PROJEKT

Zgodnie z art. 116 ust. 6 ustawy o łączności elektronicznej (UL RS nr 130/22 i 18/23 – ZDU-1O) Agencja ds. Sieci i Usług Komunikacyjnych Republiki Słowenii, z uwzględnieniem procedury informacyjnej zgodnie z dyrektywą (UE) Parlamentu Europejskiego i Rady 2015/1535 z dnia 9 września 2015 r. ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1), wydaje następującą

USTAWĘ OGÓLNĄ
o dodatkowych wymogach i ograniczeniach bezpieczeństwa

Artykuł 1
(Treść ustawy ogólnej)

Niniejsza ustawa ogólna określa:

1. wytyczne dla operatorów sieci łączności ruchomej (zwanych dalej „operatorami"), którzy udostępniają te sieci podmiotom krytycznym będącym zarządcami infrastruktury krytycznej w innych obszarach regulacji infrastruktury krytycznej, jak określono w przepisach prawa regulujących obszar infrastruktury krytycznej (zwanym dalej „zarządcami infrastruktury krytycznej"), dostawcom usług kluczowych w rozumieniu przepisów prawa dotyczących bezpieczeństwa informacji (zwanym dalej „dostawcami usług kluczowych"), organom administracji państwowej określonym w przepisach prawa dotyczących bezpieczeństwa informacji (zwanym dalej „organami administracji państwowej") lub podmiotom odpowiedzialnym za kluczowe części systemu bezpieczeństwa kraju; oraz
2. krytyczne elementy sieci i związanych z nią systemów informatycznych wraz z ich funkcjami, o których mowa w art. 116 ust. 6 ustawy o łączności elektronicznej (UL RS nr 130/22 i 18/23 – ZDU-1O; zwanej dalej „Ustawą"), określonych w Załączniku stanowiącym integralną część niniejszej ustawy ogólnej i sporządzonego we współpracy z organem odpowiedzialnym za bezpieczeństwo informacji.

Artykuł 2
(Znaczenie terminów)

(1) Terminy użyte w niniejszej ustawie ogólnej mają następujące znaczenie:

1. Łańcuch dostaw oznacza cały system procesów, ludzi, organizacji i dystrybucji zaangażowany w projektowanie, produkcję, magazynowanie, dystrybucję i dostawy, a także w instalację i konserwację komponentów krytycznych elementów sieci zainstalowanych w sieci operatora lub u dostawcy usług w chmurze świadczącego takie usługi na rzecz operatora.

2. Krytyczne elementy sieci oznaczają elementy sieci, funkcje, usługi i wspierające systemy informatyczne w formie fizycznej, programowej lub zwirtualizowanej u operatora lub dostawcy usług w chmurze, które zostały wymienione w załączniku do niniejszej ustawy ogólnej.

3. Podmioty krytyczne oznaczają zarządców infrastruktury krytycznej w innych obszarach regulacji infrastruktury krytycznej określonych zgodnie z przepisami prawa regulującymi dziedzinę infrastruktury krytycznej, dostawców usług kluczowych określonych zgodnie z przepisami prawa regulującymi bezpieczeństwo informacji, organy administracji państwowej określone zgodnie z przepisami prawa dotyczącymi bezpieczeństwa informacji i podmioty odpowiedzialne za kluczowe części systemu bezpieczeństwa kraju.

(2) Pozostałe terminy użyte w niniejszej ustawie ogólnej mają takie samo znaczenie jak w Ustawie i w ustawie ogólnej o bezpieczeństwie sieci, usług i danych.

