EUROPEAN COMMISSION
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

Numer powiadomienia : 2023/0761/ES (Spain)

DEKRET KRÓLEWSKI ZATWIERDZAJĄCY KRAJOWY SYSTEM BEZPIECZEŃSTWA SIECI I USŁUG 5G

Data otrzymania : 29/12/2023
Koniec zawieszenia : 02/04/2024 (closed)

Message

Wiadomość 001

Informacja od Komisji - TRIS/(2023) 3739

dyrektywa (UE) 2015/1535

Powiadomienie: 2023/0761/ES

Powiadomienie o projekcie tekstu przez państwo członkowskie

Notification – Notification – Notifzierung – Нотификация – Oznámení – Notifikation – Γνωστοποίηση – Notificación – Teavitamine – Ilmoitus – Obavijest – Bejelentés – Notifica – Pranešimas – Paziņojums – Notifika – Kennisgeving – Zawiadomienie – Notificação – Notificare – Oznámenie – Obvestilo – Anmälan – Fógra a thabhairt

Does not open the delays - N'ouvre pas de délai - Kein Fristbeginn - Не се предвижда период на прекъсване - Nezahajuje prodlení - Fristerne indledes ikke - Καμμία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késéseket - Non fa decorrere la mora - Atidėjimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħx il-perijodi ta’ dewmien - Geen termijnbegin - Nie otwiera opóźnień - Não inicia o prazo - Nu deschide perioadele de stagnare - Nezačína oneskorenia - Ne uvaja zamud - Inleder ingen frist - Ní osclaíonn sé na moilleanna

MSG: 20233739.PL

1. MSG 001 IND 2023 0761 ES PL 29-12-2023 ES NOTIF

2. Spain

3A. Subdirección de Asuntos Industriales, Energéticos, de Transportes, Comunicaciones y de Medioambiente
D.G. de Mercado Interior y otras Políticas Comunitarias
Ministerio de Asuntos Exteriores, UE y Cooperación

3B. Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
Secretaría General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual.
Subdirección General de Ordenación de las Telecomunicaciones.
Ministerio de Transformación Digital

4. 2023/0761/ES - V00T - Telekomunikacja

5. DEKRET KRÓLEWSKI ZATWIERDZAJĄCY KRAJOWY SYSTEM BEZPIECZEŃSTWA SIECI I USŁUG 5G

6. Sieci i usługi łączności elektronicznej 5G

Sprzęt telekomunikacyjny.

7.

