiber Abweichungen hinsichtlich der optionalen Teile zB durch vergleichbare Sicherheitsmaßnahmen, mit denen dasselbe Sicherheitsziel erreicht wird, zu begründen hat. Der Anregung aus dem Konsultationsverfahren, die angeführten ETS-GS-NFV-SEC-Standards durch das ENISA-Dokument „Security Aspects of virtualization“ (vgl. https://www.enisa.europa.eu/publications/security-aspects-of-virtualization/

at_download/fullReport, Feb 10, 2017) zu ersetzen, wurde nachgekommen. Die Notwendigkeit zur Einhaltung des vorerwähnten ENISA-Dokuments und insb der Vorgaben aus dessen Kapitel 3 „Virtualization Good Practices“ anstelle der zuvor angeführten ETSI-Standards zu Network Function Virtualisation („NFV“, vgl. https://www.etsi.org/standards#page=1&search=&title=1&etsiNumber=1&content=1&version=0&onApproval=0&published=1&historical=0&startDate=&endDate=&harmonized=0&keyword=&TB=799&stdType=&frequency=&mandate=&collection=&sort=1) ergibt sich aus dem Umstand, dass die durch die Virtualisierung herbeigeführte Komplexität auch erhöhte Risiken in sich birgt, und der Anforderung des EU-Instrumentariums, dass 5G-Betreiber in Bezug auf NFV gute Praktiken befolgen sollen. Die Notwendigkeit zur Einhaltung der im ENISA-Dokument „Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services“ (vgl. https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services) angeführten Empfehlungen folgt der Anforderung im EU-Instrumentarium zur Einhaltung spezifischer Sicherheitsstandards im Beschaffungsprozess bei IKT-Komponenten und Dienstleistungen. Die im Konsultationsverfahren geäußerte Vermutung, eine Umsetzung der Vorgaben der vorerwähnten „Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services“ könne erst für Vergaben nach dem 30.06.2021 gelten, ist in dieser Form unzutreffend; vielmehr ist bis zum genannten Zeitpunkt die entsprechende Konformitätserklärung vorzulegen, aus der hervorgeht, dass die ENISA ICT Baseline Security Requirements bereits eingehalten werden.

Abs. 3: Die angeführten Sicherheitsmaßnahmen entsprechen zusätzlichen Sicherheitsmaßnahmen im EU-Instrumentarium, die sich nicht aus den Anforderungen in Abs. 1 und 2 ergeben.

So soll etwa der Betrieb des Network Operation Centers und Security Operation Centers in eigenen Räumlichkeiten (Räume unter Kontrolle des Betreibers eines 5G-Netzes, zB auch selbst angemietete Rechenzentren, nicht aber Räume externer Dienstleister) und das effektive Monitoring aller kritischen Netzkomponenten und sensibler Teile der 5G-Netze sicherstellen, dass Anomalien entdeckt und Bedrohungen (wie zB durch kompromittierte Endgeräte inkl IoT-Komponenten) identifiziert und verhindert werden. Aus diesen Gründen und aufgrund der Notwendigkeit zur Einhaltung der Vorgaben des EU-Instrumentariums konnte der von zahlreichen Konsultationsteilnehmern begehrten Abschwächung der Anforderung zum Betrieb von NOC und SOC in eigenen Räumlichkeiten – etwa durch Streichung des Worts „eigenen“ – nicht entsprochen werden; klargestellt wird aber, dass NOC und SOC gemeinsam in einem Raum unter Kontrolle des Betreibers eines 5G-Netzes untergebracht und betrieben werden können.

Der Schutz des Management-Verkehrs von Kommunikationsnetzen oder -diensten soll nicht autorisierte Änderungen von Netz- oder Dienstkomponenten verhindern.

Der physische Schutz von kritischen Netzkomponenten und sensiblen Teilen der 5G-Netze mit risikobasiertem Ansatz hat auch Netzkomponenten außerhalb des Kernnetzes wie zB Basisstationen zu umfassen, die zur Erreichung niedrigerer Latenzzeichen miteinander kommunizieren („Multi-access Edge Computing“). Der Kritik im Konsultationsverfahren an einem Fehlen von Begriffsdefinitionen für die in § 6 Abs. 1 Z 2 und 6 verwendeten Ausdrücke „kritische Netzkomponenten“ und „sensible Teile“ ist zu erwidern, dass das mit der Kritikalität von Netzkomponenten und sensiblen Teilen des Netzes einhergehende Risiko nicht statisch ist, sondern abhängig von der aktuellen Situation immer wieder neu bewertet werden muss, weshalb eine abschließende Definition dieser Begriffe nicht möglich ist.

