Spis treści

1. Wyciągi z ustawy zmieniającej ustawę o łączności elektronicznej, kodeks budowlany i ustawę o opłatach państwowych.

§ 1. Nowelizacja ustawy o łączności elektronicznej

Do ustawy o łączności elektronicznej wprowadza się następujące zmiany:

111) Uchyla się art. 87 ust. 2^1 i 2^2;

118) Ustawę uzupełnia się o art. 87^3–87^5 w brzmieniu:

„**§ 87^3. Wymogi dotyczące sieci i usług łączności w celu zapewnienia bezpieczeństwa narodowego**

(1) Sprzęt i oprogramowanie wykorzystywane do świadczenia usług łączności w sieci łączności nie mogą stanowić zagrożenia dla bezpieczeństwa narodowego.

(2) Sprzęt i oprogramowanie wykorzystywane do świadczenia usług łączności w sieci łączności mogą stanowić zagrożenie dla bezpieczeństwa narodowego ze względu na:
1) wysokie ryzyko wynikające ze strony producenta lub dostawcy usług utrzymania lub pomocy technicznej (zwane dalej »sprzętem lub oprogramowaniem wysokiego ryzyka«);
2) ryzyko wynikające z charakterystyki technicznej lub konfiguracji sprzętu lub oprogramowania.

3)) Przy ocenie sprzętu lub oprogramowania wysokiego ryzyka uwzględnia się między innymi informacje na temat tego, czy:
1) producent lub dostawca usług utrzymania lub pomocy technicznej ma zarejestrowaną siedzibę lub centralę w kraju (zwanym dalej »krajem zamieszkania«), który nie jest państwem członkowskim Unii Europejskiej, Organizacji Traktatu Północnoatlantyckiego (zwanego dalej »NATO«) lub Organizacji Współpracy Gospodarczej i Rozwoju (zwanej dalej »OECD«);
2) zasady demokratycznych rządów prawa nie są przestrzegane lub prawa człowieka nie są przestrzegane w kraju zamieszkania producenta lub dostawcy usług utrzymania lub pomocy technicznej;
3) własność intelektualna, dane osobowe lub tajemnice handlowe osób z innych krajów nie są chronione w kraju zamieszkania producenta lub dostawcy usług utrzymania lub pomocy technicznej;
4) kraj zamieszkania producenta lub dostawcy usług utrzymania lub pomocy technicznej wykazuje agresywne zachowania w cyberprzestrzeni;
5) państwa członkowskie Unii Europejskiej, NATO lub OECD przypisały cyberataki krajowi zamieszkania producenta lub dostawcy usług utrzymania lub pomocy technicznej;
6) producent lub dostawca usług utrzymania lub pomocy technicznej podlega rządowi lub organowi państwowemu kraju zamieszkania lub innego państwa obcego, w którym nie występuje niezależna kontrola sądowa;
7) kraj zamieszkania producenta lub dostawcy usług utrzymania lub pomocy technicznej lub inne państwo obce może zobowiązać go do działania w sposób stwarzający zagrożenie dla bezpieczeństwa narodowego Estonii;
8) działalność gospodarcza producenta lub dostawcy usług utrzymania lub pomocy technicznej nie opiera się na konkurencji opartej na zasadach rynkowych lub nie stworzono w tym celu odpowiednich warunków w kraju zamieszkania;
9) struktura własnościowa, struktura organizacyjna lub struktura zarządzania producenta lub dostawcy usług utrzymania lub pomocy technicznej nie są przejrzyste;

10) finansowanie producenta lub dostawcy usług utrzymania lub pomocy technicznej nie jest przejrzyste;
11) produkty lub usługi producenta lub dostawcy usług utrzymania lub pomocy technicznej obejmują luki w zabezpieczeniach i nie wdrożono odpowiednich środków bezpieczeństwa w celu ich wyeliminowania;
12) producent lub dostawca usług utrzymania lub pomocy technicznej nie jest w stanie zapewnić ciągłości dostaw produktów lub usług, chyba że jest to spowodowane działaniem siły wyższej.

(4) W celu zapewnienia bezpieczeństwa narodowego przedsiębiorstwo świadczące usługi łączności jest zobowiązane powiadamiać Urząd Ochrony Konsumentów i Regulacji Technicznych o sprzęcie i oprogramowaniu używanym w sieci łączności.