8. Rozporządzenie składa się z części wyjaśniającej, jednego artykułu zatwierdzającego ENS5G (krajowy system bezpieczeństwa sieci 5G), dwóch dodatkowych przepisów i czterech przepisów końcowych.
ENS5G, który ma zostać zatwierdzony, składa się z 33 artykułów podzielonych na osiem rozdziałów oraz trzech załączników.
W uzasadnieniu wyjaśniono powody przyjęcia rozporządzenia oraz opracowywane artykuły dekretu królewskiego z mocą ustawy.
W jednym artykule zatwierdzono krajowy system bezpieczeństwa sieci i usług 5G.
Pierwszy przepis dodatkowy stanowi, że rząd, w drodze dekretu królewskiego, na wniosek Ministerstwa Transformacji Cyfrowej, w następstwie sprawozdania Rady Bezpieczeństwa Narodowego, dokonuje przeglądu krajowego systemu bezpieczeństwa sieci i usług 5G, gdy wymagają tego okoliczności, a w każdym razie co cztery lata.
Drugi przepis dodatkowy stanowi, że dekret królewski z mocą ustawy 7/2022 z dnia 29 marca 2022 r. i ENS5G mają zastosowanie do generacji łączności elektronicznej wykraczających poza piątą generację, podczas gdy nie ma w odniesieniu do nich szczegółowych rozporządzeń.
Pierwszy przepis końcowy dotyczący jurysdykcji stanowi, że dekret królewski i zatwierdzony przez niego system są wydawane na podstawie art. 149 ust. 1 pkt 21 i art. 149 ust. 1 pkt 29 Konstytucji Hiszpańskiej, które przyznają państwu, odpowiednio, wyłączną jurysdykcję nad ogólnym systemem telekomunikacyjnym i bezpieczeństwem publicznym.
Drugi przepis końcowy stwierdza, że ustawa 11/2022 z dnia 28 czerwca 2022 r. w sprawie ogólnej telekomunikacji oraz jej przepisy wykonawcze mają zastosowanie uzupełniające, i stanowi, że we wszystkich sprawach nieuregulowanych we wspomnianych przepisach dekret królewski z mocą ustawy 12/2018 z dnia 7 września 2018 r. w sprawie bezpieczeństwa sieci i systemów informatycznych oraz ustawa 8/2011 z dnia 28 kwietnia 2011 r. ustanawiająca środki ochrony infrastruktury krytycznej, jak również ich odpowiednie przepisy wykonawcze, mają zastosowanie uzupełniające.
Trzeci przepis końcowy dotyczący rozwoju regulacyjnego umożliwia szefowi Ministerstwa Transformacji Cyfrowej opracowanie przepisów niniejszego dekretu królewskiego i zatwierdzonego przez nie systemu, a także zmianę treści załączników zgodnie z rozwojem postępu technologicznego, zatwierdzenie nowych standardów technicznych i systemów certyfikacji sprzętu telekomunikacyjnego i produktów podłączonych do sieci oraz rozwój różnych konfiguracji i parametrów technicznych sieci i usług 5G oraz przyszłych generacji łączności elektronicznej.
Czwarty przepis końcowy stanowi, że rozporządzenie wchodzi w życie następnego dnia po jego opublikowaniu w Dzienniku Urzędowym.
W odniesieniu do zatwierdzonej treści ENS5G:
Artykuł 1 stanowi, że rozporządzenie jest wydawane w celu wykonania dekretu królewskiego z mocą ustawy 7/2022 z dnia 29 marca 2022 r., w szczególności w zastosowaniu jego rozdziału IV.
Artykuł 2 odnosi się do celów rozporządzenia, które zostały już przeanalizowane.
Artykuł 3 stanowi, że stosuje się definicje zawarte w dekrecie królewskim z mocą ustawy 7/2022 z dnia 29 marca 2022 r., ustawie 11/2022 z dnia 28 czerwca 2022 r. w sprawie ogólnej telekomunikacji i Europejskim kodeksie łączności elektronicznej.
Artykuł 4 stanowi, że rozporządzenie ma zastosowanie do operatorów sieci 5G, dostawców 5G i użytkowników korporacyjnych sieci 5G, którzy mają prawo do korzystania z publicznej domeny radiowej do instalowania, wdrażania lub obsługi prywatnej sieci 5G lub do świadczenia usług 5G do celów zawodowych lub na własny użytek.
Artykuł 5 określa minimalne elementy, infrastrukturę i zasoby, które tworzą sieć łączności elektronicznej 5G, odwołując się do załącznika I w celu ich szczegółowego opisu. Określa również krytyczne elementy sieci 5G, które co do zasady muszą znajdować się na terytorium kraju (w tym ewentualne wyjątki).
Artykuł 6 odnosi się do kompleksowego traktowania bezpieczeństwa zgodnie z międzynarodowym prawodawstwem wspólnotowym i krajowym, które zostało zatwierdzone lub które może zostać zatwierdzone, wymagającym od stron zobowiązanych przeprowadzenia, za pomocą całościowej metody, analizy słabych punktów, zagrożeń i ryzyk, które dotyczą ich jako podmiotów gospodarczych oraz różnych komponentów, a także odpowiedniego i kompleksowego zarządzania tymi ryzykami za pomocą technik i środków, które są odpowiednie do ich ograniczenia lub wyeliminowania oraz do osiągnięcia ostatecznego celu, jakim jest bezpieczne użytkowanie i eksploatacja sieci i usług 5G.

