Załącznik nr 1 do OSR

Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G w Europie

Austria 2
Belgia 3
Bułgaria 3
Chorwacja 4
Cypr 4
Czechy 4
Dania 5
Estonia 6
Finlandia 7
Francja 8
Grecja 9
Hiszpania 9
Irlandia 10
Litwa 11
Luksemburg 12
Łotwa 12
Malta 13
Niderlandy 13
Niemcy 14
Portugalia 17
Rumunia 18
Słowacja 18
Słowenia 19
Szwecja 20
Wielka Brytania 21
Węgry 21
Włochy 21

Austria

W zakresie bezpieczeństwa sieci 5G kluczowym aktem prawnym jest austriackie rozporządzenie w sprawie bezpieczeństwa sieci[1)] z 2020 r. Zgodnie z nim na operatorów telekomunikacyjnych, posiadających ponad 100 000 abonentów, nałożono liczne obowiązki informacyjne, w tym obowiązek przedstawiania na uzasadnione żądanie organu regulacyjnego wykazu funkcji i producentów urządzeń wykorzystywanych do obsługi sieci 5G oraz, w stosownych przypadkach, innych komponentów przez nich wykorzystywanych.

Ponadto, muszą oni:

1) prowadzić Sieciowe Centra Operacyjne (NOC), jak również Centra Operacyjne Bezpieczeństwa (SOC) we własnych obiektach na terenie Unii Europejskiej;
2) skutecznie monitorować przez NOC/SOC wszystkie krytyczne elementy sieci 5G, w celu wykrywania anomalii oraz identyfikacji i zapobiegania zagrożeniom;
3) zarządzać ruchem sieciowym lub usługami komunikacyjnymi, w celu zapobiegania nieuprawnionym nieautoryzowanym zmianom w komponentach sieci lub usług;
4) zapewniać ochronę fizyczną krytycznych komponentów sieci i sieci 5G z zastosowaniem podejścia opartego na analizie ryzyka w przypadku wielodostępowych komputerów brzegowych (MEC) i stacji bazowych;
5) zapewnić, aby dostęp do sieci miał wyłącznie wykwalifikowany personel, który przeszedł kontrolę bezpieczeństwa, a dostęp osób trzecich był ograniczony i monitorowany;
6) stosować odpowiednie narzędzia i procesy w celu zapewnienia integralności oprogramowania, w szczególności aktualizować oprogramowanie oraz likwidować wykryte podatności;
7) posiadać strategię wielu dostawców uwzględniającą ograniczenia techniczne i wymogi interoperacyjności różnych części sieci 5G.

W załączniku do tego rozporządzenia została określona lista funkcji komponentów sieci 5G[2)].

Federalny Minister Rolnictwa, Regionów i Turystyki może ze względów bezpieczeństwa narodowego zakwalifikować, w drodze decyzji, producentów elementów sieci łączności elektronicznej lub dostawców usług dla takich sieci, w każdym przypadku, z wyjątkiem sieci nadawczych w rozumieniu federalnej ustawy o radiofonii i telewizji (BVG-Rundfunk), jako dostawców wysokiego ryzyka.

Taki dostawca jest wykluczony:

[1)] https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/TKNSiV-Text-BGBLA_2020_II_301.pdf .

[2)] https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/TKNSiV-Anhang2.pdf .

a) z dostaw składników istotnych dla bezpieczeństwa lub składników sieciowych dla sieci oraz

b) ze świadczenia usług związanych z bezpieczeństwem sieci.

Tego typu decyzja może obowiązywać maksymalnie 2 lata.

Prawo austriackie w zakresie czynników wpływających na uznanie za dostawcę wysokiego ryzyka nie odnosi się wprost do kwestii wpływu państw trzecich na dostawcę.

Belgia

11 marca 2022 r. opublikowano w Dzienniku Ustaw Belgii ustawę o zmianie niektórych przepisów dotyczących łączności elektronicznej w celu wprowadzenia dodatkowych środków bezpieczeństwa w odniesieniu do świadczenia usług telefonii komórkowej 5G[3)]. Przewidziano w niej procedurę autoryzacji dla sprzętu wykorzystywanego w sieci 5G. Wnioski w tym zakresie zgłasza się do ministra, który będzie wydawał decyzje przy autoryzacji.

Będą przy tym brane pod uwagę czynniki związane z dostawcą takie jak:

1) powiązania z rządami państw trzecich;
2) prawo lub sytuacja w kraju dostawcy, w szczególności w przypadku braku nadzoru demokratycznego lub legislacyjnego;
3) funkcjonowanie konwencji o ochronie danych lub bezpieczeństwa między Unią Europejską a danym państwem;
4) zdolność danego państwa do wywierania jakiejkolwiek formy nacisku, w tym w odniesieniu do miejsca produkcji sprzętu;
5) zdolność dostawcy do zabezpieczenia dostaw;
6) ogólna jakość produktów lub usług oraz praktyki bezpieczeństwa dostawcy, w tym stopień kontroli nad jego własnym łańcuchem dostaw oraz czy praktyki bezpieczeństwa są odpowiednio traktowane priorytetowo.

Bułgaria

Obecne przepisy prawa komunikacji elektronicznej w Bułgarii nakładają jedynie ogólny obowiązek zapewniania bezpieczeństwa sieci telekomunikacyjnych oraz szacowania ryzyka[4)]. Od 9 czerwca 2023 r. w Bułgarii obowiązuje akt określający minimalne wymagania w zakresie bezpieczeństwa publicznych sieci i usług łączności elektronicznej oraz sposobów zarządzania ryzykiem bezpieczeństwa[5)].Kwestie dostawcy wysokiego ryzyka są na razie na etapie

[3)] http://reflex.raadvst-consetat.be/reflex/pdf/Mbbs/2022/03/11/149027.pdf
[4)] https://www.lex.bg/laws/ldoc/2135553187.
[5)] https://crc.bg/files/Pravna/Pravila_minimalni_iziskvania.pdf

opracowywania przepisów w ramach planowanych zmian w prawie komunikacji elektronicznej. Proponowane zasady nie zostały jeszcze opublikowane.

Chorwacja

Na razie nie wprowadziła żadnych regulacji w zakresie HRV. Nie ujawniono też informacji o planowanej legislacji.

Cypr

Funkcjonuje tam regulacja dotycząca oceny ryzyka dostawców. Podstawą dla niej jest decyzja cypryjskiego organu ds. cyberbezpieczeństwa, która reguluje szczegóły związane z oceną ryzyka dostawców – przypomina ona rozporządzenie z naszego porządku prawnego[6)]. W ramach cypryjskiej ustawy o bezpieczeństwie sieci i systemów informacyjnych[7)] implementowano przepisy Europejskiego Kodeksu Łączności Elektronicznej dotyczące bezpieczeństwa sieci.