Artykuł 3
(Wytyczne ogólne)

(1) Operatorzy w łańcuchu dostaw komponentów krytycznych elementów sieci i usług wsparcia trzeciego poziomu w odniesieniu do tych komponentów uwzględniają przez cały cykl życia tychże komponentów co najmniej następujące wytyczne:

1. w przypadku indywidualnego producenta lub dostawcy oraz dostawcy usług wsparcia trzeciego stopnia realizowanych w oparciu o nawiązane z nimi stosunki i zawarte umowy, przeprowadzają oni ocenę ryzyka pod względem podaży i potencjalnego wpływu wywieranego przez osoby fizyczne lub prawne będące osobami trzecimi na podstawie prawa publicznego lub prywatnego (zwane dalej „osobami trzecimi”), kompatybilności ze sprzętem innych producentów, jakości i bezpieczeństwa produktów oraz potencjalnego negatywnego wpływu na funkcjonowanie usług operatora i podmiotów krytycznych,
2. zabezpieczenia muszą zostać wbudowane i wdrożone już na etapie projektu, a umowy muszą przewidywać terminy wyeliminowania dostrzeżonych luk w zabezpieczeniach,
3. kluczowe cechy zabezpieczeń (dostępność, poufność, integralność i autentyczność) muszą pozostawać zapewnione przez cały cykl ich użytkowania,
4. należy zagwarantować bezpieczeństwo i nieprzerwane dostawy oraz potwierdzić obsługę zabezpieczeń wysokiego poziomu zgodnie z normami uznanymi na szczeblu międzynarodowym (3GPP) i europejskimi normami technicznymi (ETSI),
5. realizacja wytycznych, o których mowa w pkt. 2 – 4 niniejszego ustępu, musi być możliwa do zweryfikowania na podstawie dokumentacji umownej zawartej z producentem lub dostawcą,
6. w odniesieniu do każdego producenta lub dostawcy należy również ocenić i uwzględnić ryzyko związane z prawami do korzystania z kluczowych technologii, które są niezbędne do produkcji i użytkowania sprzętu oraz ryzyko związane z dostarczaniem sprzętu, części zamiennych lub usług wsparcia trzeciego stopnia,
7. w przypadku stosowanych komponentów nie mogą istnieć żadne znane i nieusunięte luki krytyczne lub luki aktywnie wykorzystywane,
8. należy unikać korzystania z usług jednego producenta lub dostawcy, o ile jest to technicznie wykonalne i uzasadnione ekonomicznie, w celu zmniejszenia zależności i zwiększenia odporności w przypadku wystąpienia luk w zabezpieczeniach komponentów krytycznych, awarii sieci o charakterze katastrofalnym lub zagrożenia dla bezpieczeństwa sieci i usług podmiotów krytycznych ze strony zewnętrznych osób fizycznych lub prawnych podlegających prawu publicznemu lub prywatnemu.

(2) Dostarczając sprzęt, systemy i usługi informacyjno-komunikacyjne, operatorzy zobowiązani są w pełni przestrzegać wytycznych Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (zwanej dalej „ENISA") oraz obowiązujących przepisów Unii Europejskiej dotyczących podstawowych wymogów bezpieczeństwa przy zamawianiu bezpiecznych produktów i usług z zakresu technologii informacyjno-komunikacyjnych (ICT). Agencja publikuje na swojej stronie internetowej łącza do aktualnych dokumentów ENISA i przepisów UE dotyczących wyżej wymienionego obszaru i aktualizuje je.

(3) Przy dostarczaniu komponentów krytycznych elementów sieci lub korzystaniu z usług w chmurze pierwszeństwo ma wybór komponentów od tych producentów lub dostawców, albo usług od dostawców usług w chmurze, którzy zostali certyfikowani przez jednostki oceniające zgodność, które otrzymały akredytację i - w razie potrzeby - zezwolenie na podstawie art. 60 ust. 3 rozporządzenia 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 oraz uchylenia rozporządzenia (UE) nr 526/2013 (zwanego dalej „rozporządzeniem") w odniesieniu do wydawania europejskich certyfikatów cyberbezpieczeństwa na określonym poziomie uzasadnienia zaufania, jak przewidziano w art. 52 rozporządzenia.