Artykuł 7 podkreśla, że analiza ryzyka i zarządzanie ryzykiem są zasadniczym elementem procesu bezpieczeństwa i powinny być działaniami bieżącymi, stale aktualizowanymi.
Artykuł 8 odnosi się do bieżącego monitorowania i okresowej ponownej oceny.
Artykuł 9 stanowi, że analiza ryzyka na szczeblu krajowym jest określona w załączniku II i została przeprowadzona z uwzględnieniem różnych elementów, takich jak informacje zebrane od stron zobowiązanych, badanie słabych punktów związanych z łańcuchem dostaw sieci i usług 5G, ocena stopnia zależności dostawców, ryzyko przerwania dostaw ze względu na sytuację gospodarczą, korporacyjną lub handlową wpływającą na dostawców lub ocena skuteczności stosowanych środków bezpieczeństwa.
Artykuł 10 dotyczący zarządzania ryzykiem na szczeblu krajowym stanowi, że kryteria, wymogi, warunki i terminy dla stron zobowiązanych do opracowania i wdrożenia technik i środków ograniczających ryzyko określono w załączniku III.
Artykuł 11 rozwija przepisy art. 14 dekretu królewskiego z mocą ustawy 7/2022 z dnia 29 marca 2022 r. w odniesieniu do procedury i aspektów, które mają zostać ocenione przez Radę Ministrów w odniesieniu do klasyfikacji dostawców jako dostawców wysokiego ryzyka oraz elementów, które należy uwzględnić przy zamawianiu ewentualnej wymiany sprzętu, produktów i usług świadczonych przez tych dostawców. Podobnie, zgodnie z przepisami wspomnianego dekretu królewskiego z mocą ustawy, stwierdza się, że dostawcy wysokiego ryzyka, których sprzęt telekomunikacyjny, urządzenia, oprogramowanie lub usługi pomocnicze są wykorzystywane tylko i wyłącznie w prywatnych sieciach 5G lub w celu świadczenia usług 5G na własny użytek, są klasyfikowani jako dostawcy średniego ryzyka.
Artykuł 12 dotyczący określania lokalizacji, w których nie można instalować urządzeń dostawców sklasyfikowanych jako dostawcy wysokiego ryzyka, stanowi, że Rada Bezpieczeństwa Narodowego, na podstawie sprawozdania Ministerstwa Transformacji Cyfrowej, może określić lokalizacje, obszary i ośrodki, w których nie można instalować urządzeń dostawców sklasyfikowanych jako dostawcy wysokiego ryzyka. W przypadku instalacji, modyfikacji lub adaptacji stacji radiowych zapewniających zasięg w tych lokalizacjach, obszarach i ośrodkach operatorzy sieci 5G muszą zwrócić się o zezwolenie do Ministerstwa Transformacji Cyfrowej.
Artykuł 13 zobowiązuje operatorów sieci 5G do opracowania strategii dywersyfikacji łańcucha dostaw oraz do posiadania w sieci dostępu urządzeń przesyłowych dostarczanych przez co najmniej dwóch różnych dostawców. Określono w nim również kryteria, które Rada Ministrów powinna uwzględnić w celu podjęcia decyzji, czy możliwe jest utrzymanie jednego dostawcy, jeżeli w wyniku fuzji liczba dostawców ulegnie zmniejszeniu. Ponadto określono w nim założenia i procedurę, dzięki której Ministerstwo Transformacji Cyfrowej może zmienić strategię dywersyfikacji łańcucha dostaw operatora sieci 5G.
Artykuł 14 skupia się na analizie ryzyka, która ma być przeprowadzona przez operatorów sieci 5G w odniesieniu do wszystkich elementów, infrastruktury i zasobów sieci wymienionych w załączniku I, wymienia czynniki, które należy uwzględnić i zobowiązuje operatorów do zebrania od swoich dostawców praktyk i środków w zakresie bezpieczeństwa przyjętych w odniesieniu do produktów i usług, które im dostarczali, a także do uwzględniania priorytetów i hierarchii ryzyk zgodnie z określonymi parametrami, które również są wymienione. Do dnia 1 października 2024 r. operatorzy sieci 5G muszą przedłożyć analizę ryzyka, a następnie co dwa lata.
Artykuł 15 dotyczący analizy ryzyka przeprowadzanej przez dostawców 5G wymaga analizy ryzyk związanych ze sprzętem telekomunikacyjnym, urządzeniami i oprogramowaniem oraz usługami pomocniczymi związanymi z funkcjonowaniem lub eksploatacją sieci 5G lub świadczeniem usług 5G, a także dostarczenia tej analizy ministerstwu na żądanie. W przypadku dostawców sklasyfikowanych jako dostawcy wysokiego lub średniego ryzyka analiza jest przedkładana w ciągu sześciu miesięcy od tej klasyfikacji, a następnie co dwa lata.
Artykuł 16 dotyczący analizy ryzyka przez użytkowników korporacyjnych sieci 5G wymaga, aby ta analiza ryzyka była przekazywana Ministerstwu Transformacji Cyfrowej, w przypadku gdy tacy użytkownicy są do tego zobowiązani.
Artykuł 17 pozwala Ministerstwu Transformacji Cyfrowej zbierać od stron zobowiązanych informacje niezbędne do przeprowadzenia analizy ryzyka oraz klasyfikuje nieudzielenie takich informacji w ciągu 15 dni roboczych jako poważne naruszenie. Informacje te uznaje się za poufne i nie mogą być wykorzystywane do celów innych niż realizacja celów i obowiązków określonych w dekrecie królewskim z mocą ustawy 7/2022 z dnia 29 marca 2022 r., w ENS5G oraz w aktach wydanych w celu wykonania obu przepisów.
Artykuł 18 stanowi, że ogólnym obowiązkiem wszystkich stron zobowiązanych jest zarządzanie ryzykiem związanym z bezpieczeństwem.
Artykuł 19 skupia się na zarządzaniu bezpieczeństwem przez operatorów sieci 5G, wymienia obowiązki wszystkich operatorów (takie jak przyjęcie planów i środków awaryjnych, zapewnienie zgodności z normami europejskimi lub specyfikacjami technicznymi i systemami certyfikacji, poddanie się audytowi bezpieczeństwa na własny koszt lub żądanie