W ramach kryteriów branych pod uwagę przy ocenie dostawców są również czynniki strategiczne.

Czechy

Czechy regulują kwestię bezpieczeństwa sieci 5G i szerzej bezpieczeństwa łańcuchów dostaw w ramach ustawy o cyberbezpieczeństwie i zmianie ustaw powiązanych[8)]. Ustawa ta nakłada na operatorów telekomunikacyjnych oraz operatorów innych kluczowych usług ogólny obowiązek uwzględniania wymagań wynikających ze środków bezpieczeństwa przy wyborze dostawców dla ich systemów informacyjnych lub komunikacyjnych oraz do uwzględnienia tych wymagań w umowie, którą zawierają z dostawcą. Uwzględnianie wymogów wynikających ze środków bezpieczeństwa zgodnie ze zdaniem pierwszym w zakresie niezbędnym do spełnienia wymogów zgodnie z niniejszą ustawą nie jest uznawane za niezgodne z prawem ograniczenie konkurencji lub nieuzasadnioną barierę dla konkurencji.

W lutym 2022 roku czeski CSIRT wystosował rekomendacje dotyczące oceny wiarygodności dostawców technologii dla sieci 5G w Republice Czeskiej[9)]. Nie są one wiążące, ale podmioty, na które nałożone są ogólne obowiązki zapewniania cyberbezpieczeństwa, powinny brać je pod uwagę.

---

6) https://dsa.cy/images/pdf-upload/Decision-408-2020.pdf.
7) https://dsa.cy/images/pdf-upload/DSA-Law-89-I-2020.pdf.
8) https://nukib.cz/download/publications_en/legislation/EN_Decree-82-2018_v1.3_final.pdf.
9) https://nukib.cz/download/aktuality/5G-Recommendation_EN.pdf.

W tym dokumencie wskazane zostało, że na wiarygodność dostawców wpływają następujące czynniki:

1) rezydowanie lub podleganie prawu w demokratycznym państwie;
2) naruszanie prawa międzynarodowego, w szczególności jeśli zostały przeciwko nim skierowane rezolucje Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych lub restrykcyjne środki wspólnej polityki zagranicznej i bezpieczeństwa Unii Europejskiej;
3) prowadzenie działań sprzecznych z podstawowymi interesami Republiki Czeskiej lub jej państw sprzymierzonych;
4) nieznajdowanie się pod niewłaściwym wpływem obcego rządu lub organu administracji państwowej i możliwość zapewnienia dostępności, integralności i wiarygodności danych w dostarczanych rozwiązaniach technologicznych z odpowiednim stopniem autonomii;
5) spełnianie norm bezpieczeństwa, które są powszechne na rynku w momencie dostawy i jest skłonny zobowiązać się do ich spełniania w przyszłości;
6) prowadzenie działalności gospodarczej zgodnie z międzynarodowymi praktykami handlowymi oraz to, że nie czerpie nieproporcjonalnych korzyści od państwa, w którym zamieszkuje lub pod którego wpływy podlega.

Dania

Kwestie dostawcy wysokiego ryzyka zostały uregulowane w Ustawie o bezpieczeństwie dostawców w krytycznej infrastrukturze telekomunikacyjnej[10)]. Zgodnie z nią Centrum Cyberbezpieczeństwa może zakazać dostawcy publicznych usług telekomunikacyjnych zawarcia umowy lub nakazać odstąpienie od umowy, która stwarza zagrożenie dla bezpieczeństwa narodowego.

Przy ocenie czy umowa stwarza takie zagrożenie, Centrum bierze pod uwagę cechy kontrahenta takie, jak:

1) wpływ jego poddostawców i podmiotów mogących wywierać kontrolę na danego przedsiębiorcę;
2) pochodzenie z kraju, który nie ma zawartej umowy związanej z bezpieczeństwem z Danią, bądź nie gwarantuje współpracy w obszarze bezpieczeństwa;
3) bycie kontrolowanym, pośrednio lub bezpośrednio, przez obcy rząd;

[10)] https://www.retsinformation.dk/api/pdf/223450.

4) historia zaangażowania w działania w Danii lub innych krajach, które spowodowały zagrożenie dla bezpieczeństwa narodowego, bezpieczeństwa informacji lub porządku publicznego.

Centrum może nakazać ww. środki tylko, gdy bezpieczeństwa narodowego nie da się zapewnić w inny sposób. Decyzja Centrum może prowadzić do wywłaszczenia własności prywatnej za odszkodowaniem.

Taka decyzja może być zaskarżona do sądu. W ramach procesu sądowego powoływany jest specjalny adwokat, który ma mieć dostęp do dokumentów będących podstawą ww. decyzji. Te dokumenty nie są ujawniane bezpośrednio stronie. Jednakże minister obrony może wskazać, że niektóre dokumenty nie będą przedstawione temu specjalnemu przedstawicielowi.

Estonia

Estonia wprowadziła kwestie bezpieczeństwa sieci 5G do swojego porządku prawnego w ramach wdrażania Europejskiego Kodeksu Łączności Elektronicznej[11)]. Akt ten zobowiązuje operatorów telekomunikacyjnych do stosowania odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa swoim sieciom oraz do szacowania ryzyka w tym obszarze. Zgodnie z art. 87^3 sprzęt lub oprogramowanie używane w sieci telekomunikacyjnej nie może powodować zagrożenia dla bezpieczeństwa narodowego[12)]. Przy ocenie sprzętu lub oprogramowania wysokiego ryzyka bierze się pod uwagę m.in. informacje o tym czy:

1) lokalizacja lub siedziba znajduje się w państwie (dalej: państwo lokalizacji), które nie jest członkiem Unii Europejskiej, Organizacji Traktatu Północnoatlantyckiego (dalej: NATO) lub państwem członkowskim Organizacji Współpracy Gospodarczej i Rozwoju (dalej: OECD);
2) w państwie pochodzenia nie są przestrzegane zasady demokratycznego państwa prawa lub nie są przestrzegane prawa człowieka;
3) w państwie przyjmującym nie jest chroniona własność intelektualna, dane osobowe lub tajemnice handlowe osób z innego państwa;
4) państwo pochodzenia zachowuje się agresywnie w cyberprzestrzeni;
5) państwa członkowskie Unii Europejskiej, NATO lub OECD przypisały cyberataki państwu pochodzenia;

[11)] https://www.riigiteataja.ee/en/eli/501042015003/consolide.
[12)] riigiteataja.ee/akt/ESS.