(4) W celach przewidzianych w poprzedzającym ustępie operator sprawdza specjalną stronę internetową, prowadzoną przez ENISA zgodnie z art. 55 rozporządzenia, mającą na celu informowanie społeczeństwa o europejskich programach certyfikacji cyberbezpieczeństwa, europejskich certyfikatach cyberbezpieczeństwa i unijnych deklaracjach zgodności, z uwzględnieniem informacji o wycofanych europejskich programach certyfikacji cyberbezpieczeństwa lub o unieważnionych bądź wygasłych europejskich certyfikatach cyberbezpieczeństwa i unijnych deklaracjach zgodności, jak również repozytorium łączy do stron zawierających informacje dotyczące cyberbezpieczeństwa.

Artykuł 4
(Ocena ryzyka)

(1) Określając ryzyko producenta lub dostawcy komponentów oraz dostawcy usług trzeciego poziomu w odniesieniu do krytycznych elementów sieci, operator bierze pod uwagę wyszczególnione poniżej aspekty ryzyka, które poddaje ocenie.

(2) W ramach oceny, o której mowa w poprzednim ustępie, operator ocenia i uwzględnia co najmniej:

1. ogólną jakość (w tym aspekty bezpieczeństwa) i niezawodność,
2. poziom wykorzystania otwartych norm i interfejsów zapobiegających przywiązaniu i uzależnieniu od produktów danego producenta lub dostawcy,
3. zgodność z uznanymi międzynarodowymi i europejskimi normami technicznymi (3GPP, ETSI) oraz z przepisami Unii Europejskiej, jak również z domyślnymi ustawieniami bezpieczeństwa wg profesjonalnych zaleceń (Stowarzyszenie GSMA),
4. poziom kompatybilności z urządzeniami i funkcjami sieciowymi stron trzecich,
5. możliwość dostarczania aktualizacji i dostosowywania,
6. proces zarządzania lukami w zabezpieczeniach, ich ujawniania i bieżącego stosowania aktualizacji oraz poprawek,

7. dostępność i przejrzystość dokumentacji dotyczącej:
   - kluczowych funkcji i informacji dotyczących bezpieczeństwa oraz pozostałych cech komponentu i możliwych ustawień oraz
   - zastosowanego oprogramowania, w tym otwartego kodu źródłowego (zestawienie podstawowych materiałów do produkcji oprogramowania – SBOM),
8. poziom uzależnienia od usług wsparcia trzeciego stopnia w zakresie zarządzania i konserwacji sprzętu, jeżeli operator nie wykonuje tych usług samodzielnie, przy pomocy własnego personelu,
9. wstępną ocenę zgodności sprzętu lub podmiotu, który świadczyłby usługi wsparcia trzeciego stopnia przez jednostki akredytowane w Unii Europejskiej zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa, przy czym informacje o jednostkach akredytowanych są publikowane w Dzienniku Urzędowym Unii Europejskiej.

(3) Operator dokumentuje czynniki ryzyka i wyniki oceny ryzyka w odniesieniu do każdego wybranego producenta, dostawcy lub usługodawcy trzeciego szczebla, o którym mowa w ust. 2 i 3 niniejszego artykułu, i regularnie aktualizuje informacje zawarte w dokumentacji.

Artykuł 5
(Ogólne wytyczne dotyczące eksploatacji krytycznych elementów sieci)

(1) Komponenty krytycznych elementów sieci, ich eksploatacja i ustawienia domyślne nie mogą obejmować cech technicznych, które mogłyby negatywnie wpłynąć na bezpieczeństwo lub działanie podmiotów krytycznych, między innymi wskutek sabotażu, szpiegostwa, kradzieży własności intelektualnej lub terroryzmu.

(2) Krytyczne elementy sieci lokalizuje się zazwyczaj w Republice Słowenii lub - biorąc pod uwagę wszystkie zagrożenia dla bezpieczeństwa i przy zapewnieniu wysokiego poziomu środków bezpieczeństwa, a także o ile obowiązujące przepisy nie stanowią inaczej - na terytorium Unii Europejskiej. Operator informuje Agencję ds. Sieci i Usług Komunikacyjnych Republiki Słowenii (zwaną dalej „Agencją”) oraz organ odpowiedzialny za bezpieczeństwo informacji o planowanej relokacji na co najmniej 30 dni przed relokacją poza Unię Europejską.