przestrzegania norm bezpieczeństwa przez dostawców) oraz dodatkowe obowiązki operatorów, którzy posiadają lub eksploatują krytyczne elementy publicznej sieci 5G (takie jak zakazy korzystania z urządzeń od dostawców wysokiego ryzyka w krytycznych elementach sieci lub w niektórych lokalizacjach, obszarach i ośrodkach). Operatorzy sieci 5G muszą przedłożyć Ministerstwu Transformacji Cyfrowej opis środków technicznych i organizacyjnych opracowanych i wdrożonych w celu zarządzania ryzykiem i ograniczania go do dnia 1 października 2024 r., a następnie co dwa lata. Ponadto operatorzy sieci 5G, którzy są właścicielami lub eksploatują krytyczne elementy publicznej sieci 5G, muszą przedłożyć Ministerstwu Transformacji Cyfrowej strategię dywersyfikacji łańcucha dostaw do dnia 1 października 2024 r., a następnie za każdym razem, gdy podlega ona modyfikacjom. Informacje na temat stanu realizacji tej strategii muszą być przedkładane do dnia 1 października każdego roku.
Artykuł 20 dotyczący zarządzania bezpieczeństwem przez dostawców 5G zawiera wykaz obowiązków, w tym przeprowadzenie audytu bezpieczeństwa ich sprzętu, produktów i usług, dostarczanie informacji na temat możliwych ingerencji podmiotów trzecich w projektowanie, działanie i funkcjonowanie ich sprzętu, produktów i usług oraz współpracę z operatorami sieci 5G i użytkownikami korporacyjnymi sieci 5G poprzez dostarczanie informacji i poświadczanie zgodności z normami i certyfikatami. Dostawcy 5G muszą przygotować sprawozdanie na temat środków technicznych i organizacyjnych opracowanych i wdrożonych w celu zarządzania ryzykiem i ograniczania go, a także przedłożyć to sprawozdanie ministerstwu na żądanie. W przypadku dostawców sklasyfikowanych jako dostawcy wysokiego lub średniego ryzyka sprawozdanie przedkłada się w terminie sześciu miesięcy od tej klasyfikacji, a następnie co dwa lata.
Artykuł 21 dotyczący zarządzania bezpieczeństwem przez użytkowników korporacyjnych sieci 5G stanowi, że nie mogą oni wykorzystywać sprzętu telekomunikacyjnego, systemów przesyłowych, urządzeń przełączających lub routingowych oraz innych zasobów, które umożliwiają przesyłanie sygnałów, urządzeń, oprogramowania lub usług pomocniczych od dostawców sklasyfikowanych jako dostawcy średniego ryzyka w krytycznych elementach sieci. Ponadto użytkownicy muszą przedstawić Ministerstwu Transformacji Cyfrowej, na żądanie, opis środków technicznych i organizacyjnych opracowanych i wdrożonych w celu zarządzania ryzykiem i ograniczania go.
Artykuł 22 dotyczący zarządzania bezpieczeństwem przez administrację publiczną stanowi, że ze względu na bezpieczeństwo narodowe, przy instalowaniu, wdrażaniu i eksploatacji sieci 5G, zarówno publicznie dostępnych, jak i prywatnych, lub świadczenia usług 5G, zarówno publicznie dostępnych lub na własny użytek, administracja publiczna nie może korzystać ze sprzętu, produktów i usług dostarczanych przez dostawców wysokiego ryzyka lub dostawców średniego ryzyka.
Artykuł 23 stanowi, że zgodnie z obowiązkami określonymi w poprzednich artykułach strony zobowiązane uwzględniają i stosują przepisy ustanowione w dekrecie królewskim z mocą ustawy 7/2022 z dnia 29 marca 2022 r., w ENS5G oraz w aktach wydanych w celu wykonania obu przepisów.
Artykuł 24 pozwala Ministerstwu Transformacji Cyfrowej zbierać od stron zobowiązanych informacje niezbędne do zarządzania ryzykiem i klasyfikuje nieudzielenie takich informacji w ciągu 15 dni roboczych jako poważne naruszenie. Informacje te uznaje się za poufne i nie mogą być wykorzystywane do celów innych niż realizacja celów i obowiązków określonych w dekrecie królewskim z mocą ustawy 7/2022 z dnia 29 marca 2022 r., w ENS5G oraz w aktach wydanych w celu wykonania obu przepisów.
Artykuł 25 stanowi, że wszystkie strony zobowiązane, a także organy administracji publicznej, producenci, importerzy, dystrybutorzy oraz podmioty, które wprowadzają do obrotu i sprzedają urządzenia końcowe i urządzenia do podłączenia do sieci 5G i świadczenia usług 5G, muszą współpracować i przedkładać informacje wymagane do modyfikacji i wdrożenia ENS5G.
Artykuł 26 stanowi, że na mocy rozporządzenia szefa Ministerstwa Transformacji Cyfrowej korzystanie z określonego sprzętu, systemu, programu lub usługi może podlegać uprzedniej certyfikacji zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych lub zgodnie z systemami certyfikacji i normami technicznymi dotyczącymi certyfikacji urządzeń i produktów 5G, które mogą zostać zatwierdzone na szczeblu europejskim lub międzynarodowym.
Artykuł 27 stanowi, że rozporządzenie stosuje się bez uszczerbku dla inwestycji zagranicznych i prawa konkurencji.
Artykuł 28 dotyczący urządzeń końcowych stanowi, że produkcja, import, dystrybucja, wprowadzanie do obrotu i sprzedaż urządzeń końcowych i urządzeń do podłączenia do sieci 5G oraz świadczenia usług 5G uzależnione są od zgodności z wymogami bezpieczeństwa produktów cyfrowych i mającymi zastosowanie zasadniczymi wymogami związanymi z cyberbezpieczeństwem, przyjętymi zgodnie z prawodawstwem europejskim, w szczególności w odniesieniu