6) podlega władzy rządowej lub państwowej państwa pochodzenia lub innego obcego państwa bez niezależnej kontroli sądowej;
7) państwo pochodzenia lub inne obce państwo może zobowiązać go do działania w sposób zagrażający bezpieczeństwu państwa estońskiego;
8) działalność gospodarcza nie jest oparta na konkurencji rynkowej lub w kraju pochodzenia nie stworzono do tego celu wystarczających warunków;
9) struktura własności, struktura organizacyjna lub struktura zarządzania nie jest przejrzysta;
10) finansowanie nie jest przejrzyste;
11) produkty lub usługi zawierają słabe punkty bezpieczeństwa i nie wdrożono odpowiednich środków bezpieczeństwa w celu ich wyeliminowania;
12) nie jest konsekwentnie w stanie zapewnić dostaw produktów lub usług, z wyjątkiem przypadków spowodowanych siłą wyższą.

Sprzęt, który zostanie uznany za stanowiący zagrożenie będzie mógł być wykorzystywany tylko po uzyskaniu zgody odpowiedniego organu. W przypadku obecnie wykorzystywanych urządzeń wprowadzono kilka kategorii sprzętu w zależności od jego funkcji. Danym kategoriom wyznaczono terminy w jakich mogą być użytkowane bez potrzeby uzyskania pozwolenia.

Przepisy te weszły w życie 3 września 2022 r.

Finlandia

Kluczowymi fińskimi aktami prawnymi w tym obszarze są Prawo Komunikacji Elektronicznej[13)] oraz Rozporządzenie Agencji Transportu i Komunikacji w sprawie krytycznych części sieci łączności[14)]. Rozporządzenie to zawiera listę funkcji krytycznych w sieci 5G. Z kolei Prawo Komunikacji Elektronicznej przewiduje, że urządzenie sieci komunikacyjnej nie może być używane w krytycznych częściach publicznej sieci komunikacyjnej, jeżeli istnieją poważne podstawy do podejrzeń, że użycie urządzenia zagrażałoby bezpieczeństwu narodowemu lub obronie narodowej w taki sposób, że użycie to umożliwiłoby działania obcego wywiadu lub działania, które zakłóciłyby, sparaliżowały lub w inny sposób negatywnie wpłynęły na ważne interesy Finlandii, podstawowe funkcje społeczeństwa lub demokratyczny porządek społeczny. Agencja Transportu i Łączności może

[13)] https://www.finlex.fi/fi/laki/ajantasa/2014/20140917#O9L29P244a.
[14)] https://finlex.fi/data/normit/47015/Regulation_on_critical_parts_of_a_communications_network.pdf.

zobowiązać właściciela lub innego posiadacza sieci łączności do usunięcia urządzenia sieci łączności z krytycznych części jego sieci.

Powołana została również Rada doradcza ds. bezpieczeństwa sieci, w której zasiadają zarówno przedstawiciele administracji publicznej, jak i biznesu, która będzie prezentować rekomendacje organom rządowym.

Francja

1. W celu zagwarantowania bezpieczeństwa i obrony narodowej w ustawie „LOI n° 2019-810" wprowadza się przepis o wcześniejszej kontroli wszelkiej działalności polegającej na eksploatacji niektórych urządzeń radioelektrycznych w sieciach 5G. Operatorzy będą musieli składać wniosek o zezwolenie do premiera. Premier udzieli odpowiedzi w terminie dwóch miesięcy od dnia otrzymania pełnej dokumentacji wniosku.

Ustali, czy istnieje poważne ryzyko naruszenia interesów w obszarze obrony i bezpieczeństwa narodowego na podstawie kryteriów określonych w ustawie, a zwłaszcza w świetle gwarancji, jakie dają urządzenia co do integralności, bezpieczeństwa, dostępności sieci lub poufności przekazywanych wiadomości i informacji powiązanych z komunikacją.

W razie niespełniania jednego z tych kryteriów wniosek o zezwolenie może zostać odrzucony przez premiera. Aby ocenić ryzyko, uwzględnia się zasady budowy i eksploatacji wprowadzone przez operatora, poziom bezpieczeństwa urządzenia i fakt, czy operator lub jego usługodawcy, w tym podwykonawcy, podlegają lub nie podlegają kontroli lub ingerencji państwa niebędącego członkiem Unii Europejskiej.

2. Budowa sieci 5G zwiększa ryzyko w obszarze cyberbezpieczeństwa związane z urządzeniami sieci ze względu na:

(1) szczególny charakter techniczny sieci 5G (dynamiczne zarządzanie siecią dostępu, wprowadzenie jednostek przetwarzania informacji na końcówkach sieci – edge computing), oraz

(2) przypadki używania sieci 5G w dziedzinach przemysłowych, w niektórych gałęziach o znaczeniu krytycznym (np. pojazd podłączony / pojazd autonomiczny, przemysł przyszłości, sieć elektroenergetyczna itp.).

To zwiększone ryzyko wpływa na nowe wymogi w obszarze bezpieczeństwa w odniesieniu do urządzeń, które będą wspierać przyszłe sieci 5G, dotyczące zarówno ich cech technicznych, jak i zobowiązań prawnych, które mogą zmuszać dostawców do współpracy z obcymi organami w gromadzeniu informacji.

Mając na uwadze te nowe obawy dotyczące bezpieczeństwa i najnowsze zmiany w planach budowy sieci 5G niektórych francuskich operatorów telekomunikacyjnych, które mogą zagrażać bezpieczeństwu narodowemu Francji, przyjęto ustawę o bezpieczeństwie sieci. Celem jest ustanowienie wcześniejszego systemu zezwoleń na urządzenia sieci radioelektrycznych.
Przepisy francuskie wpisują się również w skoordynowane działania na szczeblu Unii Europejskiej zainicjowane przez Komisję Europejską.
Ustawa ta zapewnia ochronę ruchomych sieci radiowych przed zagrożeniami szpiegostwa, piractwa i sabotażu.

Grecja

Obecnie prowadzone są prace nad ustawą w tym zakresie. Wciąż nie zostały określone szczegóły związane z HRV.