(3) Usługi wsparcia trzeciego poziomu w odniesieniu do krytycznych elementów sieci świadczy się zasadniczo w Republice Słowenii lub - biorąc pod uwagę wszystkie zagrożenia dla bezpieczeństwa i przy zapewnieniu wysokiego poziomu środków bezpieczeństwa, a także o ile obowiązujące przepisy nie stanowią inaczej - na terytorium Unii Europejskiej. Operator powiadamia Agencję i organ odpowiedzialny za bezpieczeństwo informacji o planowanej relokacji swoich usług wsparcia trzeciego stopnia co najmniej 30 dni przed relokacją poza terytorium państw Unii Europejskiej.

(4) Wdrożenie usług wsparcia trzeciego stopnia nie może zagrażać bezpieczeństwu lub funkcjonowaniu usług podmiotów krytycznych albo bezpieczeństwu narodowemu.

(5) Operator ustanawia i regularnie realizuje proces identyfikacji krytycznych elementów sieci. Musi on być przeprowadzany co najmniej raz w roku lub gdy zamawiane są komponenty krytycznych elementów sieci.

(6) Jeżeli pojedynczy komponent tylko częściowo reprezentuje krytyczny element sieci, uznaje się go za część krytycznego elementu sieci.

(7) Operator prowadzi aktualny wykaz wszystkich komponentów krytycznych elementów sieci, ich funkcji, lokalizacji, administratorów i menedżerów, dostawców dotyczących ich usług wsparcia trzeciego szczebla oraz ich producentów lub dostawców. Wykaz udostępnia się na żądanie Agencji i organowi odpowiedzialnemu za bezpieczeństwo informacji.

Artykuł 6

(Środki bezpieczeństwa dotyczące dostaw komponentów krytycznych elementów sieci)

(1) Operator musi posiadać wiedzę na temat całego łańcucha dostaw i związanego z nim ryzyka, w tym podwykonawców poszczególnych komponentów krytycznych elementów sieci, co obejmuje również klucze szyfrowania, UICC/eUICC i inne elementy bezpieczeństwa, których niewłaściwe wykorzystanie mogłoby zagrozić bezpieczeństwu podmiotów krytycznych.

(2) Operator zobowiązany jest zapewnić, aby wymogi bezpieczeństwa mające zastosowanie między operatorem a producentami lub dostawcami komponentów krytycznych elementów sieci lub działającymi na jego rzecz dostawcami usług wsparcia trzeciego poziomu były ustalane umownie i dokumentowane oraz wymagały od producentów lub dostawców przestrzegania uzgodnionych środków bezpieczeństwa w ramach całego łańcucha dostaw.

(3) Aby w porę zapobiegać wykorzystywaniu luk w zabezpieczeniach przez szkodliwe podmioty, operator zobowiązany jest zapewnić, aby producent lub dostawca komponentów krytycznego elementu sieci zobowiązał się umownie do niezwłocznego informowania operatora o wykrytych lukach oraz o środkach mających na celu zmniejszenie ryzyka, a także do zapewnienia doradztwa w zakresie środków ochronnych lub zaradczych, które operator może podjąć w odpowiedzi na zagrożenie.

(4) Operator weryfikuje co najmniej raz w roku adekwatność praw dostępu do krytycznych elementów sieci lub niezwłocznie je aktualizuje zgodnie ze zmianami następującymi w organizacji lub po stronie dostawców usług wsparcia trzeciego poziomu.

(5) Operator zapobiega powstaniu zależności od indywidualnego dostawcy lub dostawcy usług trzeciego poziomu (tj. uzależnienia od jednego dostawcy), jeżeli jest to technicznie wykonalne i ekonomicznie uzasadnione, w celu zmniejszenia zależności i zwiększenia odporności w przypadku luk w zabezpieczeniach komponentów krytycznych, w tym poprzez unikanie zawierania długoterminowych umów z poszczególnymi producentami lub dostawcami albo dostawcami usług wsparcia trzeciego poziomu lub zapewnienie możliwości ich zmiany w celu ograniczenia zakłóceń w świadczeniu usług na rzecz podmiotów krytycznych do możliwie najniższego poziomu.