do ochrony danych osobowych, prywatności i ochrony przed nadużyciami finansowymi.
Artykuł 29 odnosi się do współpracy międzynarodowej, która ma być rozwijana przez Ministerstwo Transformacji Cyfrowej, w szczególności na szczeblu Unii Europejskiej.
Artykuł 30 odnosi się do kompetencji Ministerstwa Transformacji Cyfrowej w zakresie wdrażania ENS5G. Ministerstwo powinno koordynować działania z innymi organami odpowiedzialnymi za cyberbezpieczeństwo i infrastrukturę krytyczną, aby zapewnić spójne wdrażanie ENS5G.
Artykuł 31 określa uprawnienia w zakresie wdrażania ENS5G, które odpowiadają Ministerstwu Transformacji Cyfrowej, w tym na przykład opracowanie, specyfikację i doprecyzowanie treści ENS5G, przeprowadzanie audytów w celu weryfikacji i monitorowania przestrzegania nałożonych obowiązków oraz przyznawania pomocy publicznej.
Artykuł 32 przyznaje Ministerstwu Transformacji Cyfrowej wszystkie uprawnienia związane z funkcją kontrolną.
Artykuł 33 dotyczący systemu kar odnosi się do przepisów art. 30 i 31 dekretu królewskiego z mocą ustawy 7/2022 z dnia 29 marca 2022 r.
Załącznik I opisuje elementy, infrastrukturę i zasoby, które tworzą sieć 5G.
Załącznik II zawiera analizę ryzyka na szczeblu krajowym.
Załącznik III określa zarządzanie ryzykiem na szczeblu krajowym.