Die Multi-Vendor-Strategie (dh strategische Bewertung des Betreibers eines 5G-Netzes hinsichtlich einer Auswahlmöglichkeit eines Betreibers unter zumindest zwei Lieferanten für Netzinfrastrukturelemente eines 5G-Netzes gemäß § 2 Z 9 unter Berücksichtigung des Stands der Technik und Orientierung an entsprechenden Empfehlungen der Europäischen Union) soll Abhängigkeiten von einem einzigen Lieferanten (oder Lieferanten mit ähnlichem Risikoprofil) aufzeigen und Abhängigkeiten von Lieferanten, die zu einem hohen Risiko führen können, ersichtlich machen und nach Möglichkeit vermeiden. Der zahlreich vorgebrachten Kritik im Konsultationsverfahren wurde dahingehend Rechnung getragen, als mit der adaptierten Formulierung klargestellt wurde, dass der Betreiber eines 5G-Netzes sich mit der Thematik einer Vermeidung der Abhängigkeit von einem einzigen Lieferanten substantiiert auseinandersetzen muss.

Das Risikoprofil von Lieferanten kann auf Basis verschiedener Faktoren bewertet werden wie insbesondere der Wahrscheinlichkeit einer Einflussnahme aus Nicht-EU-Staaten, der Lieferfähigkeit des Lieferanten und der Gesamtqualität seiner Produkte und Sicherheitspraktiken.

Dies bedarf aus Sicht der RTR-GmbH jedoch einer gesonderten rechtlichen Grundlage. Zum Vorbringen im Konsultationsverfahren, dass allfällige Vorschriften im TKG zur Beurteilung des mit der Auswahl bestimmter Lieferanten verbundenen Risikos mit der Umsetzung anderer Vorgaben des EU-Instrumentariums in der gegenständlichen Verordnung aufeinander abgestimmt werden sollten, ist auszuführen, dass ein Inkrafttreten des neuen TKG nicht vor Ende 2020, eine Umsetzung des EU-Instrumentariums jedoch noch im Sommer dieses Jahres erwartet wird, was zusätzliche Abstimmungsprozesse nicht zulässt.

Abs. 4: Sicherheitsrelevante Komponenten, die bei Betrieb des 5G-Netzes eingesetzt werden, sind – gruppiert und nach Funktionen – in Anhang 2 angeführt. Zu den mit der Übermittlung einer Aufstellung der Funktionen gemäß Abs. 4 angeblich verbundenen Sicherheitsrisiken wird festgehalten, dass die Vorschrift aufgrund entsprechender Anmerkungen und Beanstandungen der Betreiber mehrfach grundlegend überarbeitet und in ihrer Eingriffsintensität deutlich abgeschwächt wurde. Mit der im Konsultationsverfahren erneut vorgebrachten Kritik werden nun tlw frühere Vorschläge wieder aufgegriffen, was nicht zielführend erscheint. Neben dem Umstand, dass der erhöhte Abstraktionsgrad durch bloße Angabe von Funktionen und Herstellern die Nutzbarkeit dieser Informationen für Außenstehende deutlich erschwert, wird festgehalten, dass die RTR-GmbH seit mehreren Jahrzehnten sensible Informationen der Betreiber verwaltet und über sämtliche erforderlichen Strukturen verfügt, mit denen nicht nur eine verschlüsselte Übermittlung der Informationen über das Einbringungsportal der Behörde, sondern auch eine sichere Speicherung der Informationen gewährleistet werden kann. Zu dem nun vorgebrachten Argument, dass die Übermittlung einer Gesamtliste zu Anfang und danach von entsprechenden Änderungen im Halbjahresabstand datenschutzfreundlicher sei, wird angemerkt, dass in früheren Gesprächen argumentiert wurde, dass die halbjährliche Erzeugung einer Gesamtliste im Vergleich zu einer Liste der Änderungen den geringeren Aufwand beim Betreiber erzeuge. Soweit im Konsultationsverfahren empfohlen wurde, die Hersteller mit der Übermittlung einer entsprechenden Liste zu befassen, wird darauf hingewiesen, dass Auskunftsrechte der Regulierungsbehörde im Zusammenhang mit der Sicherheit von Netzen und Diensten nur gegenüber Betreibern von Kommunikationsnetzen und Anbietern von Kommunikationsdiensten bestehen.