Artykuł 7

(Warunki umów zawieranych z producentami, dostawcami lub dostawcami usług wsparcia trzeciego poziomu)

W celu zapewnienia wysokiego poziomu bezpieczeństwa operator uwzględnia w nowych warunkach umów zawieranych z producentami, dostawcami lub dostawcami usług wsparcia trzeciego szczebla co najmniej następujące elementy:

1. oświadczenie producenta lub dostawcy, że komponent lub jego ustawienia domyślne nie zawierają nieudokumentowanych, pozostawionych umyślnie luk (tzw. backdoor), ani nie wywierają żadnego negatywnego wpływu na funkcjonowanie podmiotów krytycznych,
2. zobowiązanie producenta lub dostawcy albo dostawcy usług trzeciego poziomu do ochrony danych, w których posiadanie wejdą podczas świadczenia usług lub do których dostęp uzyskają w związku ze świadczeniem usługi dostępu,
3. zobowiązanie producenta lub dostawcy albo dostawcy usług trzeciego poziomu do niezwłocznego informowania operatora w przypadku naruszenia ochrony danych komunikacyjnych lub danych o ruchu, które mają lub mogą mieć wpływ na operatora lub podmioty krytyczne, o których mowa w art. 1 pkt 1 niniejszej ustawy ogólnej,
4. zobowiązanie producenta lub dostawcy albo dostawcy usług trzeciego poziomu do niezwłocznego powiadamiania operatora o wszelkich incydentach związanych z bezpieczeństwem i lukach w zabezpieczeniach, które mogłyby mieć wpływ na bezpieczeństwo sieci, powiązanych usług lub danych operatora,
5. zobowiązanie producenta lub dostawcy albo dostawcy usług trzeciego poziomu do przestrzegania norm i zasad bezpieczeństwa określonych przez operatora oraz do podejmowania odpowiednich środków bezpieczeństwa w celu zapewnienia bezpieczeństwa systemów i sieci informacyjnych oraz danych operatora lub podmiotu krytycznego,
6. zdolność operatora do dokonywania przeglądu środowisk, procedur, środków bezpieczeństwa i narzędzi stosowanych przez dostawcę usług wsparcia trzeciego poziomu przy dostępie do sieci i danych operatora w dowolnym momencie,
7. odpowiedzialność producenta lub dostawcy albo dostawcy usług wsparcia trzeciego stopnia za szkody, które zostałyby spowodowane przez zidentyfikowane luki w zabezpieczeniach lub niewłaściwe wykorzystanie komponentów krytycznych elementów sieci, ich domyślnych ustawień lub w trakcie świadczenia usług wsparcia trzeciego poziomu, które producent lub dostawca albo dostawca wsparcia trzeciego stopnia zaniedbał lub celowo wdrożył,
8. obowiązek regularnego szkolenia personelu producenta lub dostawcy albo dostawcy usług wsparcia trzeciego poziomu w dziedzinie bezpieczeństwa danych oraz systemów i sieci informacyjnych.

Artykuł 8
(Przepisy dotyczące dostępu do krytycznych elementów sieci i korzystania z nich)

(1) W przypadku fizycznego lub logicznego dostępu do komponentów krytycznych elementów sieci, ich ustawień oraz danych operatora przechowywanych, przetwarzanych lub zmodyfikowanych przy ich użyciu, operator zapewnia:

1. ograniczenie dostępu wyłącznie do osób, które zostały uprzednio upoważnione,
2. kontrolowanie przez operatora wszystkich prac nad krytycznymi elementami sieci wykonywanych na miejscu lub w ramach zdalnego dostępu,
3. stosowanie uwierzytelniania wieloskładnikowego w przypadku użytkowników, którym przypisano najwyższe uprawnienia dostępu do poszczególnych komponentów

krytycznych elementów sieci, ich ustawień lub danych przechowywanych bądź przetwarzanych przy ich użyciu,