(5) Zakres obowiązku zgłoszenia określonego w ust. 4 niniejszego artykułu, jak również szczególne wymagania, termin wykonania obowiązku i procedurę zgłoszenia określa się w drodze rozporządzenia Rządu Republiki.

(6) W celu zapewnienia bezpieczeństwa narodowego przedsiębiorstwo świadczące usługi łączności jest zobowiązane do ubiegania się o zezwolenie na używanie sprzętu lub oprogramowania sieci łączności (zwane dalej »zezwoleniem na używanie sprzętu lub oprogramowania«) od Urzędu Ochrony Konsumentów i Regulacji Technicznych.

(7) Zakres obowiązku ubiegania się o zezwolenie na używanie sprzętu lub oprogramowania, szczególne wymagania, termin i procedura postępowania oraz specyfikacje dotyczące okresu zezwolenia na używanie określa się w drodze rozporządzenia Rządu Republiki.

(8) Przy wydawaniu przepisów określonych w ust. 5 i 7 niniejszej ustawy Rząd Republiki bierze pod uwagę znaczenie sieci łączności, jej sprzętu lub oprogramowania oraz usług komunikacyjnych świadczonych w sieci, a także potencjalne zagrożenia dla bezpieczeństwa narodowego.

§ 87[4]. Postępowanie w sprawie zezwolenia na używanie sprzętu lub oprogramowania

(1) Po otrzymaniu wniosku o zezwolenie na używanie sprzętu lub oprogramowania Urząd Ochrony Konsumentów i Regulacji Technicznych zwraca się do organów ds. bezpieczeństwa i Urzędu ds. Systemów Informatycznych o opinię na temat tego, czy sprzęt lub oprogramowanie określone we wniosku przedsiębiorstwa świadczącego usługi łączności o zezwolenie na używanie sprzętu lub oprogramowania stanowią zagrożenie dla bezpieczeństwa narodowego. Jeżeli sprzęt lub oprogramowanie mogą stanowić zagrożenie dla bezpieczeństwa narodowego zgodnie z otrzymaną opinią, Urząd Ochrony Konsumentów i Regulacji Technicznych zwraca się o zatwierdzenie przez organ określony w statucie Komitetu ds. Bezpieczeństwa Republiki Estońskiej (zwany dalej »organem administracyjnym«) przed rozstrzygnięciem wniosku przedsiębiorstwa świadczącego usługi łączności o zezwolenie na używanie sprzętu lub oprogramowania.

(2) W procesie zatwierdzania określonym w ust. 1 niniejszego artykułu organ administracyjny ocenia, czy używanie sprzętu lub oprogramowania określonych we wniosku o zezwolenie na używanie sprzętu lub oprogramowania stanowi zagrożenie dla bezpieczeństwa narodowego. W procesie zatwierdzania organ administracyjny może zaproponować zakaz używania sprzętu lub oprogramowania określonych we wniosku o zezwolenie na używanie sprzętu lub oprogramowania lub ustanowić warunki ich używania. Warunki używania sprzętu lub oprogramowania mogą obejmować, między innymi, ograniczenie czasowe używania,

używanie w niektórych częściach lub funkcjach lub z określoną konfiguracją sieci łączności.

(3) Uwzględniając postanowienia ust. 1 i 2 niniejszego artykułu, Urząd Ochrony Konsumentów i Regulacji Technicznych podejmuje decyzję o zatwierdzeniu, warunkowym zatwierdzeniu lub odmowie zatwierdzenia wniosku o zezwolenie na używanie sprzętu lub oprogramowania.

(4) W przypadku gdy sprzęt lub oprogramowanie nie stanowią zagrożenia dla bezpieczeństwa narodowego, zezwolenie na używanie jest udzielane na okres ośmiu lat. W przypadku gdy sprzęt lub oprogramowanie stanowią zagrożenie dla bezpieczeństwa narodowego, nie udziela się zezwolenia na używanie lub udziela się warunkowego zezwolenia na używanie.

§ 87^5. Audyt

1. Przedsiębiorstwo świadczące usługi łączności, na które nałożono obowiązki na podstawie art. 87^3 niniejszej ustawy, zleca przeprowadzenie audytu zgodności swojej działalności co najmniej raz na trzy lata po nałożeniu obowiązku, w celu oceny w sprawozdaniu z audytu, czy przedsiębiorstwo świadczące usługi łączności wywiązało się z obowiązków nałożonych na podstawie tego samego artykułu.