Hiszpania

Od 31 marca 2022 r. obowiązuje w Hiszpanii dekret królewski z mocą ustawy w sprawie wymogów mających na celu zagwarantowanie bezpieczeństwa sieci i usług łączności elektronicznej piątej generacji[15)]. Nakłada on na operatorów telekomunikacyjnych m.in. obowiązek szacowania i zarządzania ryzykiem w obszarze 5G oraz stosowania odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia sieci. Ustawa przewiduje, że rząd będzie mógł dokonywać oceny dostawców. Przy dokonywaniu takiej oceny mają być brane pod uwagę następujące czynniki:

1) powiązania dostawców i ich łańcucha dostaw z rządami państw trzecich;
2) skład kapitału zakładowego i struktura organów dostawcy;
3) uprawnienie państwa trzeciego do wywierania nacisku na wyniki lub lokalizację przedsiębiorstwa;
4) cechy reżimu politycznego państwa pochodzenia dostawcy i jego polityki w zakresie cyberbezpieczeństwa, takie jak:
   a) charakterystyka reżimu politycznego państwa trzeciego i jego polityki cyberbezpieczeństwa,
   b) umowy o współpracy w dziedzinie bezpieczeństwa, umowy o współpracy w zakresie cyberbezpieczeństwa, cyberprzestępczości lub ochrony danych podpisane z danym

[15)] BOE-A-2022-4973 Dekret królewski z mocą ustawy nr 7/2022 z dnia 29 marca 2022 r. w sprawie wymogów mających na celu zagwarantowanie bezpieczeństwa sieci i usług łączności elektronicznej piątej generacji.

państwem trzecim, jak również traktaty międzynarodowe dotyczące tych dziedzin, których stroną jest to państwo,

c) stopień zgodności jego przepisów o ochronie danych osobowych z przepisami unijnymi w tym zakresie.

Ustawa przewiduje trzy poziomy ryzyka jakie można przypisać dostawcy.

Szczegółowe obowiązki mają być nakładane na operatorów telekomunikacyjnych w drodze aktów wykonawczych (schematów bezpieczeństwa sieci i usług 5G), które szczegółowo będą określały środki techniczne i organizacyjne jakie będą musieli przyjąć. W takim schemacie może być nałożony obowiązek zmiany dostawcy oraz inne obowiązki związane z bezpieczeństwem łańcucha dostaw.

Irlandia

Dnia 2 marca 2023 r. uchwalona została ustawa Communications Regulation and Digital Hub Development Agency Act 2023[16)], która częściowo wdraża dyrektywę 2018/1972 ustanawiającą Europejski Kodeks Łączności Elektronicznej. Ustawa ma na celu zapewnienie, że podmioty udostępniające publiczne sieci łączności elektronicznej i podmioty świadczące publicznie dostępne usługi łączności elektronicznej będą podejmowały odpowiednie, proporcjonalne środki w celu zarządzania zagrożeniami dla bezpieczeństwa sieci i usług, w szczególności łańcuchów dostaw.

Ustawa wyposaża Ministra Środowiska, Klimatu i Komunikacji w uprawnienie do określania, czy dostawcę należy uznać za dostawcę wysokiego ryzyka. Minister może dokonać oceny czy dany dostawca kwalifikuje się do określenia go mianem dostawcy wysokiego ryzyka w każdym czasie. Bierze przy tym pod uwagę poniższe kryteria:

a) istnieje prawdopodobieństwo, że dostawca pozostaje pod wpływem państwa trzeciego,

b) istnieje znaczące ryzyko, że dostawca nie będzie w stanie zabezpieczyć dostaw krytycznych komponentów,

c) ogólna jakość krytycznych komponentów dostarczanych przez dostawcę jest nieodpowiednia

lub

d) praktyki w zakresie cyberbezpieczeństwa stosowane przez dostawcę są nieodpowiednie.

Określając prawdopodobieństwo dla pozostawania dostawcy pod wpływem państwa trzeciego Minister rozważa czy istnieje silny związek między dostawcą a rządem jakiegokolwiek państwa

[16)] https://data.oireachtas.ie/ie/oireachtas/act/2023/4/eng/enacted/a0423.pdf

trzeciego, stan praworządności i sytuację polityczną w danym państwie trzecim, w szczególności czy istnieje nadzór demokratyczny i legislacyjny, niezależne sądownictwo, umowy o ochronie danych lub bezpieczeństwie pomiędzy UE a danym państwem trzecim oraz czy państwo trzecie z którego pochodzi dostawca prowadzi ofensywną politykę politykę cyberbezpieczeństwa lub jest z nią powiązany. Minister bada również charakterystykę praktyk biznesowych dostawcy, w szczególności czy jego struktura i źródła finansowaniasą przejrzyste. Istotne znaczenie ma także zdolność danego państwa trzeciego do wywierania jakiejkolwiek formy nacisku na dostawcę, w tym w odniesieniu do wpływania na to, gdzie sprzęt się znajduje.

Minister może m.in. zakazać instalowania krytycznych komponentów wyprodukowanych lub dostarczonych przez dostawcę wysokiego ryzyka, zakazać lub ograniczyć stosowanie tych komponentów, nałożyć konkretne warunki związane z instalacją lub używaniem tego rodzaju komponentów, wymagać usunięcia, wyłączenia lub modyfikacji krytycznych komponentów wyprodukowanych lub dostarczonych przez dostawcę wysokiego ryzyka. Usługodawca, który nie zastosuje się do postanowienia Ministra popełnia przestępstwo i podlega w związku z tym karze grzywny nieprzekraczającej 250 000 euro lub pozbawienia wolności nawet do 5 lat.

Litwa

Rząd lub upoważniony przez niego organ określa kryteria, zgodnie z którymi uznaje się, że przedsiębiorstwo świadczy usługi mobilne piątej generacji (5G) lub zarządza infrastrukturą niezbędną do świadczenia takich usług.

Na Litwie zobowiązanie do wyeliminowania niezaufanych dostawców oprogramowania i sprzętu z sieci 5G zostało ujęte jako jeden ze strategicznych celów nowego programu rządowego, zatwierdzonego w marcu 2021 r. 25 maja 2021 r. litewski parlament jasno zadeklarował, że Litwa nie chce należeć do technosfery kontrolowanej przez Chiny i wprowadził zmiany do istniejących ram prawnych, które umożliwiają rządowi uniemożliwienie udziału nierzetelnych dostawców w rynku komunikacji elektronicznej. Jednym z głównych kryteriów przy definiowaniu zaufanego producenta jest to, czy jest on (lub jego beneficjent) zarejestrowany w kraju NATO, Unii Europejskiej lub EOG i/lub Organizacji Współpracy Gospodarczej i Rozwoju (OECD). Kryterium to dotyczy firmy telekomunikacyjnej, dostawcy sprzętu oraz dostawcy usług utrzymania sprzętu, co oznacza, że na rynku komunikacji elektronicznej nie mogą uczestniczyć tzw. firmy z krajów trzecich.