4. przydzielenie każdej upoważnionej osobie, której udzielono dostępu, unikalnego konta użytkownika i hasła,
5. wykorzystywanie wyłącznie haseł, które są zmieniane regularnie lub natychmiast w przypadku wykrycia niewłaściwego użycia i składają się z co najmniej 15 znaków, w tym wielkich i małych liter, cyfr i znaków specjalnych, jeżeli oprogramowanie na to pozwala,
6. wdrażanie w miarę możliwości zasady zerowej tolerancji lub zaufania w zakresie dostępu,
7. ochronę bezpieczeństwa połączenia komunikacyjnego między upoważnionym użytkownikiem a poszczególnymi komponentami realizowaną przy użyciu szyfrowania, z uwzględnieniem najnowszych osiągnięć technologicznych i najlepszych dobrych praktyk branżowych w dziedzinie bezpieczeństwa informacji lub zalecanych przez uznane instytucje zajmujące się bezpieczeństwem informacji,
8. sporządzanie nieusuwalnego zapisu przypadków uzyskania dostępu i prób uzyskania dostępu, który będzie przechowywany przez co najmniej 6 miesięcy, włącznie z kopią zapasową, przy czym okres ten może być dłuższy jeśli analiza zarządzania ryzykiem i ocena dopuszczalnego poziomu ryzyka wskazują, że ryzykiem należy odpowiednio zarządzać poprzez przechowywanie rejestrów przez wydłużony czas,
9. rejestrowanie i monitorowanie, o ile to możliwe, wszystkich ingerencji w komponenty realizowanych przy użyciu oprogramowania, łącznie ze zmianami konfiguracji. Zapisy, w tym kopię zapasową tych danych, przechowuje się przez okres wskazany w poprzednim punkcie,
10. czasowe ograniczenie dostępu do poszczególnych komponentów oraz do danych przechowywanych lub przetwarzanych przy ich użyciu i jego umożliwianie tylko na czas wykonywania niezbędnej pracy.

(2) W przypadku dostępu pracowników lub pracowników dostawcy usług wsparcia trzeciego poziomu do poszczególnych komponentów krytycznych elementów sieci:

1. muszą oni korzystać wyłącznie z bezpiecznej, pośredniej, dedykowanej stacji roboczej (serwera przesiadkowego, ang. „jump server”), która podlega regularnym kontrolom bezpieczeństwa,
2. muszą oni zainstalować na dedykowanej stacji roboczej tylko absolutnie niezbędne i aktualizowane o najnowsze poprawki bezpieczeństwa narzędzia, komponenty i aktywne usługi pozwalające uzyskać dostęp do innych, absolutnie niezbędnych zasobów w sieci,
3. muszą oni korzystać z bezpiecznych operacji kryptograficznych i kluczy na dedykowanej stacji roboczej, która musi znajdować się w sieci operatora i pozostawać pod jego wyłączną kontrolą,
4. każdy przypadek uzyskania dostępu musi być zatwierdzany i aktywowany przez operatora ręcznie i tylko na czas trwania dostępu,
5. wszystkie przypadki uzyskania dostępu i działania muszą być fizycznie kontrolowane i rejestrowane przez operatora,
6. muszą oni stosować uwierzytelnianie dwuskładnikowe i hasła składające się z co najmniej 15 znaków, w tym wielkich i małych liter, cyfr i znaków specjalnych, które należy zmieniać w oparciu o ocenę ryzyka.

(3) Zanim operator przekaże osobie trzeciej zarządzanie, utrzymanie lub aktualizowanie krytycznych elementów sieci bądź ich poszczególnych komponentów, sprawdza i upewnia się, że osoba ta stosuje mechanizmy bezpieczeństwa i procesy zarządzania

bezpieczeństwem, które są co najmniej takie same lub lepsze w porównaniu z mechanizmami i procesami stosowanymi przez operatora. Operator niezwłocznie informuje o zamiarze przekazania zainteresowany podmiot krytyczny, Agencję i organ odpowiedzialny za bezpieczeństwo informacji.