2. Osoba przeprowadzająca audyt musi być niezależnym audytorem posiadającym certyfikat audytora systemów informatycznych wydany przez ISACA lub podobny certyfikat.

3. Osoba przeprowadzająca audyt przedkłada audyt do Urzędu Ochrony Konsumentów i Regulacji Technicznych.

4. Koszty przeprowadzenia audytu pokrywa przedsiębiorstwo świadczące usługi łączności.

5. Treść obowiązku przeprowadzenia audytu określonego w ust. 1 niniejszego artykułu oraz termin i procedurę przedłożenia audytu określa rozporządzenie Rządu Republiki.”;

152) ustawę uzupełnia się o art. 170^3 w brzmieniu:

„**§ 170^3. Naruszenie obowiązków nałożonych dla celów bezpieczeństwa narodowego**

(1) Naruszenie obowiązków nałożonych na podstawie art. 87^3 lub 87^5 ustawy podlega karze grzywny w wysokości do 300 stawek dziennych.

(2) Ten sam czyn, jeżeli został popełniony przez osobę prawną, podlega karze grzywny w wysokości do 50 000 EUR.”;

156) Ustawę uzupełnia się o art. 196^3–196^5 w brzmieniu:

§ 196^5. Wykonanie art. 87^3 oraz 87^4 niniejszej ustawy

(1) Obowiązek ubiegania się o zezwolenie na używanie sprzętu lub oprogramowania, o którym mowa w art. 87^3 ust. 6 niniejszej ustawy, ma zastosowanie w przypadku sprzętu lub oprogramowania wdrożonych przed dniem 1 lutego 2022 r., jeżeli w sprzęcie lub oprogramowaniu została lub zostanie wdrożona funkcja standardu 5G non-stand alone (zwanego dalej »5G NSA«) lub standardu sieci łączności ruchomej nowszej generacji.

(2) Sprzęt lub oprogramowanie wysokiego ryzyka, w przypadku gdy funkcja 5G NSA lub standardu sieci łączności ruchomej nowszej generacji jest lub zostałaby wdrożona i które nie posiadają funkcji krytycznej, mogą być używane na podstawie zezwolenia na używanie do dnia 31 grudnia 2025 r. Zezwolenie na używanie nie jest wydawane na sprzęt lub oprogramowanie wysokiego ryzyka określone w zdaniu pierwszym po dniu 31 grudnia 2025 r.

Termin składania wniosków o zezwolenie na używanie sprzętu lub oprogramowania wysokiego ryzyka określone w zdaniu pierwszym jest określony w rozporządzeniu określonym w art. 87^3 ust. 7 niniejszej ustawy.

(3) Ze sprzętu lub oprogramowania, które nie posiadają funkcji 5G NSA lub standardu sieci łączności ruchomej nowszej generacji lub funkcji krytycznej można korzystać do dnia 31 grudnia 2029 r. bez ubiegania się o zezwolenie na używanie określone w art. 87^3 ust. 6 niniejszej ustawy.

(4) Jeżeli sprzęt lub oprogramowanie określone w ust. 3 niniejszego artykułu mają być używane po dniu 31 grudnia 2029 r., wniosek o zezwolenie na używanie musi zostać złożony nie później niż dnia 1 lipca 2029 r. Zezwolenie na używanie nie jest wydawane na sprzęt lub oprogramowanie wysokiego ryzyka określone w zdaniu pierwszym po dniu poniedziałek, 31 grudnia 2029 r.

(5) Funkcje krytyczne sprzętu i oprogramowania są następujące: 1) funkcja sieci bazowej zgodnie ze standardami Europejskiego Instytutu Norm Telekomunikacyjnych, niezależnie od lokalizacji funkcji w sieci łączności; 2) funkcja, której celem jest umożliwienie organom bezpieczeństwa i agencjom nadzoru prowadzenia działań nadzorczych lub ograniczenie prawa do poufności wiadomości w przypadkach przewidzianych przez prawo.";

2. Rozporządzenie Rządu Republiki nr 119 z dnia 16 grudnia 2021 r. w sprawie zmian do rozporządzenia Rządu Republiki nr 140 z dnia 22 czerwca 2006 r. w sprawie wymogów dotyczących świadczenia usług łączności i wymogów technicznych dla sieci łączności oraz rozporządzenia Rządu Republiki nr 129 z dnia 11 grudnia 2015 r. w sprawie statutu Komitetu ds. Bezpieczeństwa Rządu Republiki.