Litewskie Narodowe Centrum Cyberbezpieczeństwa[17)] (NCSC) będzie odgrywać główną rolę w procesie weryfikacji zaufania do urządzeń, gdzie jedną z funkcji NCSC jest zapewnienie oceny bezpieczeństwa cybernetycznego konkretnych urządzeń i aplikacji w oparciu o potrzeby sektora prywatnego i publicznego. Między innymi na podstawie jego opinii litewski rząd będzie mógł wydać decyzję stwierdzającą, że inwestor stanowi potencjalne zagrożenie dla bezpieczeństwa narodowego. W przypadku wydania takiej decyzji inwestor nie może zawierać decyzji dotyczących obszarów, w których stanowi to zagrożenia do czasu aż ustanie powód, dla którego uznano go za zagrożenie. Decyzje w tej sprawie podejmuje Komisja Bezpieczeństwa Narodowego, w której skład wchodzą przedstawiciele administracji oraz służb specjalnych.

Ww. środki mogą być przedsięwzięte wobec producentów i dostawców sprzętu komputerowego, urządzeń lub oprogramowania wykorzystywanego w działalności związanej z łącznością elektroniczną i/lub dostawcy usług konserwacyjnych lub pomocniczych.

Luksemburg

Luksemburg nie zdefiniował w swoim prawie pojęcia dostawcy wysokiego ryzyka. Wprowadzone jednak zostały regulacje związane z ochroną sieci 5G w ramach ustawy implementującej Europejski Kodeks Łączności Elektronicznej[18)]. Zgodnie z tą ustawą w przypadku poważnego zagrożenia dla bezpieczeństwa sieci i usług, wpływającego na bezpieczeństwo narodowe, które jest spowodowane wykorzystywanym sprzętem lub oprogramowaniem, na wniosek ministra właściwego do spraw komunikacji elektronicznej i poczty, rząd może wprowadzić środki odnoszące się do tych urządzeń lub programów, w tym zakaz ich stosowania. W ustawie wpisano wprost, że zastosowanie tych środków nie rodzi uprawnień do jakichkolwiek roszczeń odszkodowawczych od rządu.

Powołany został również narodowy komitet telekomunikacji składający się z 20 przedstawicieli ministerstw i innych organów państw, który ma doradzać rządowi w zakresie środków opisanych powyżej.

Łotwa

Funkcjonują zasady związane z zawieraniem umów dotyczących systemów wysokiego ryzyka. Umowy ich dotyczące mogą zawierać tylko:

1) osoby prawne:

[17)] https://www.nksc.lt/en/.
[18)] https://legilux.public.lu/eli/etat/leg/loi/2021/12/17/a927/jo.

a) mające siedzibę w państwie członkowskim NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego,
b) których rzeczywisty właściciel jest obywatelem państwa członkowskiego NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego lub jest obywatelem Republiki Łotewskiej,
c) producentem oprogramowania lub sprzętu wykorzystywanego przez nich do świadczenia usługi jest osoba prawna mająca siedzibę w państwie członkowskim NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego lub osoba fizyczna będąca obywatelem Republiki Łotewskiej lub obywatelem państwa NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;

2) osoby fizyczne będące obywatelami Republiki Łotewskiej lub obywatelami państwa należącego do NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego.

Podmiot, który nie spełnia tych wymagań musi uzyskać zgodę organu odpowiedzialnego za bezpieczeństwo narodowe.

Malta

Malta stoi na stanowisku, że ryzyka związane z dostawcą wysokiego ryzyka, a zwłaszcza powiązane ze środkiem strategicznym SM03, nie stanowią realnego zagrożenia dla ich systemu. Na Malcie została wydana decyzja w sprawie przyznania częstotliwości[19)], zgodnie z którą operatorzy telekomunikacyjni muszą szacować ryzyko i stosować adekwatne środki. Nie ma tam jednak bezpośrednich odniesień do dostawcy wysokiego ryzyka.

Niderlandy

W Niderlandach funkcjonuje kategoria dostawcy wysokiego ryzyka[20)]. Minister Sprawiedliwości i Bezpieczeństwa, nałoży na dostawcę publicznej sieci lub usługi łączności elektronicznej obowiązek wyłącznego korzystania, w wyznaczonych częściach jego sieci lub urządzeń towarzyszących, z produktów lub usług podmiotów innych niż podmiot wyznaczony przez Ministra.

Dostawcą Wysokiego Ryzyka jest podmiot, który:

[19)] https://www.mca.org.mt/sites/default/files/Assignment%20process%20for%20additional%20spectrum%20for%20wireless%20broadband%20electronic%20communications%20service.pdf .
[20)] https://wetten.overheid.nl/BWBR0042843/2020-03-01.

a) jest państwem, podmiotem lub osobą, o której wiadomo lub co do której istnieją podstawy do podejrzeń, że zamierza ona niewłaściwie korzystać z sieci łączności elektronicznej lub usług oferowanych w Niderlandach lub zakłócać ich działanie, lub
b) ma bliskie powiązania z państwem, podmiotem lub osobą, o których mowa w lit. a, lub jest podmiotem lub osobą, co do których istnieją podstawy do podejrzeń, że mają takie powiązania lub wpływ.
W przypadku, gdy produkty danego dostawcy są już wykorzystywane w funkcjonujących sieciach, minister wyznaczy termin na ich wymianę biorąc pod uwagę konieczność zapewnienia ciągłości świadczenia usług.

Niemcy

W Niemczech zaprezentowano aktualizację modelu dotyczącego cyberbezpieczeństwa z uwzględnieniem funkcjonowania sieci 5G. Podstawowe zasady funkcjonowania systemu zostały przedstawione w kwietniu 2020 r. w opracowaniu zatytułowanym „Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG)”[21)]. Publikację przygotowały podmioty zajmujące się cyberbezpieczeństwem oraz rynkiem telekomunikacyjnym, w tym m.in. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn.
Wśród uwzględnionych kwestii wskazano np.: katalog wymagań z zakresu cyberbezpieczeństwa, składniki infrastruktury telekomunikacyjnej dla 5G, komponenty systemu odpowiedzialne za realizację funkcji krytycznych, a także stworzono listę funkcji krytycznych odnoszących się m.in. do infrastruktury zapewniającej przekazywanie i przechwytywanie danych telekomunikacyjnych. Wiele uwagi poświęcono również procesowi certyfikacji gwarantującej, że dany komponent systemu spełnia określone wymagania z zakresu bezpieczeństwa, odwołując się w tym przypadku do obowiązujących już przepisów Unii Europejskiej oraz regulacji niemieckich. Ważnym aspektem jest ponadto wprowadzenie zasad odnoszących się bezpośrednio do dostawców, takich jak choćby ich różnorodność, wiarygodność, weryfikacja technologiczna czy zobowiązanie do wczesnego informowania o nowych produktach i usługach.