(4) Operator weryfikuje rzeczywisty stan procesów bezpieczeństwa przed rozpoczęciem świadczenia usług, a następnie co najmniej raz w roku. Operator prowadzi rejestr wewnętrznych przeglądów i kontroli dotyczących świadczenia usług wsparcia przez osoby trzecie i przechowuje go przez okres świadczenia usług oraz przez okres jednego roku po ich zakończeniu, nie dłużej jednak niż przez pięć lat.

PRZEPISY PRZEJŚCIOWE I KOŃCOWE

Artykuł 9
(Przepisy przejściowe)

(1) Operator powiadamia Agencję i organ odpowiedzialny za bezpieczeństwo informacji o istniejących lokalizacjach krytycznych elementów sieci w terminie 30 dni od wejścia w życie niniejszej ustawy ogólnej.

(2) Operator powiadamia Agencję i organ odpowiedzialny za bezpieczeństwo informacji o istniejących lokalizacjach usług wsparcia trzeciego poziomu w odniesieniu do krytycznych elementów sieci w terminie 30 dni od wejścia w życie niniejszej ustawy ogólnej.

(3) Agencja publikuje po raz pierwszy dokumenty, o których mowa w art. 3 ust. 2 niniejszej ustawy ogólnej, w dniu jej wejścia w życie.

Artykuł 10
(Wejście w życie)

Niniejsza ustawa ogólna wchodzi w życie trzydziestego dnia po jej opublikowaniu w Dzienniku Urzędowym Republiki Słowenii, wskutek czego operatorzy mogą korzystać ze sprzętu i kontynuować świadczenie usług wsparcia trzeciego poziomu do upływu terminów określonych w art. 312 ust. 2 i 3 Ustawy.

Nr _____ mgr Marko Mišmaš

Lublana, dnia _____ dyrektor

EVA 2023-3150-0034

PROJEKT

Załącznik

Wykaz krytycznych elementów sieci i powiązanych systemów informacyjnych:

Krytyczne elementy sieci	**Funkcje sieci i systemów informacyjnych**
Mechanizmy zarządzania abonentami i szyfrowania	- zarządzanie sesjami (głos i dane), - uwierzytelnianie użytkowników i urządzeń w sieci, - zarządzanie i przechowywanie kluczy do autoryzacji abonentów i komponentów sieci (UICC/eUICC, certyfikaty cyfrowe/HSM), - funkcje bezpiecznego uwierzytelniania, ochrony integralności komunikacji (szyfrowania) i przechowywania kluczy użytkownika, komponentów sieciowych i zarządzających, - zarządzanie prawami dostępu.
Połączenia wzajemne	- funkcje hostingu i interfejsy do innych sieci i usług.
Zarządzane usługi sieciowe	- rejestracja i autoryzacja usług sieciowych, - przechowywanie i przetwarzanie danych dotyczących komunikacji, lokalizacji i ruchu, - ekspozycja sieci i funkcji sieciowych na zewnętrzne aplikacje i usługi.
Zarządzanie i orkiestracja zwirtualizowanych funkcji sieciowych (NFV) oraz orkiestracja sieci (MANO), z uwzględnieniem infrastruktury wirtualizacji	- funkcje zarządzania orkiestracją i konfiguracją NFV niezależnie od rodzaju implementacji (VM, kontener, mikrousługi), - funkcje wirtualizacji na potrzeby wdrożenia i wykorzystania NFV, - funkcja wyboru elementu sieci (NSSF);
Sieć dostępu radiowego	- stacje bazowe obsługujące technologię 5G lub wyższą.
Systemy zarządzania i pozostałe systemy wsparcia	- monitorowanie funkcjonowania sieci łączności ruchomej i zarządzania nią, z uwzględnieniem części dostępowej (RAN/O-RAN), - systemy wykrywania zdarzeń dotyczących bezpieczeństwa, anomalii, zagrożeń i zarządzania nimi (funkcje bezpieczeństwa, w tym SIEM/SOAR).
Legalne przejęcie	- funkcje dostępu właściwego organu do treści komunikacji i danych dotyczących ruchu generowanego przez użytkowników.