Wydawca: ROZPORZĄDZENIE

Rodzaj: rozporządzenie

Rodzaj tekstu: tekst wstępny

Wejście w życie: 1 lutego 2022 r.

Nr ref. publikacji: RT I, 21.12.2021, 1

Zmiany do rozporządzenia Rządu Republiki nr 140 z dnia 22 czerwca 2006 r. w sprawie wymogów dotyczących świadczenia usług łączności i wymogów technicznych dla sieci łączności oraz rozporządzenia Rządu Republiki nr 129 z dnia 11 grudnia 2015 r. w sprawie statutu Komitetu ds. Bezpieczeństwa Rządu Republiki

Przyjęto 16 grudnia 2021 r., nr 119

Rozporządzenie wprowadza się na podstawie art. 87 ust. 2, art. 87^3 ust. 5 i 7 oraz art. 87^5 ust. 5 ustawy o łączności elektronicznej oraz art. 4 ust. 2 ustawy o obronie narodowej.

§ 1. Zmiana rozporządzenia Rządu Republiki nr 140 z dnia 22 czerwca 2006 r. w sprawie wymogów dotyczących świadczenia usług łączności i wymogów technicznych dla sieci łączności

Do rozporządzenia Rządu Republiki nr 140 z dnia 22 czerwca 2006 r. w sprawie wymogów dotyczących świadczenia usług łączności i wymogów technicznych dla sieci łączności wprowadza się następujące zmiany:

1) W art. 2 ust. 1, art. 3 ust. 4 pkt 1 oraz art. 6 ust 1 preambuły rozporządzenia słowa „Ustawa o łączności elektronicznej" zastępuje się słowami „Ustawa o łączności elektronicznej";

2) preambułę rozporządzenia uzupełnia się po słowach „ust. 2" słowami „, art. 87^3 ust. 5 i 7 oraz art. 87^5 ust. 5";

3) Art. 1 otrzymuje brzmienie:

„Niniejsze rozporządzenie ustanawia:

1) wymogi dotyczące świadczenia usług publicznej łączności elektronicznej (zwanych dalej »usługami łączności«) wynikające z celów określonych w art. 87 ust. 2 pkt 1, 3 i 4 ustawy o łączności elektronicznej;

2) wymogi techniczne i dotyczące bezpieczeństwa narodowego w odniesieniu do publicznej sieci łączności elektronicznej (zwanej dalej »siecią łączności«);

3) obowiązek powiadamiania o sprzęcie i oprogramowaniu wykorzystywanym w sieci łączności, treść i procedurę składania wniosku o zezwolenie na używanie oraz treść i procedurę obowiązku przeprowadzenia audytu.";

4) rozporządzenie uzupełnia się o rozdział 2^1 w brzmieniu:

„Rozdział 21.

WYMOGI DOTYCZĄCE USŁUG ŁĄCZNOŚCI ELEKTRONICZNEJ I SIECI ŁĄCZNOŚCI W CELU ZAPEWNIENIA BEZPIECZEŃSTWA NARODOWEGO

Część 1

Przepisy ogólne

§ 3^1 Zakres stosowania wymogów

(1) Wymogi ustanowione w niniejszym rozdziale mają zastosowanie do przedsiębiorstwa świadczącego usługi łączności, które jest dostawcą zasadniczej usługi wymienionej w art. 87 ust. 4 ustawy o łączności elektronicznej lub które stosuje funkcję standardu 5G non-stand alone (zwanego dalej: »5G NSA«) lub standardu sieci łączności ruchomej nowszej generacji Europejskiego Instytutu Norm Telekomunikacyjnych podczas świadczenia usług łączności.

(2) Wymogi ustanowione w niniejszym rozdziale nie mają zastosowania do następującego sprzętu:

1) fizycznej infrastruktury sieci łączności w rozumieniu art. 61^2 ust. 1 kodeksu budownictwa;

2) elementów sieci, które nie są w stanie przetworzyć sygnałów lub nie wymagają energii do działania;

3) jednostek zasilających;

4) urządzeń klimatyzacyjnych;

5) urządzeń końcowych będących własnością użytkownika końcowego lub znajdujących się w jego posiadaniu.