[21)] https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf?__blob=publicationFile&v=6 .

1. Nowe regulacje bezpieczeństwa zostały opublikowane przez niemiecki urząd Bundesnetzagentur (BNetzA), regulujący funkcjonowanie sektora telekomunikacyjnego. Według serwisu Tech Radar wprowadzają one dodatkowe wymagania wobec wszystkich firm, które będą chciały brać udział w budowie niemieckiej sieci łączności 5G. Według nowych przepisów producenci sprzętu zobowiązani są do certyfikowania krytycznych komponentów zgodnie z wymogami bezpieczeństwa ustalanymi przez niemieckie organy państwowe. Zobowiązani są również do zatrudniania w obszarach związanych z bezpieczeństwem jedynie kwalifikowanych pracowników, a także do ciągłego monitorowania procedur bezpieczeństwa. Niemiecka administracja wezwała również działające w kraju firmy telekomunikacyjne do dywersyfikacji dostawców sprzętu i „unikania monokultury".
2. Niemiecki rząd uchwalił projekt nowej ustawy dotyczącej bezpieczeństwa informatycznego. Ma ona umożliwić dokładne sprawdzenie wiarygodności dostawców komponentów dla systemów infrastrukturalnych o krytycznym znaczeniu, takich jak sieć 5G. Kwestia ta była przedmiotem ożywionych publicznych dyskusji w związku z ewentualnym uczestnictwem chińskich koncernów w budowaniu niemieckiej sieci 5G. W ustawie tej chodzi zdecydowanie o zagadnienia bezpieczeństwa informatycznego, a nie o poszczególnych producentów.

Zgodnie z brzmieniem ustawy producenci mają składać oświadczenia, w których będą musieli między innymi zadeklarować, czy i jak mogą zapewnić, by komponenty o krytycznym znaczeniu nie posiadały żadnych technicznych właściwości pozwalających na ich nadużywanie – „w szczególności na potrzeby sabotażu, szpiegowania lub terroryzmu poprzez wpływanie na bezpieczeństwo, integralność, dostępność lub zdolność funkcjonowania krytycznie ważnej infrastruktury". Minimalne wymogi bezpieczeństwa, jakie ma spełniać producent, określi federalne ministerstwo spraw wewnętrznych.

Gdyby okazał się on nie w pełni wiarygodny, na przykład nie zgłaszając użytkownikowi znanych sobie niedociągnięć systemu, będzie mu można wymówić współpracę. W razie utrzymującego się braku dowodów wiarygodności resortowi spraw wewnętrznych wolno będzie w porozumieniu z innymi zainteresowanymi ministerstwami zabronić dalszego użytkowania wszystkich pochodzących od tego producenta komponentów.

Projekt ustawy zawiera również nakaz zgłaszania przez zarządców krytycznej infrastruktury kierowanych przeciwko niej cyberataków. Wprowadza ponadto jednolitą formę wystawianych przez Federalny Urząd Bezpieczeństwa Techniki Informacyjnej (BSI) certyfikatów

bezpieczeństwa dla sprzętu - https://cyberdefence24.pl/polityka-i-prawo/niemcy-wzmacniaja-cyberbezpieczenstwo

3. W Niemczech Federalna Agencja ds. Sieci (Bundesnetzagentur – BnetzA) określiła bardzo konkretny katalog wymagań w zakresie bezpieczeństwa. Według zaostrzonych kryteriów, w szczególności pod lupę będą brane te elementy infrastruktury, które realizują tzw. funkcje krytyczne. Będą one musiały przejść przez proces certyfikacji, tj. po przeprowadzeniu odpowiedniej procedury technicznej zdobyć świadectwo, że dany komponent spełnia wymagania w zakresie bezpieczeństwa –https://biznes.interia.pl/gospodarka/news-bezpieczenstwo-sieci-5g-kluczowe-dla-funkcjonowania-panstwa,nId,4732854#utm_source=paste&utm_medium=paste&utm_campaign=firefox.
4. 11 sierpnia 2020 r. Federalna Agencja ds. Sieci opublikowała aktualny projekt katalogu wymagań bezpieczeństwa dla obsługi systemów telekomunikacyjnych i przetwarzania danych oraz przetwarzania danych osobowych. Katalog został opracowany w porozumieniu z Federalnym Urzędem Bezpieczeństwa Informacji (BSI) oraz Federalnym Komisarzem ds. Ochrony Danych i Wolności Informacji (BfDI).

Katalog wymagań bezpieczeństwa dotyczy operatorów sieci telekomunikacyjnych i systemów przetwarzania danych oraz przetwarzania danych osobowych. Jest podstawą koncepcji bezpieczeństwa, uzgodnień technicznych i innych środków zwiększających bezpieczeństwo sieci i usług.

Katalog zawiera w szczególności krytyczne komponenty do certyfikacji:

1) deklaracje wiarygodności do uzyskania od producentów i dostawców systemów;
2) zapewnienie integralności produktu;
3) wprowadzenie monitoringu bezpieczeństwa;
4) zatrudnianie wyłącznie przeszkolonego i wykwalifikowanego personelu do pracy w obszarach związanych z bezpieczeństwem;
5) dostępność wystarczającej refundacji;
6) unikanie monokultur.

Katalog zawiera dodatkowe wymagania bezpieczeństwa dla publicznych sieci i usług telekomunikacyjnych o wysokim poziomie ryzyka. W związku z tym należy stworzyć listę funkcji krytycznych dla infrastruktur o wysokim poziomie ryzyka. Te krytyczne funkcje zostaną wymienione w dokumencie sporządzonym wspólnie z BSI.

W przyszłości lista funkcji krytycznych ma być stale aktualizowana i poprawiana. Uwzględniono i są brane pod uwagę wyniki międzynarodowych analiz, np. Agencji Unii

Europejskiej ds. Cyberbezpieczeństwa (ENISA) czy Organu Europejskich Regulatorów Łączności Elektronicznej (BEREC).

Następujące funkcje są uważane za krytyczne:

1) zarządzanie abonentami i mechanizmami kryptograficznymi (jeśli jest to element sieci);
2) interfejsy międzysieciowe;
3) zarządzane usługi sieciowe;
4) zarządzanie wirtualizacją funkcji sieciowych i orkiestracja sieci (MANO), a także wirtualizacja;
5) systemy zarządzania i inne systemy wsparcia;
6) kontrola transportu i przepływu informacji.