9. Komunikacja mobilna piątej generacji, czyli 5G, to nowy paradygmat łączności elektronicznej o dużym potencjale transformacyjnym z korzyścią dla społeczeństwa i gospodarki, ponieważ otwiera możliwość włączenia nowych funkcji, które będą miały duży wpływ, takich jak obliczenia sieciowe, i umożliwią tworzenie sieci wirtualnych, oferując niskie opóźnienia i świadcząc usługi o wysokiej wartości dodanej w obszarach takich jak medycyna, transport i energia.
W związku z tym zarówno Unia Europejska, jak i Hiszpania promują szybkie wdrażanie sieci 5G oraz realizację projektów wykazujących ich przydatność dla różnych sektorów poprzez świadczenie usług 5G.
Sieci i usługi 5G mają przewagę w zakresie bezpieczeństwa w porównaniu z poprzednimi generacjami. Jednakże wiążą się z nimi również określone ryzyka, wynikające na przykład z ich bardziej złożonej, otwartej i rozproszonej architektury sieci, a także z ich zdolności do przesyłania ogromnych ilości informacji i umożliwienia jednoczesnej interakcji wielu osób i rzeczy. Ich wzajemne powiązania z innymi sieciami oraz ponadnarodowy charakter wielu zagrożeń mają wpływ na ich bezpieczeństwo, a przewidywalne powszechne wykorzystanie tych sieci do podstawowych funkcji gospodarczych i społecznych zwiększy potencjalny wpływ incydentów związanych z bezpieczeństwem.
Te nowe szczególne ryzyka związane z bezpieczeństwem typowe dla komunikacji mobilnej 5G zostały uwzględnione w przepisach dekretu królewskiego z mocą ustawy 7/2022 z dnia 29 marca 2022 r. w sprawie wymogów mających zapewnić bezpieczeństwo sieci i usług łączności elektronicznej piątej generacji, który w pełni uwzględnia zalecenie Komisji Europejskiej (UE) 2019/534 z dnia 26 marca 2019 r. cyberbezpieczeństwo sieci 5G, a także zalecenia zawarte w komunikacie Komisji Europejskiej z dnia 29 stycznia 2020 r. bezpieczne wprowadzanie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi (COM/2020/50 final) skierowanym do państw członkowskich na temat stosowania tego zestawu narzędzi.
Wspomniany dekret królewski z mocą ustawy 7/2022 z dnia 29 marca 2022 r. przewiduje jego rozwój regulacyjny za pośrednictwem krajowego systemu bezpieczeństwa sieci i usług 5G (ENS5G).
Zgodnie z art. 5 ust. 3 wspomnianego dekretu królewskiego z mocą ustawy ENS5G prowadzi kompleksową analizę bezpieczeństwa sieci i usług 5G, biorąc pod uwagę wkład każdego podmiotu łańcucha wartości 5G, a także przepisy, zalecenia i standardy techniczne Unii Europejskiej, Międzynarodowego Związku Telekomunikacyjnego (ITU) i innych organizacji międzynarodowych, aby zagwarantować ostateczny cel, jakim jest bezpieczne użytkowanie i eksploatacja sieci i usług 5G w Hiszpanii.
Z kolei art. 20 dekretu królewskiego z mocą ustawy stanowi, że w celu zapewnienia nieprzerwanego i bezpiecznego funkcjonowania sieci i usług 5G ENS5G przeprowadza na szczeblu krajowym analizę ryzyka w zakresie bezpieczeństwa sieci i usług 5G oraz identyfikuje, określa i opracowuje środki mające na celu ograniczenie analizowanych ryzyk i zarządzanie nimi.
Wreszcie, zgodnie z art. 21 dekretu królewskiego z mocą ustawy ENS5G jest zatwierdzany przez rząd dekretem królewskim na wniosek Ministerstwa Transformacji Cyfrowej, na podstawie sprawozdania Rady Bezpieczeństwa Narodowego.
Niniejsze rozporządzenie zatwierdza ENS5G, rozwijając przepisy dekretu królewskiego z mocą ustawy 7/2022 z dnia 29 marca 2022 r. w sprawie wymogów mających zapewnić bezpieczeństwo sieci i usług łączności elektronicznej piątej generacji.

10. Odniesienia do tekstów podstawowych:

11. Nie

12.

13. Nie

14. Nie

15. Tak

16.
Aspekty TBT: Nie

Aspekty SPS: Nie

****
Komisja Europejska
Punkt kontaktowy Dyrektywa (UE) 2015/1535
e-mail: grow-dir2015-1535-central@ec.europa.eu