Część 2

Obowiązek powiadomienia

§ 3^2 Powiadomienie o sprzęcie i oprogramowaniu używanym w sieci łączności

1. Do dnia 1 marca każdego roku kalendarzowego przedsiębiorstwo świadczące usługi łączności powiadamia Urząd Ochrony Konsumentów i Regulacji Technicznych o sprzęcie i oprogramowaniu używanym w swojej sieci łączności na dzień 1 stycznia danego roku.

2. W powiadomieniu, o którym mowa w ust. 1, przedsiębiorstwo świadczące usługi łączności przekazuje następujące informacje na temat sprzętu i oprogramowania używanego w sieci łączności:

1) nazwę i numer wersji;

2) liczbę;

3) nazwę producenta;

4) nazwę właściciela;

5) nazwy stron umowy dotyczącej prawa do używania i okres ważności prawa do używania, jeżeli właściciel sprzętu lub oprogramowania nie jest przedsiębiorstwem świadczącym usługi łączności;

6) funkcję w sieci łączności;

7) fizyczną lokalizację używania, którą można określić jako państwo, jednostkę administracyjną, siedzibę, adres lub inne uściślenie regionalne;

8) istnienie lub brak zezwolenia na używanie sprzętu lub oprogramowania;

9) w przypadku sprzętu lub oprogramowania używanego w sieci ruchomej, generację sieci ruchomej, z którą sprzęt i oprogramowanie działają;

10) wykaz osób prawnych, które – poza przedsiębiorstwem świadczącym usługi łączności – mają administracyjny dostęp do sprzętu lub oprogramowania oraz warunki dostępu każdej z osób prawnych;

11) dostawców usług utrzymania i pomocy technicznej dla sprzętu i oprogramowania używanego w sieci łączności, indywidualnie przez osoby prawne, jeśli są to osoby inne niż osoby, o których mowa w pkt 4 i 5;

12) określenie części powiadomienia, które powinny podlegać ograniczeniom dostępu zgodnie z ustawą o informacji publicznej.

(3) Urząd Ochrony Konsumentów i Regulacji Technicznych przekazuje powiadomienie, o którym mowa w ust. 1, do organów bezpieczeństwa oraz Państwowego Urzędu Systemu

Informacyjnego w celach informacyjnych.

Część 3

Obowiązek uzyskania zezwolenia na używanie

§ 3[3] Zezwolenie na używanie sprzętu lub oprogramowania oraz procedura aplikacyjna

(1) Przedsiębiorstwo świadczące usługi łączności składa wniosek o zezwolenie na używanie sprzętu lub oprogramowania do Urzędu Ochrony Konsumentów i Regulacji Technicznych przed planowanym użyciem sprzętu lub oprogramowania.

(2) Przedsiębiorstwo świadczące usługi łączności składa wniosek o zezwolenie na używanie nie później niż 10 dni roboczych po wdrożeniu sprzętu lub oprogramowania, jeżeli wymagane jest natychmiastowe wdrożenie sprzętu lub oprogramowania w celu wyeliminowania lub natychmiastowego powstrzymania cyberincydentu w rozumieniu ustawy o cyberbezpieczeństwie.

(3) We wniosku o zezwolenie na używanie przedsiębiorstwo świadczące usługi łączności przedkłada informacje, o których mowa w art. 3[2] ust. 2 pkt 1, 3–7 i 9–11, oraz określa części wniosku o zezwolenie na używanie sprzętu lub oprogramowania, które powinny podlegać ograniczeniom dostępu zgodnie z ustawą o informacji publicznej.

(4) Przedsiębiorstwo świadczące usługi łączności może wymienić sprzęt i wprowadzić aktualizacje oprogramowania bez ubiegania się o zezwolenie na używanie sprzętu lub oprogramowania, w którym to przypadku zmienia się nazwa lub numer wersji sprzętu lub oprogramowania zatwierdzonego w zezwoleniu, pod warunkiem że inne informacje zatwierdzone w zezwoleniu pozostają bez zmian.

§ 3[4] Przetwarzanie i zatwierdzanie wniosku o zezwolenie na używanie sprzętu lub oprogramowania

(1) Urząd Ochrony Konsumentów i Regulacji Technicznych przekazuje wniosek o zezwolenie na używanie w ciągu 5 dni roboczych od jego otrzymania do organów bezpieczeństwa oraz Państwowego Urzędu Systemu Informacyjnego do zaopiniowania.