Portugalia

Portugalia wdrożyła przepisy Toolboxa 5G w ramach Prawa Komunikacji Elektronicznej z 16 sierpnia 2022 r.[22)] Nowe przepisy nałożyły na przedsiębiorców komunikacji elektronicznej obowiązki związane z obsługą incydentów jak również uregulowały postępowanie w sprawie potencjalnie niebezpiecznego sprzętu. Organy państwa mogą nałożyć na przedsiębiorców komunikacji elektronicznej dodatkowe obowiązki takie jak:

1) obowiązek stosowania produktów, usług i procesów certyfikowanych w ramach systemów certyfikacji cyberbezpieczeństwa, tj. na podstawie przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych;
2) obowiązek zapewnienia zgodności ze szczególnymi warunkami wirtualizacji funkcji sieciowych w zakresie eksploatacji i bezpieczeństwa sieci i usług;
3) obowiązek zapewnienia zgodności ze szczegółowymi warunkami podwykonawstwa funkcji w zakresie eksploatacji i bezpieczeństwa sieci i usług lub ich zakaz;
4) obowiązek przyjęcia strategii dywersyfikacji dostawców w zakresie eksploatacji i bezpieczeństwa sieci i usług;
5) obowiązek lokalizacji centrum operacyjnego sieci i centrum operacyjnego bezpieczeństwa na terytorium krajowym lub na terytorium państwa członkowskiego.

Ponadto, korzystanie z urządzeń w sieciach łączności elektronicznej może podlegać ocenie bezpieczeństwa, przeprowadzanej z inicjatywy dowolnego członka Komitetu Oceny Bezpieczeństwa. Ocenę tą przeprowadza ww. Komitet w którego skład wchodzą wysocy

[22)] https://diariodarepublica.pt/dr/detalhe/lei/16-2022-187481298

przedstawiciele administracji. W wyniku oceny bezpieczeństwa Komitet może nakazać wykluczenie, zastosowanie ograniczeń w użytkowaniu lub zaprzestanie użytkowania sprzętu lub usług i musi ustanowić, w stosownych przypadkach, rozsądny termin na dostosowanie się. Wydana została jedna decyzja w tym trybie dotycząca firmy Huawei[23)].

W ramach warunków aukcji 5G wskazano, że posiadacze nabytych częstotliwości będą podlegali obowiązkom wynikającym z implementacji Europejskiego Kodeksu Łączności Elektronicznej oraz Toolboxa 5G.

Rumunia

W Rumunii funkcjonuje ustawa nr 163/2021 o przyjęciu środków dotyczących infrastruktur informacyjnych i komunikacyjnych o znaczeniu krajowym oraz warunków wdrażania sieci 5G[24)]. Zgodnie z nią producent sprzętu, który miałby być wykorzystany do budowy sieci 5G musi uzyskać autoryzację w formie decyzji Premiera, wydanej na podstawie zgody Najwyższej Rady Obrony Narodowej. W procesie oceny dostawcy brane pod uwagą są uwagę kwestie, takie jak:

1) kontrola obcego rządu nad producentem przy braku niezależnego systemu prawnego;
2) brak przejrzystej struktury akcjonariatu producenta;
3) brak historii etycznego postępowania korporacyjnego producenta;
4) funkcjonowanie producenta w systemie prawnym, który nie narzuca przejrzystych praktyk korporacyjnych.

W Najwyższej Radzie Obrony Narodowej zasiadają przedstawiciele rządu, wojska oraz służb specjalnych[25)]. Decyzją nr 35 z dnia 21 lutego 2024 r. Rumunia odmówiła firmie Huawei zezwolenia na dostarczanie sprzętu do sieci 5G.

Słowacja

Słowacja nie posiada ściśle określonych zasad dotyczących bezpieczeństwa sieci 5G. W niektórych ustawach pojawiają się ogólne obowiązki związane z zarządzaniem bezpieczeństwem w łańcuchu dostaw.

Ponadto, przewidywana jest procedura oceny ryzyka dostawcy produktów do działań bezpośrednio związanych z eksploatacją sieci i systemów informatycznych dla operatora usługi

---

[23)] https://www.gns.gov.pt/docs/cas-1-2023.pdf
[24)] https://lege5.ro/gratuit/haydomrygy2q/legea-nr-163-2021-privind-adoptarea-unor-masuri-referitoare-la-infrastructuri-informatice-si-de-comunicatii-de-interes-national-si-conditiile-implementarii-retelelor-5g .
[25)] https://csat.presidency.ro/ro/prima-pagina/componenta-csat .

podstawowej (zwanego dalej „osobą trzecią”) na rzecz cyberbezpieczeństwa Republiki Słowackiej.

W 2020 r. podpisane zostało przez Słowację i USA memorandum[26)] dotyczące sieci 5G. podkreślają znaczenie zachęcania do udziału rzetelnych i godnych zaufania dostawców sprzętu sieciowego i oprogramowania na rynkach 5G, uwzględniania ocen profilu ryzyka oraz promowania ram, które skutecznie chronią sieci 5G przed nieautoryzowanym dostępem i zakłóceniami.

Wskazano, że w szczególności, oceny bezpieczeństwa powinny być staranne i kompletne oraz obejmować zwłaszcza następujące elementy:

1) czy dostawcy sprzętu sieciowego i oprogramowania podlegają kontroli ze strony obcego rządu;
2) czy dostawcy sprzętu sieciowego i oprogramowania mają przejrzyste struktury własności, partnerstwa i ładu korporacyjnego;
3) czy dostawcy sprzętu sieciowego i oprogramowania są zaangażowani w działalność innowacyjną i poszanowanie praw własności intelektualnej;
4) czy dostawcy sprzętu sieciowego i oprogramowania mają na koncie etyczne zachowania korporacyjne i podlegają systemowi prawnemu, który wymusza przejrzyste praktyki korporacyjne.

Słowenia

Przepisy rangi ustawowej dotyczące bezpieczeństwa sieci 5G nie zostały jeszcze wprowadzone. Zgodnie z projektem ustawy rząd będzie mógł zabronić stosowania urządzeń dostarczanych przez dostawcę wysokiego ryzyka w niektórych częściach sieci. Istniejące urządzenia HRV w tych częściach należy wymienić. Jego produkty będą mogły być również zakazane w niektórych innych obszarach takich jak infrastruktura krytyczna, systemy rządowe, obrona narodowa czy systemy ratownicze. Decyzja w sprawie HRV będzie miała charakter niejawny. Rząd, na podstawie opinii Rady Bezpieczeństwa Narodowego, będzie określać dostawców wysokiego ryzyka w drodze decyzji.