(2) Jeżeli organ bezpieczeństwa lub Państwowy Urząd Systemu Informacyjnego stwierdzą, że sprzęt lub oprogramowanie sieci łączności wymienione we wniosku o zezwolenie mogą zagrażać bezpieczeństwu narodowemu, przedstawiają uzasadnioną opinię na temat wniosku o używanie w ciągu 20 dni roboczych wraz z propozycją zakazu używania sprzętu lub oprogramowania lub nałożenia warunków na ich używanie.

(3) Jeżeli organ bezpieczeństwa lub Państwowy Urząd Systemu Informacyjnego stwierdzą w opinii, że sprzęt lub oprogramowanie wymienione we wniosku mogą zagrażać bezpieczeństwu narodowemu, Urząd Ochrony Konsumentów i Regulacji Technicznych zapewnia przedsiębiorstwu świadczącemu usługi łączności możliwość przedstawienia w ciągu 20 dni roboczych opinii na temat tego, w jaki sposób odrzucenie wniosku lub nałożenie warunków wpływa na przedsiębiorstwo świadczące usługi łączności i świadczenie usług łączności, przedstawiając jednocześnie propozycję warunków.

(4) Po upływie terminu na przedstawienie opinii, o której mowa w ust. 3, Urząd Ochrony Konsumentów i Regulacji Technicznych przekazuje wniosek przedsiębiorstwa świadczącego usługi łączności wraz z opiniami określonymi w ust. 2 i 3 Radzie ds. Cyberbezpieczeństwa

Komitetu ds. Bezpieczeństwa Rządu Republiki (zwanej dalej »Radą ds. Cyberbezpieczeństwa«)

(5) W ramach zatwierdzenia Rada ds. Cyberbezpieczeństwa dokonuje oceny, czy sprzęt lub oprogramowanie sieci łączności wymienione we wniosku o zezwolenie na używanie są sprzętem lub oprogramowaniem wysokiego ryzyka oraz czy ich używanie może zagrażać bezpieczeństwu narodowemu ze względu na cechy techniczne lub ustawienia. Jeżeli sprzęt lub oprogramowanie mogą stanowić zagrożenie dla bezpieczeństwa narodowego, Rada ds. Cyberbezpieczeństwa ocenia warunki używania sprzętu lub oprogramowania i uwzględnia wpływ odmowy lub nałożenia warunków na zezwolenie na używanie sprzętu lub oprogramowania na przedsiębiorstwo świadczące usługi łączności, ciągłość usług łączności i sieci łączności, rynek łączności i konkurencję, a także ocenia okres obowiązywania zezwolenia na używanie.

(6) Rada ds. Cyberbezpieczeństwa zatwierdza wniosek albo w sposób uzasadniony odmawia jego zatwierdzenia w ciągu 30 dni roboczych od otrzymania materiałów wymienionych w ust. 4. W razie potrzeby Rada ds. Cyberbezpieczeństwa może przedłużyć termin zatwierdzenia o nie więcej niż 15 dni roboczych, powiadamiając o tym Urząd Ochrony Konsumentów i Regulacji Technicznych.

§ 3^5 Specyfikacja okresu zezwolenia na używanie

W wyniku wymiany sprzętu lub aktualizacji oprogramowania w przypadku, o którym mowa w art. 3^3 ust. 4, okres obowiązywania wcześniej przyznanego zezwolenia na wymieniony sprzęt lub zaktualizowane oprogramowanie jest kontynuowany w odniesieniu do nowego sprzętu lub oprogramowania.

§ 3^6 Termin procedury udzielania zezwolenia

(1) Urząd Ochrony Konsumentów i Regulacji Technicznych podejmuje decyzję w sprawie uwzględnienia wniosku o używanie przedsiębiorstwa świadczącego usługi łączności i wydania zezwolenia na używanie w ciągu 30 dni roboczych od otrzymania wniosku, z wyjątkiem konieczności przeprowadzenia procedury przewidzianej w art. 3^4 ust. 3–6.

(2) Jeżeli do wniosku ma zastosowanie art. 3^4 ust. 3–6, Urząd Ochrony Konsumentów i Regulacji Technicznych podejmuje decyzję w sprawie uwzględnienia lub odrzucenia wniosku o używanie i wydania zezwolenia na używanie w ciągu 105 dni roboczych od otrzymania wniosku.

Część 4

Obowiązek przeprowadzenia audytu

§ 3^7 Treść i organizacja obowiązku przeprowadzenia audytu

(1) Audyt zgodności zlecany przez przedsiębiorstwo świadczące usługi łączności weryfikuje, czy przedsiębiorstwo świadczące usługi łączności wypełniło obowiązki nałożone na mocy art. 87^3 ustawy o łączności elektronicznej i określone w niniejszym rozporządzeniu.

(2) W odniesieniu do obowiązku powiadamiania o sprzęcie i oprogramowaniu, audytor sprawdza, czy przedsiębiorstwo świadczące usługi łączności:

1) wywiązało się z obowiązku powiadomienia w terminie;

2) treść złożonego powiadomienia odpowiada wymogom określonym w art. 3^2 ust. 2 i w pełni

odzwierciedla sprzęt i oprogramowanie używane przez przedsiębiorstwo świadczące usługi łączności w momencie składania powiadomienia.

(3) W odniesieniu do obowiązku uzyskania zezwolenia na używanie sprzętu lub oprogramowania audytor sprawdza, czy przedsiębiorstwo świadczące usługi łączności:

1) wywiązało się z obowiązku uzyskania zezwolenia w terminie i w odniesieniu do każdego elementu sprzętu lub oprogramowania podlegającego obowiązkowi uzyskania zezwolenia;

2) złożyło wniosek o zezwolenie na używanie sprzętu lub oprogramowania o treści zgodnej z wymogami art. 3^3 ust. 3;

3) w sposób uzasadniony polegało na wymogach art. 3^3 ust. 2, eliminując cyberincydent lub bezpośrednio mu zapobiegając;

4) zasadnie pominęło wniosek o zezwolenie na używanie sprzętu lub oprogramowania w sytuacjach, o których mowa w art. 3^3 ust. 4.

(4) Audytor przedkłada wyniki audytów określonych w ust. 2 i 3 Urzędowi Ochrony Konsumentów i Regulacji Technicznych 30 dni po przeprowadzeniu audytu.";

5) rozporządzenie uzupełnia się o art. 8^1 i 8^2 w brzmieniu:

„**§ 8^1. Wykonanie obowiązku złożenia wniosku o zezwolenie na używanie**

(1) Wniosek o zezwolenie na używanie sprzętu lub oprogramowania, które zostały oddane do użytku przed dniem 1 lutego 2022 r. lub w okresie od dnia 1 lutego do dnia 31 maja 2022 r. i które obejmują funkcję 5G NSA lub standardu sieci łączności ruchomej nowszej generacji, należy złożyć do dnia 1 czerwca 2022 r.

(2) Terminy określone w art. 3^4 oraz art. 3^6 ust. 2 nie mają zastosowania do przetwarzania wniosku, o którym mowa w ust. 1. Urząd Ochrony Konsumentów i Regulacji Technicznych rozpatruje wnioski o zezwolenie na używanie sprzętu lub oprogramowania złożone na podstawie ust. 1 w terminie do dnia 31 grudnia 2022 r.

§ 8^2. Wykonanie obowiązku zgłoszenia sprzętu lub oprogramowania używanego w sieci łączności

Obowiązek zgłoszenia, o którym mowa w art. 3^2 ust. 1, wypełnia się po raz pierwszy do dnia 1 marca 2023 r.".

§ 2. Zmiana rozporządzenia Rządu Republiki nr 129 z dnia 11 grudnia 2015 r. w sprawie statusu komisji bezpieczeństwa Rządu Republiki

Rozporządzenie Rządu Republiki nr 129 z dnia 11 grudnia 2015 r. w sprawie statusu komisji bezpieczeństwa Rządu Republiki otrzymuje brzmienie:

1) w art. 2 ust. 1 rozporządzenia wyrazy „minister handlu zagranicznego i technologii informacyjnej" zastępuje się słowami „minister przedsiębiorczości i technologii informacyjnej";

2) rozporządzenie uzupełnia się o art. 7^1 w brzmieniu:

§ 7^1. Rada ds. Cyberbezpieczeństwa

(1) Rada ds. Cyberbezpieczeństwa działa w ramach komisji.

(2) Rada ds. Cyberbezpieczeństwa:

1) opracowuje wytyczne na potrzeby rozwoju polityki cyberbezpieczeństwa;

2) zajmuje stanowisko lub przyjmuje plany w obszarze cyberbezpieczeństwa;

3) zapewnia zgodność używania sprzętu i oprogramowania wskazanego we wniosku przedsiębiorstwa świadczącego usługi łączności z interesami państwa w obszarze bezpieczeństwa;

4) wykonuje inne zadania przydzielone przez komisję.