Będą przy tym brane pod uwagę następujące kryteria, z których będą musiały wystąpić przynajmniej trzy:

1) powiązanie dostawcy z rządem państwa trzeciego;

[26)] https://2017-2021.state.gov/united-states-slovak-republic-joint-declaration-on-5g-security/index.html .

2) ustawodawstwo państwa trzeciego, szczególnie w przypadku braku demokratycznej kontroli i trójpodziału władz, oraz zawarte umowy o bezpieczeństwie lub ochronie danych między UE a danym państwem trzecim;
3) cechy własności korporacyjnej dostawcy;
4) zdolność państwa trzeciego do wywierania jakiejkolwiek formy nacisku, w tym w odniesieniu do miejsca produkcji sprzętu;
5) zdolność dostawcy do zapewnienia dostaw;
6) ogólna jakość produktów i praktyk dostawcy w zakresie bezpieczeństwa cybernetycznego, w tym stopień kontroli nad własnym łańcuchem dostaw oraz to, czy praktykom w zakresie bezpieczeństwa nadano odpowiedni priorytet.

Nie rzadziej jednak niż raz na dwa lata będzie przeprowadzany przegląd wydanych decyzji.

W tym momencie kwestia bezpieczeństwa sieci 5G jest regulowana przez rozporządzenie w sprawie środków ograniczających ryzyko dla sieci 5G, które zostało znowelizowane w 2023 r. Jego zapisy odnoszą się do kwestii związanych z dostawcą wysokiego ryzyka.

Szwecja

Szwedzkie prawo komunikacji elektronicznej zawiera jedynie ogólne obowiązki będące implementacją Europejskiego Kodeksu Łączności Elektronicznej[27]. Implementacja przepisów Toolboxa 5G nastąpiła poprzez określenie warunków aukcji sieci 5G.

W październiku 2020 r. szwedzki krajowy regulacyjny organ telekomunikacyjny (PTS) nałożył następujące warunki udziału w aukcji widma 5G:

1) nowe instalacje i wdrożenie funkcji centralnych dla radia w pasmach częstotliwości nie mogą korzystać z produktów pochodzących od chińskich sprzedawców;
   oraz
2) wszelka istniejąca infrastruktura pochodząca od takich dostawców musi zostać wycofana najpóźniej do 1 stycznia 2025 r.

Ponadto w 2020 r., na podstawie ogólnych przepisów dotyczących aukcji 5G, wykluczył z udziału w aukcji firmę Huawei[28]. Zakaz został podtrzymany przez szwedzkie sądy.

[27] https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482#K8 .
[28] https://perma.cc/645J-YLKL

Wielka Brytania

Telecommunications (Security) Act 2021[29)] znowelizował *The Communications Act 2003*. Właściwy sekretarz stanu może wydać *„designated vendor directions”*, jeśli uważa, że są one niezbędne ze względu na interes bezpieczeństwa narodowego i jeśli nałożone przez ten środek wymagania są proporcjonalne. Do tych aktów muszą stosować się przedsiębiorcy telekomunikacyjni.

Designated vendor direction zawierają zakazy lub ograniczenia dotyczące używania produktów, usług dostarczanych przez dostawcę.

Designated vendor directions mają być przeglądane, co jakiś czas. Sekretarz stanu może wymagać od dostawców usług telekomunikacyjnych przygotowania i przedstawienia planu wdrożenia wymagań określonych w *designated vendor directions*.

Dostawca zostaje określony w *designation notice*. Przy wydawaniu tego aktu sekretarz stanu bierze pod uwagę zarówno czynniki techniczne (jakość, niezawodność, bezpieczeństwo produktów), jak i nietechniczne (związki między dostawcą a krajem pochodzenia, tożsamość osób uczestniczących w rozwoju lub produkcji produktów).

Węgry

Węgry nie wprowadziły przepisów związanych z dostawcą wysokiego ryzyka. Art. 156 ich Prawa telekomunikacyjnego[30)] nakłada na operatorów telekomunikacyjnych ogólne obowiązki związane z zapewnianiem bezpieczeństwa, nie odnosi się jednak do kwestii bezpieczeństwa łańcucha dostaw czy oceny wysokiego ryzyka.

W tym obszarze funkcjonuje jeszcze rozporządzenie 41/2015 Ministra Spraw Wewnętrznych, które wprowadza ogólne wymogi bezpieczeństwa informacji dla podmiotów węgierskiego systemu cyberbezpieczeństwa[31)].

Włochy

Włochy implementowały przepisy Toolboxa 5G w zakresie dostawcy wysokiego ryzyka poprzez zastosowanie do operatorów w tej sieci zasad zawartych w ustawie z 15 marca 2012 r. o specjalnych uprawnień dotyczących struktur korporacyjnych w sektorach obronności i bezpieczeństwa narodowego, a także dla działalności o znaczeniu strategicznym w sektorach energii, transportu i komunikacji[32)]. Do 2022 r. środki z tej ustawy, takie jak możliwość

[29)] Telecommunications (Security) Act 2021 chapter 31 https://www.legislation.gov.uk/ukpga/2021/31/enacted .
[30)] https://net.jogtar.hu/jogszabaly?docid=a0300100.tv .
[31)] https://njt.hu/jogszabaly/2015-41-20-0A .
[32)] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2012-03-15;21 .

zablokowania zawarcia umowy bądź nałożenia określonych obowiązków, miały zastosowanie do umów z podmiotami spoza UE dotyczących:

1) zakupu towarów i usług związanych z projektowaniem, wdrażaniem, utrzymaniem i obsługą sieci 5G; i/lub
2) nabycia powiązanych komponentów zaawansowanych technologicznie.

Ustawa nakłada obowiązek notyfikacji takich transakcji. Krajowy Urząd Oceny i Certyfikacji (Centro di valutazione e certificazione nazionale – CVCN) ocenia ewentualne czynniki podatności, które mogłyby zagrozić integralności i bezpieczeństwu sieci 5G i przesyłanych danych poprzez wstępne dochodzenie[33)].

W 2022 r. Włochy rozszerzyły tę regulację także na te dotyczące cyberbezpieczeństwa i usługi chmurowe, które zostaną wskazane szczegółowo w aktach wykonawczych. Zmieniono także procedurę, wprowadzając że obowiązek zgłoszenie nie dotyczy już zamiaru zawarcia konkretnej umowy z dostawcą spoza UE na dostawę towarów lub usług ale, rocznego planu dotyczącego zamiaru zakupu przez cały rok, od dowolnego dostawcy (niezależnie od jego narodowości), towarów lub usług związanych z danymi usługami. Realizacja planu następuje po otrzymaniu zezwolenia. W ramach postepowania administracja może proponować wprowadzenia określonych zmian w planie.

[33)] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2019-09-21;105.