(3) Podczas wykonywania zadania określonego w ust. 2 pkt 3 Rada ds. Cyberbezpieczeństwa ma prawa i obowiązki przyznane organowi administracyjnemu w ustawie o postępowaniu administracyjnym.

(4) Rada ds. Cyberbezpieczeństwa ma przewodniczącego i kierownika. Praca Rady ds. Cyberbezpieczeństwa jest zarządzana przez kierownika.

(5) W skład Rady ds. Cyberbezpieczeństwa wchodzą członkowie następujących ministerstw i agencji:

1) Inspektorat Ochrony Danych;

2) Ministerstwo Edukacji i Badań Naukowych;

3) Ministerstwo Sprawiedliwości;

4) Liga Obrony;

5) Ministerstwo Obrony;

6) Estońska Służba Bezpieczeństwa Wewnętrznego;

7) Siły obronne;

8) Ministerstwo Środowiska;

9) Ministerstwo Kultury;

10) Ministerstwo Wsi;

11) Ministerstwo Gospodarki i Komunikacji;

12) Rada Policji i Straży Granicznej;

13) Prokuratura;

14) Ministerstwo Finansów;

15) Państwowy Urząd Systemu Informatycznego;

16) Biuro Rządu;

17) Ministerstwo Spraw Wewnętrznych;

18) Ministerstwo Spraw Społecznych;

19) Urząd ds. Ochrony Konsumentów i Regulacji Technicznych;

20) Agencja Wywiadu Zagranicznego;

21) Ministerstwo Spraw Zagranicznych.

(6) Zastępca członka Rady ds. Cyberbezpieczeństwa ma prawa zastępowanego członka.

(7) W razie potrzeby udział innych osób w pracach Rady ds. Cyberbezpieczeństwa jest organizowany przez kierownika Rady ds. Cyberbezpieczeństwa.

(8) Rada ds. Cyberbezpieczeństwa uzyskuje kworum, jeżeli co najmniej dwie trzecie liczby jej członków z prawem do głosowania uczestniczy w posiedzeniu. Po wykonaniu zadania określonego w ust. 2 pkt 3 Rada ds. Cyberbezpieczeństwa uzyskuje kworum, jeżeli w posiedzeniu uczestniczą członkowie Rady ds. Cyberbezpieczeństwa z Biura Rządu, Ministerstwa Obrony, Ministerstwa Gospodarki i Komunikacji, Ministerstwa Spraw Wewnętrznych i Ministerstwa Spraw Zagranicznych.

(9) Rada ds. Cyberbezpieczeństwa podejmuje decyzje większością głosów członków z prawem głosu obecnych na posiedzeniu. Biuro Rządu i ministerstwa mają prawo głosu. Każde ministerstwo i Biuro Rządu mają jeden głos. W przypadku równego rozłożenia głosów głos decydujący należy do przewodniczącego Rady ds. Cyberbezpieczeństwa lub, w razie jego nieobecności, do kierownika.

(10) Przy wykonywaniu zadania określonego w ust. 2 pkt 3 prawo głosu mają Biuro Rządu, Ministerstwo Obrony, Ministerstwo Gospodarki i Komunikacji, Ministerstwo Spraw Wewnętrznych i Ministerstwo Spraw Zagranicznych.

(11) Zasady proceduralne Rady ds. Cyberbezpieczeństwa są zatwierdzane przez komitet.

(12) Zasady proceduralne, o których mowa w ust. 11, określają:

1) przewodniczący i kierownik Rady ds. Cyberbezpieczeństwa;

2) członkowie z ministerstw i agencji, o których mowa w ust. 5, ze względu na swoje stanowisko;

3) zastępstwo członków, przewodniczącego i kierownika Rady ds. Cyberbezpieczeństwa;

4) inne wymogi organizacyjne.”.

§ 3. Wejście rozporządzenia w życie

Niniejsze rozporządzenie wchodzi w życie z dniem 1 lutego 2022 r.

Jaak Aab

Minister Administracji Publicznej pełniący obowiązki Premiera

Andres Sutt

Minister Przedsiębiorczości i Technologii Informacyjnej

Taimar Peterkop

Sekretarz Stanu